БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ – СОФИЯ

ИВО МИХАЙЛОВ МИХАЙЛОВ

КОХОМОЛОГИИ НА ГАЛОА И РЕАЛИЗИРАНЕ НА p-ГРУПИ КАТО ГРУПИ НА ГАЛОА

Д И С Е Р Т А Ц И Я

за придобиване на научната степен
“доктор на математическите науки”
по научна специалност
01.01.02 – Алгебра и теория на числата

БАН, София, 2011 г.

Съдържание

Увод

Нека първо да припомним, че крайното разширение K/k наричаме *нормално* (или *разширение на Галоа*), ако k е неподвижно подполе на някоя група $G \leq \mathrm{Aut}(K)$. Групата G се нарича група на Галоа на разширението K/k, която ще означаваме с $\mathrm{Gal}(K/k)$.

Тази дефиниция включва изискването за сепарабелност, тъй като едно разширение K/k е нормално тогава и само тогава, когато е поле на разлагане на някакъв сепарабелен полином $p(x) \in k[x]$ (виж [МЗ, Гл. V, Теорема 5]). Ние ще използваме предимно термина "разширение на Галоа", тъй като много автори дефинират нормално разширение като поле на разлагане на полином, който не е непременно сепарабелен, а разширение на Галоа като нормално и сепарабелно разширение.

Нека G е крайна група, и нека K е поле. **Обратната задача** в теорията на Галоа се състои от две части:

I Съществуване. Да се определи дали съществува разширение на Галоа M/K такова, че групата на Галоа $\mathrm{Gal}(M/K)$ е изоморфна на G.

II Явна конструкция. Ако G се реализира като група на Галоа над K, да се конструират в явен вид разширения на Галоа или полиноми над K, притежаващи G като група на Галоа.

Класическата обратна задача в теорията на Галоа е всъщност частта за съществуване за полето $K = \mathbb{Q}$ на рационалните числа. Въпросът дали всички крайни групи могат да се реализират над $\mathbb{Q}$ е един от най-предизвикателните проблеми в математиката, който все още не е решен. В тази връзка, съществува една интересна версия на обратната задача, която касае регулярните разширения: Нека $\mathbf{t} = (t_1, t_2, \ldots, t_n)$ са независими променливи. Крайното разширение на Галоа $\mathbb{M}/\mathbb{Q}(\mathbf{t})$ тогава се нарича *регулярно*, ако $\mathbb{Q}$ е относително алгебрично затворено в $\mathbb{M}$, т.е. всеки елемент в $\mathbb{M} \setminus \mathbb{Q}$ е трансцедентен над $\mathbb{Q}$.

Регулярната обратна задача се състои в следното: Дали всяка крайна група се реализира като група на Галоа на регулярно разширение на $\mathbb{Q}(\mathbf{t})$? Когато имаме регулярно разширение на Галоа $\mathbb{M}/\mathbb{Q}(\mathbf{t})$, според теоремата на Хилберт за неразложимостта слева, че съществува 'специализирано' разширение $M/\mathbb{Q}$ със същата група на Галоа. Нещо повече, такива специализирани разширения M/K съществуват за всяко Хилбертово поле с характеристика 0.

Изброените по-горе обратни задачи са получили положителен отговор в някои частни случаи, например:

1. Ако $K = \mathbb{C}(t)$, където t е променлива, всяка крайна група G се реализира като група на Галоа над K. Това следва принципно от теоремата за съществуване на Риман. По-общо, абсолютната група на Галоа на функционалното поле $K(t)$ е свободна про-крайна група с безброй пораждащи, когато K е алгебрично затворено, виж [Har].

2. Ако $K = \mathbb{F}_q$ е крайно поле, групата на Галоа на всеки полином над K е циклична.

3. Ако K е $\mathfrak{p}$-адично поле, всеки полином над K е разрешим.

Има няколко монографии, адресиращи споменатите обратни задачи, които съдържат обширен обзор, виж например [MM2, Vö, Se4, JLY]. Преди да изложим целите на нашата дисертация, ще дадем кратък исторически преглед на най-важните резултати в областта на класическата обратна задача, постигнати до момента (виж също така [MZ5]).

В началото на 19 век е получен следният резултат, чието доказателство може да бъде намерено в повечето книги посветени на теорията на полета от класове:

Теорема 0.0.1. (Кронекер-Вебер) *Всяка крайна абелова група G се явява група на Галоа над $\mathbb{Q}$. Нещо повече, G може да се реализира като група на Галоа на подполе на циклотомното поле $\mathbb{Q}(\zeta)$, където ζ е n-ти корен на единицата за някое естествено число n.*

Първото систематично изучаване на обратната задача в теорията на Галоа е започнато от Хилберт през 1892. Той използва своята теорема за неразложимост за да докаже следния резултат:

Теорема 0.0.2. *За всяко $n \geq 1$, симетричната група S_n и алтернативната група A_n се явяват групи на Галоа над $\mathbb{Q}$.*

Първите явни примери на полиноми притежаващи алтернативната група A_n като група на Галоа се дават от Шур [Schur] през 1930 г. През 1916 г., Еми Ньотер [No] повдига следния въпрос:

НЬОТЕРОВАТА ЗАДАЧА. *Нека $M = \mathbb{Q}(t_1, \ldots, t_n)$ е полето от рационални функции на n променливи. Симетричната група S_n от ред n действа върху M чрез пермутиране на променливите. Нека G е транзитивна подгрупа на S_n, и нека $K = M^G$ е подполето на G-неподвижните рационални функции на M. Дали K е рационално разширение на $\mathbb{Q}$? Т.е., дали K е изоморфно на поле от рационални функции над $\mathbb{Q}$?*

Ако ньотеровата задача има положителен отговор, то G може да се реализира като група на Галоа над $\mathbb{Q}$, и даже над всяко хилбертово поле с характеристика 0. По подобие на обратната задача, можем да обобщим и ньотеровата задача над произволно поле k. Тогава, ако ньотеровата задача има положителен отговор за дадена група, може да се построи семейство от параметрични разширения над k (или еквивалентно, да се построят пораждащи параметрични полиноми), които реализират G по такъв начин, че при произволен набор на параметрите винаги да получаваме G-разширения.

Следващата важна стъпка е направена през 1937 г. от А. Шолц и Х. Райхард [Scho, Re], които доказват следната теорема за съществуване:

Теорема 0.0.3. *За произволно нечетно просто число p, всяка крайна p-група се реализира като група на Галоа над $\mathbb{Q}$.*

Все още не е известно дали съществува регулярно разширение на Галоа над $\mathbb{Q}(t)$, което има група на Гаола G за произволна p-група G.

Финалната стъпка относно разрешимите групи е направена от Шафаревич [Sha], макар и с грешка в случая на простото число 2. В бележките приложени към неговият сборник от статии стр. 752, Шафаревич скицира метод за корекция на своето доказателство. Подробно и вярно доказателство читателят може да намери в книката на Нойкирх, Шмид и Винберг [NSW, Chapter IX].

Теорема 0.0.4. (Шафаревич) *Всяка разрешима група е група на Галоа над $\mathbb{Q}$.*

Измежду крайните прости групи, проективните групи $\mathrm{PSL}(2,p)$ за някои нечетни прости числа p са първите реализирани като групи на Галоа. Съществуването е доказано от Ших през 1974, а по-късно са конструирани полиноми от Мале и Мацат:

Теорема 0.0.5. (Ших [Shi]) *Нека p е нечетно просто число такова, че някое от числата $2, 3$ или 7 е квадратичен неостатък по модул p. Тогава $\mathrm{PSL}(2,p)$ се явява група на Галоа над $\mathbb{Q}$.*

Теорема 0.0.6. (Мале и Мацат [MM1]) *Нека p е нечетно просто число такова, че $p \not\equiv \pm 1 \pmod{24}$. Тогава могат да бъдат конструирани явни семейства от полиноми над $\mathbb{Q}(t)$ с група на Галоа $\mathrm{PSL}(2,p)$.*

Измежду 26-те спорадични прости групи, всички, с изключение евентуално на една, а именно групата на Матьо $\mathbf{M}_{23}$, са реализирани като групи на Галоа над $\mathbb{Q}$ от Мацат и неговите сътрудници.

Групата на Фишер-Грийз M, известна като "чудовището" е най-голямата спорадична проста група. Нейният ред е

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

През 1984, Томпсън успява да докаже следната теорема за съществуване.

Теорема 0.0.7. (Томпъсн [Th]) *Групата "чудовище" е група на Галоа над $\mathbb{Q}$.*

По-късно, няколко семейства от прости линейни групи са реализирани като групи на Галоа над $\mathbb{Q}$ (виж [MM2]).

Трябва да отбележим, че всички тези резултати за реализирането на прости групи са постигнати с метода на ригидност и теоремата на Хилберт за неразложимостта. Подробно изложение на този подход може да се намери например в книгите [MM2, Se4].

Напоследък бяха разработени множество изчислителни методи, подпомогнати от компютър, даващи групите на Галоа на полиноми над $\mathbb{Q}$. Някои от тези резултати са публикувани в специалния брой "Algorithmic methods in Galois Theory" на списанието "Journal of Symbolic Computation", Volume 30, Issue 6 (Dec. 2000). В този брой се намира статията [KM1], където Клунерс и Мале показват, че всяка транзитивна група от степен по-малка или равна на 15 се реализира като група на Галоа над $\mathbb{Q}$. В друга статия от същите автори [KM2] е анонсирана база с данни за числови полета.

Тя обхваща около 100 000 полиноми, пораждащи различни числови полета над рационалните числа от степен до 15-та. Базата с данни съдържа полиноми за всички транзитивни пермутационни групи и е достъпна чрез компютърната алгебра "Kant". В същата статия е публикувано доказателството на един забележителен резултат на Сер, който твърди, че ако *всяка* крайна група се реализира като група на Галоа над $\mathbb{Q}$, то тогава е възможно те да се реализират вътре в $\mathbb{R}$.

Ще продължим нашия обзор с резултати, касаещи обобщението на класическата обратна задача над произволно поле k. В този случай се появяват допълнителни условия, които трябва да се изследват индивидуално за всяка група. Така например, цикличната група от ред 2 се реализира над поле k с характеристика различна от 2 тогава и само тогава, когато k не е квадратично затворено (т.е. съществува $a \in k$ такова, че $\sqrt{a} \notin k$). Цикличната група от ред 4 е добре известно, че се реализира над k тогава и само тогава, когато съществува елемент от k, който е сума на два квадрата, но не е квадрат.

Ако групата G притежава нормална подгрупа A, тогава реализирането на факторгрупата $F = G/A$ като група на Галоа над k се явява необходимо условие за реализирането на групата G над k. По този начин възниква и следващото обобщение на обратната задача – задачата за вложимост на полета.

Нека K/k е разширение на Галоа с група на Галоа F и нека α е епиморфизъм на G върху F. Да решим *задачата за вложимост* $(K/k, G, \alpha)$ означава да покажем, че съществува поле L, съдържащо K и нормално над k, така че групата на Галоа на разширението L/k да е изоморфна на G и за всеки елемент $g \in G$ ограничението му върху K да съвпада с $\alpha(g)$. Да означим с A ядрото на хомоморфизма α. Ще казваме, че A е ядро на задачата за вложимост, която ще бележим още с $(K/k, G, A)$.

Яковлев [Як, ИЛФ] предлага един кохомологичен подход, който е доразвит от нас в [MZ1], където намираме връзката между препятствията на първоначалната задача и съпътстващите задачи от първи и втори тип. Препятствията представляват определени елементи в кохомологичните групи $H^1(*,*)$ и $H^2(*,*)$. Тяхното "разпадане" (т.е. тривиалност като кохомологични класове) се явява необходимо и достатъчно условие за разрешимост на задачата за вложимост. Това дава възможност да се докажат някои нови резултати и да се дадат кратки доказателства на известни факти, като теоремите на Кохендорфер например, според които всяка задача за вложимост може да се сведе към еквивалентнта на нея задача за вложимост, касаеща p-групи.

Това обуславя важността на изследването на реализирането на p-групите като групи на Галоа.

Резултатите относно реализирането на групите от редове 4 и 8 се срещат в голям брой стари публикации и затова често се наричат "математически фолклор" от съвременните автори. Първият по-значим напредък при реализирането на групите от ред 16 като групи на Галоа е осъществен през 90-те години на 20-ти век в работите на Киминг [Ki] и Ледет [Le1]. Киминг използва явни кохомологични пресмятания за да намери необходими и достатъчни условия за реализирането на някои от групите от ред 16. Неговите резултати, обаче дават прекалено сложни за практически цели условия. Ледет получава по-елегентни кохомологичните критерии, които правят възможно разлагането на препятствията като произведения на кватернионни алгебри в групата на Брауер $\mathrm{Br}(k)$. Този подход е използван и от нас в публикациите [Mi8, Mi10, MZ4], а също и в докторската дисертация [Ми].

Теорията на квадратичните форми играе важна роля при конструирането на разширенията на Галоа - виж например [GSS, Le3], където са построени семейства от параметрични разширения на Галоа, които реализират всички неабелови групи от ред 16 с изключение на кватернионната група Q_{16}. Известно е, че ньотеровата задача има отрицателен отговор за тази група над някои полета, така че не е възможно да се даде параметрично описание на Q_{16} разширенията над произволно поле k. В нашата работа [Mi9] правим описание на Q_{16} разширенията в три частни случая.

Следващата крачка в изследването на реализирането на 2-групи е намирането на препятствията на групите от ред 32. Някои от тези групи са разгледани в статиите [Le2, Sm, ST]. Първото пълно описание на препятствията на всички неабелови групи от ред 32 е направено от нас в [Mi7]. По-късно се появи статията на Грундман и Смит [GS1], където се използат резултатите от [Mi7].

Ледет предлага в [Le2] един кохомологичен метод, който прави възможно пресмятането на препятствия на задачи за вложимост с ядро от ред 4, които съответстват на кватернионната, диедралната и квазидиедралната (известна още като полудиедралната) групи от ред 32. Ние доразвиваме неговите идеи в статиите [Mi1, Mi2], където пресмятаме препятствията на някои задачи за вложимост, съответстващи на четирите неабелови групи от ред 2^n имащи циклична подгрупа с индекс 2 за произволно $n \geq 4$. Това е извършено при определено предположение за принадлежност на корените на единицата.

С помощта на множество теоретични методи - изображения на рестрикция и корестрикция, ортогонални представяния на групи, алгебри на Клифорд (виж [Se3, Fr, Le4] за съответните дефиниции) и др., ние успяхме да намерим препятствията за реализирането на някои от най-често използваните неабелови 2-групи. В [Mi4] сме пресметнали препятствията и разширенията на Галоа, реализиращи модулярната 2-група и някои нейни сродни групи над произволни полета, без ограничения за корените на единицата. В статиите [Mi5] и [Mi12] сме намерили необходими и достатъчни условия за реализирането на всички неабелови групи от ред 2^n, имащи циклична подгрупа с индекс 4 над полета съдържащи корен на единицата от степен 2^{n-2} за произволно $n \geq 4$.

Що се отнася до реализирането на p-групи като групи на Галоа за p-нечетно просто число, известните резултати са оскъдни. Статиите [Br, Sw, MS2, MSS2, Wa] съдържат, може би, най-същественото, постиганто в тази насока от различни математици. Ние сме изследвали някои популярни p-групи, които не са изследвани до този момент – четири неабелови групи от ред p^4, модулярната p-група и някои нейни сродни групи. Резултатите, постигнати от нас в тази област са публикувани в [Mi3, Mi4].

Настоящата дисертация е организирана както следва. В глава 1 е изложен кохомологичния подход при изследването на задачата за вложимост с абелово ядро, който е въведен в работите [Як, Ба] и [ИЛФ, Глава 3]. Получени са нови резултати, които развиват задълбочено този подход и правят възможно пресмятането на необходими и достатъчни условия за разрешимост на задачи за вложимост за редица крайни групи. Намерена е връзката между препятствията за разрешимост на дадена задача за вложимост с абелово ядро и съответните препятствия за съпътстващите ѝ задачи. Доказани са нови теоретични критерии, които редуцират решаването на задачи за вложимост със специфично абелово или циклично ядро към решаването на техни съпътстващи задачи.

Глава 2 е посветена на теоретични кохомологични критерии за задачата за вложимост с циклично ядро от прост ред. Тези критерии позволяват прецизното пресмятане на препятствията на редица задачи за вложимост касаещи p-групи. Един от изложените методи за получаване на такива критерии използва хомоморфизма на квадратичната корестрикция и свързаните с него свойства на кохомологиите на Галоа. В параграфи 2.4, 2.5 и 2.6 използваме един съвременен и бързо развиващ се

подход към задачата за вложимост - теорията на ортогоналните представяния на крайни групи. Считаме, че получените от нас резултати в тези параграфи са особено съществени и потенциално приложими в други области на математиката, използващи алгебри и групи на Клифорд, както и производните им групи Pin и Spin.

Глава 3 съдържа резултати, касаещи реализирането на групите от ред 2^n при $n \leq 5$. Описани са три вида кватернионни разширения от ред 16 при определени условия. Параграф 3.2 е посветен на реализирането на групите от ред 32 като групи на Галоа.

В глава 4 пресмятаме препятствията за реализирането на редица p-групи. Даваме също така описание на разширенията на Галоа, които реализират тези групи. В параграф 4.1 разглеждаме неабеловите групи от ред p^3, в параграф 4.2 се спираме на четири неабелови групи от ред p^4. Най-важните резултати са изложени в параграф 4.3, където задълбочено изследваме модулярната p-група, както и някои нейни производни групи.

В глава 5 пресмятаме препятствията на задачите за вложимост с циклично ядро от ред 2^n за неабеловите групи от ред 2^{n+3} ($n \geq 1$), имащи циклична подгрупа с индекс 2, при условие, че за някой примитивен 2^n-ти корен на единицата ζ, елементите $\zeta + \zeta^{-1}$ и $i(\zeta - \zeta^{-1})$ едновременно се съдържат в основното поле k. В параграф 5.4 даваме явно описание на разширенията на Галоа, които реализират модулярната група от ред от ред 2^{n+3} при предположението, че примитивен корен на единицата от степен 2^{n+2} се съдържа в квадратично разширение на основното поле.

В глава 6 намираме необходими и достатъчни условия за реализирането на всички неабелови групи от ред 2^n, имащи циклична подгрупа с индекс 4 над полета съдържащи корен на единицата от степен 2^{n-2} за произволно $n \geq 4$. В параграф 6.3 показваме, че разпадането на препятствията на задачите за вложимост, съответстващи на някои от тези групи води до положителен отговор на ньотеровата задача.

Глава 1
Задачата за вложимост на полета с абелово ядро

В тази глава ще изложим кохомологичния подход при изследването на задачата за вложимост с абелово ядро, който е въведен в работите [Як, Ба] и [ИЛФ, Глава 3]. Получени са нови резултати, които развиват задълбочено този подход и правят възможно пресмятането на необходими и достатъчни условия за разрешимост на задачи за вложимост за редица крайни групи. В параграфи 1.3 и 1.4 намираме връзката между препятствията за разрешимост на дадена задача за вложимост с абелово ядро и съответните препятствия за съпътстващите ѝ задачи. В параграф 1.5 получаваме някои общи критерии, които доказват достатъчността на условието за съгласуваност за решаване на специфични задачи за вложимост. В параграф 1.6 излагаме още критерии, които редуцират решаването на задачи за вложимост с циклично 2-ядро към решаването на техни съпътстващи задачи. Резултатите от тази глава са публикувани в работите [Mi1, Mi2, Mi12, MZ1, MZ2, MZ3].

1.1 Постановка на задачата за вложимост

Нека K/k е разширение на Галоа с група на Галоа F и нека α е епиморфизъм на G върху F. Да решим *задачата за вложимост* $(K/k, G, \alpha)$ означава да покажем, че съществува поле L, съдържащо K и нормално над k, така че групата на Галоа на разширението L/k да е изоморфна на G и за всеки елемент $g \in G$ ограничението му върху K да съвпада с $\alpha(g)$. Да означим с A ядрото на хомоморфизма α. Ще казваме, че A е ядро на задачата за вложимост, която ще бележим още с $(K/k, G, A)$.

Оказва се, че ако "отслабим" изискването решението L да е нормално над k и позволим L да е алгебра на Галоа, ние можем да подходим към задачата за вложи-

мост от гледна точка на кохомологичната алгебра.

Определение 1.1.1. Всяка асоциативна и комутативна крайно-мерна сепарабелна алгебра $\mathcal{A}$ над полето k наричаме S-алгебра.

Известно е, че всяка S-алгебра е изоморфна на директна сума на сепарабелни разширения на полето k.

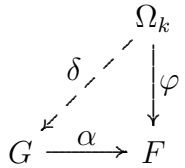
Определение 1.1.2. Една S-алгебра $\mathcal{A}$ над полето k наричаме *алгебра на Галоа* с група G, ако съществува хомоморфизъм на G в групата от автоморфизми на $\mathcal{A}$ над k и ако $\mathcal{A}$ притежава G-нормален базис над k.

Всяко нормално разширение се явява алгебра на Галоа, тъй като то притежава нормален базис.

За да подчертаем, че допускаме алгебри на Галоа за решение на задачата за вложимост, ще говорим за *слаба разрешимост* на задачата. Съответно, ако допускаме само разширения на Галоа ще говорим за *подходяща разрешимост.*

Един добре известен критерий за разрешимост се получава, като използваме групата на Галоа Ω_k на сепарабелната обвивка $\overline{k}$ над k.

Теорема 1.1.3. ([ИЛФ, Теорема 1.15.1]) *Задачата за вложимост $(K/k, G, A)$ е слабо разрешима тогава и само тогава, когато съществува хомоморфизъм $\delta : \Omega_k \to G$, такъв че диаграмата*



е комутативна, където φ е естественият епиморфизъм. Задачата за вложимост е подходящо разрешима тогава и само тогава, когато измежду хомоморфизмите $\Omega_k \to G$, за които горната диаграма е комутативна, съществува епиморфизъм.

1.2 Задачата за вложимост с абелово ядро

В този параграф ще изложим кохмологичния подход при изследването на задачата за вложимост с абелово ядро, който е описан в работите [Як, Ба] и [ИЛФ, Глава 3].

Нека $(K/k, G, A)$ е задача за вложимост с абелово ядро A, свързана с точната редица

$$1 \longrightarrow A \longrightarrow G \longrightarrow F \longrightarrow 1, \tag{1.1}$$

където $F = \mathrm{Gal}\,(K/k)$ и K съдържа примитивен корен на единицата от степен равна на периода на A.

Нека $\overline{k}$ е алгебричната сепарабелна обвивка на полето k с група на Галоа прокрайната група $\overline{F}$. Тъй като $K \subset \overline{k}$ и K е нормално разширение на k, то имаме точната редица

$$1 \longrightarrow R \longrightarrow \overline{F} \longrightarrow F \longrightarrow 1. \tag{1.2}$$

Определен е хомоморфизмът на инфлация

$$\lambda : H^2(F, A) \to H^2(\overline{F}, A).$$

Точната редица (1.1) определя кохомологичния клас $c \in H^2(F, A)$. Нека $\overline{c} = \lambda c$, където c и $\overline{c}$ са свързани с комутативната диаграма

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & \overline{G} & \longrightarrow & \overline{F} & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & A & \longrightarrow & G & \longrightarrow & F & \longrightarrow & 1, \end{array}$$

където $\overline{G}$ е директно произведение на G и $\overline{F}$ с обединена фактор-група F, т.е. $\overline{G} = G *_F \overline{F}$. В сила е

Теорема 1.2.1. ([Ба],[ИЛФ, Теорема 3.13.2]) *Задачата $(K/k, G, A)$ е слабо разрешима тогава и само тогава, когато $\overline{c} = 0$.*

Известно е (виж например [ИЛФ, §3.13]), че при решаване на задачи за вложимост възникват две "препятствия" – това са определени елементи от H^2, чиято тривиалност води до решение на задачата за вложимост $(K/k,\ G,\ A)$.

Тъй като полето K съдържа примитивен корен на единицата от степен равна на периода на A, то е определена групата на характерите на A в K^*, която означаваме с $\widehat{A} = \mathrm{Hom}\,(A, K^*)$. Групата A става F-модул като дефинираме действието $a^\rho = \overline{\rho}^{-1} a \overline{\rho}$ ($\overline{\rho}$ е про-образ на $\rho \in F$ в G). Съответно, групата $\widehat{A}$ може да се разглежда като F-модул по правилото: $\chi^\rho(a) = \chi(a^\rho)^{\rho^{-1}}$, за $\chi \in \widehat{A}$, $a \in A$, $\rho \in F$.

Нека $\mathbb{Z}[\widehat{A}]$ е груповият пръстен на $\widehat{A}$ с пораждащи елементи e_χ. Използвайки правилото $e_\chi^\rho = e_{\chi^\rho}$, груповият пръстен $\mathbb{Z}[\widehat{A}]$ се превръща в F-модул.

Имаме следната точна редица от F-модули

$$0 \longrightarrow V \longrightarrow \mathbb{Z}[\widehat{A}] \longrightarrow \widehat{A} \longrightarrow 0, \tag{1.3}$$

където епиморфизмът $\mathbb{Z}[\widehat{A}] \to \widehat{A}$ се задава така: $\sum_i k_i e_{\chi_i} \mapsto \prod_i \chi_i^{k_i}$.

Забележка 1.2.2. В [ИЛФ] всички модули на (1.3) са записани мултипликативно. Ние записваме модула $\mathbb{Z}[\widehat{A}]$ адитивно, а модула $\widehat{A}$ – мултипликативно. Използваме това малко нестандартно означение в нашата работа с цел по-добра четливост на формулите, които ще получим по-нататък.

Чрез естественият епиморфизъм $\overline{F} \to F$ всички F-модули можем да разглеждаме като $\overline{F}$-модули. Нека $\overline{k}^*$ е мултипликативната група на $\overline{k}$. Точната редица (1.3) поражда точната редица

$$0 \longrightarrow A \cong \mathrm{Hom}\,(\widehat{A}, \overline{k}^*) \longrightarrow \mathrm{Hom}\,(\mathbb{Z}[\widehat{A}], \overline{k}^*) \longrightarrow \mathrm{Hom}\,(V, \overline{k}^*) \longrightarrow 0. \tag{1.4}$$

Тъй като $H^1(\overline{F}, \mathrm{Hom}\,(\mathbb{Z}[\widehat{A}], \overline{k}^*) = 0$ (виж [ИЛФ, §3.13.3]), то (1.4) поражда точната редица

$$0 \longrightarrow H^1(\overline{F}, \mathrm{Hom}\,(V, \overline{k}^*)) \xrightarrow{\beta} H^2(\overline{F}, A) \xrightarrow{\gamma} H^2(\overline{F}, \mathrm{Hom}\,(\mathbb{Z}[\widehat{A}], \overline{k}^*). \tag{1.5}$$

Ние наричаме елемента $\eta = \gamma\overline{c}$ *първо препятствие* за разрешимост на задачата $(K/k, G, A)$. Разпадането му (т.е. $\eta = 0$) е необходимо условие за разрешимостта на задачата. Може да се покаже, че това всъщност е друга форма на известното условие за съгласуваност на Д. К. Фадеев и Х. Хасе (виж [ИЛФ, Глава 2] за различни дефиниции на това условие и [ИЛФ, §3.13.3] за доказателството на този факт). Ако $\eta = \gamma\overline{c} = 0$, то от точната редица (1.5) следва, че съществува единствен елемент $\xi \in H^1(\overline{F}, \mathrm{Hom}\,(V, \overline{k}^*))$, така че $\overline{c} = \beta\xi$.

Елементът ξ наричаме *второ препятствие* за разрешимостта на задачата $(K/k$, G, $A)$. Тогава задача е разрешима само ако $\xi = 0$, при условие, че $\eta = 0$.

Като приложим теоремата на Хохшилд-Сер за инфлацията на кохомологиите, получаваме точната редица

$$0 \longrightarrow H^1(F, \mathrm{Hom}\,(V, K^*)) \longrightarrow H^1(\overline{F}, \mathrm{Hom}\,(V, \overline{k}^*)) \longrightarrow H^1(R, \mathrm{Hom}\,(V, \overline{k}^*)). \tag{1.6}$$

От [ИЛФ, §3.13.3] е известно, че $H^1(R, \mathrm{Hom}\,(V, \overline{k}^*)) = 0$. Тогава от (1.6) следва, че

$$H^1(\overline{F}, \mathrm{Hom}\,(V, \overline{k}^*)) \cong H^1(F, \mathrm{Hom}\,(V, K^*)).$$

От друга страна, според [ИЛФ, 3, Теорема 13.3.3] съществува единствен изоморфизъм измежду групите $H^1(F, \mathrm{Hom}\,(V, K^*))$ и $\mathrm{Ext}^1_F(V, K^*)$. Така получаваме изоморфизмът

$$H^1(\overline{F}, \mathrm{Hom}\,(V, \overline{k}^*)) \cong \mathrm{Ext}^1_F(V, K^*).$$

От точната редица (1.3) получаваме следната точна редица за функтора Ext:

$$\mathrm{Ext}^1_F(\mathbb{Z}[\widehat{A}], K^*) \longrightarrow \mathrm{Ext}^1_F(V, K^*) \xrightarrow{\delta} \mathrm{Ext}^2_F(\widehat{A}, K^*),$$

където $\mathrm{Ext}^1_F(\mathbb{Z}[\widehat{A}], K^*) \cong H^1(F, \mathrm{Hom}\,(\mathbb{Z}[\widehat{A}], K^*)) = 0$. Следователно, хомоморфизмът δ е инективен и затова можем да считаме, че $\xi \in \mathrm{Ext}^2_F(\widehat{A}, K^*)$.

Второто препятствие, обаче е много трудно да се пресметне. По тази причина задачите за вложимост, за които $H^1(\overline{F}, \mathrm{Hom}(V, \overline{k}^*)) = 0$ са от особен интерес. Изясняването на структурата на модула V е от критично значение за откриването на такива задачи.

Сега ще продължим с описание на свободната абелова група V. В [ИЛФ, §3.11, стр. 84] погрешно се твърди, че V е породена като свободна абелова група от елементите $e_\chi + e_{\chi^{-1}}$. Точната редица (1.3) всъщност е свободната резолюция на $\widehat{A}$. Модулът V се явява подгрупата на $\mathbb{Z}[\widehat{A}]$, породена от елементите на $\mathbb{Z}[\widehat{A}]$, съответстващи на левите страни от дефиниционните съотношения на $\widehat{A}$. Тъй като групата $\widehat{A}$ е крайна, ранга на V трябва да е равен на ранга на $\mathbb{Z}[\widehat{A}]$. Означаваме с U подмодулът на V породен от елементите $e_\chi + e_{\chi^{-1}}$. Означаваме с n редът на A, който съвпада с ранга на $\mathbb{Z}[\widehat{A}]$. Можем да запишем $n = 1 + s + t$, където $s \geq 0$ е броят на елементите от ред 2 в $\widehat{A}$, и $t \geq 0$ е броят на елементите от ред > 2 в $\widehat{A}$. Тогава рангът на U е $1 + s + t/2$ което е по-малко от n, когато $\widehat{A}$ не е елементарната абелова 2-група.

Нещо повече, всеки елемент от вида $e_{\chi_1} + e_{\chi_2} - e_{\chi_1\chi_2} \in V$ не е в $\langle U, e_1 \rangle$ ако $\chi_1, \chi_2 \neq 1, \chi_2 \neq \chi_1^{-1}$. Да допуснем противното. Тогава

$$e_{\chi_1} + e_{\chi_2} - e_{\chi_1\chi_2} = \alpha_1(e_{\chi_1} + e_{\chi_1^{-1}}) + \alpha_2(e_{\chi_2} + e_{\chi_2^{-1}}) + \alpha_3(e_{\chi_1\chi_2} + e_{(\chi_1\chi_2)^{-1}}),$$

за някои $\alpha_i \in \mathbb{Z}$. Ако $\chi_1\chi_2 \neq \chi_1^{-1}$ и $\chi_1\chi_2 \neq \chi_2^{-1}$, трябва да са в сила и двете равенства $\alpha_1 = 0$ и $\alpha_1 = 1$, което е противоречие. Ако $\chi_1\chi_2 = \chi_1^{-1}$, то $\alpha_3 = 0, \alpha_1 = 1$ и $\alpha_1 = -1$, което отново е противоречие.

Сега ще изложим един метод за намиране на $\mathbb{Z}$-базис на V.

Лема 1.2.3. ([Mi12, Lemma 2.2]) *Нека $n = |A|$. Тогава съществува $\mathbb{Z}$-базис $v_1, \ldots, v_n$ на V, за който всяко v_i е от вида $e_\psi + e_\varphi - e_{\psi\varphi}$ за някои $\psi, \varphi \in \widehat{A}$.*

Доказателство: Можем да запишем $\widehat{A}$ като директно произведение на циклични подгрупи: $\widehat{A} = \langle\chi_1\rangle \times \langle\chi_2\rangle \times \cdots \times \langle\chi_s\rangle$ за някое $s \geq 1$. Нека $|\chi_i| = k_i$ за $i = 1, \ldots, s$.

Стъпка I. Дефинираме

$$v_1 = e_1, v_2 = e_{\chi_1} + e_{\chi_1} - e_{\chi_1^2}, v_3 = e_{\chi_1} + e_{\chi_1^2} - e_{\chi_1^3}, \ldots, v_{k_1} = e_{\chi_1} + e_{\chi_1^{k_1-1}} - e_1.$$

Да допуснем, че $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_{k_1} v_{k_1} = 0$ за някои $\alpha_i \in \mathbb{Z}$. Сравнявайки коефициентите на тази линейна комбинация, получаваме, че $\alpha_1 = \alpha_{k_1}$ и $\alpha_2 = \alpha_3 = \cdots = \alpha_{k_1}$. Следователно, $\alpha_1 k_1 e_{\chi_1} = 0$, значи $\alpha_i = 0$ за всяко i.

Стъпка II. Дефинираме

$$\begin{aligned}
&v_{k_1+i} = e_{\chi_2} + e_{\chi_2^i} - e_{\chi_2^{i+1}},\\
&v_{k_1+(k_2-1)+i} = e_{\chi_1} + e_{\chi_2^i} - e_{\chi_1\chi_2^i},\\
&v_{k_1+(2k_2-2)+i} = e_{\chi_1^2} + e_{\chi_2^i} - e_{\chi_1^2\chi_2^i},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&v_{k_1+(k_1-1)(k_2-1)+i} = e_{\chi_1^{k_1-1}} + e_{\chi_2^i} - e_{\chi_1^{k_1-1}\chi_2^i},
\end{aligned}$$

където $i = 1, 2, \ldots, k_2 - 1$. Аналогично на стъпка I, не е трудно да се провери, че така зададените вектори $v_1, \ldots, v_{k_1k_2}$ са независими над $\mathbb{Z}$.

Стъпка III. Можем да дефинираме елементите $v_{k_1k_2+1}, \ldots, v_{k_1k_2k_3}$, следвайки същия метод, както в стъпка II. Това е въпрос единствено на тромаво индексиране, така че ще пропуснем явните формули. Ще отбележим само, че тези елементи са от следните два вида: $e_{\chi_3} + e_{\chi_3^i} - e_{\chi_3^{i+1}}$ и $e_{\chi_1^i\chi_2^j} + e_{\chi_3^l} - e_{\chi_1^i\chi_2^j\chi_3^l}$ за $i = 1, 2, \ldots, k_1 - 1; j = 1, 2, \ldots, k_2 - 1; l = 1, 2, \ldots, k_3 - 1$.

Можем да продължим по същия начин с останалите $n-3$ стъпки, получавайки накрая елементи $v_1, \ldots, v_n$ които са $\mathbb{Z}$-независими. Остава само да се покаже, че тези елементи наистина пораждат V като свободна абелова група.

Нека V_1 е подгрупата на V, породена от елементите $v_1, \ldots, v_n$. Да отбележим, че за произволно $\chi \in \widehat{A}$ имаме $\chi = \prod_{i=1}^{r} \chi_i^{\alpha_i}$ за някои $r \leq s$ и $\alpha_r \neq 0$. Според дефинициите на елементите v_i получаваме, че

$$e_\chi \equiv e_{\prod_{i=1}^{r-1} \chi_i^{\alpha_i}} + e_{\chi_r^{\alpha_r}} \equiv \sum_{i=1}^{r} e_{\chi_i^{\alpha_i}} \equiv \sum_{i=1}^{r} \alpha_i e_{\chi_i} \pmod{V_1}. \tag{1.7}$$

Сега, за произволно $v \in V$ имаме $v \equiv \sum_{i=1}^{s} \beta_i e_{\chi_i} \pmod{V_1}$, където $\prod_{i=1}^{s} \chi_i^{\beta_i} = 1$. Отново от (1.7) следва, че $v \equiv \sum_i e_{\chi_i^{\beta_i}} \equiv e_{\prod_i \chi_i^{\beta_i}} \equiv e_1 \equiv 0 \pmod{V_1}$. Оттук $V = V_1$ и доказателството е завършено. $\square$

1.3 Съпътстващи задачи от първи тип

Нека $\varphi : A \to A_1$ е F-хомоморфизъм. Тогава φ индуцира комутативната диаграма

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & G & \xrightarrow{\alpha} & F = \mathrm{Gal}(K/k) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & A_1 & \longrightarrow & G_1 & \xrightarrow{\alpha} & F = \mathrm{Gal}(K/k) & \longrightarrow & 1 \end{array}$$

за някой хомоморфизъм $\psi : G \to G_1$.

Означаваме с $c \in H^2(F, A)$ кохомологичният клас, който съответства на първата редица и съответно с $c_1 \in H^2(F, A_1)$ – кохомологичният клас, който съответства на втората редица от комутативната диаграма. Очевидно c_1 е образ на 2-коцикъла c при индуцирания хомоморфизъм $\varphi_* : H^2(F, A) \to H^2(F, A_1)$.

В сила е следната комутативна диаграма

$$\begin{array}{ccc} H^2(F, A) & \xrightarrow{\lambda} & H^2(\overline{F}, A) \\ \downarrow{\scriptstyle \varphi_*} & & \downarrow{\scriptstyle \overline{\varphi}} \\ H^2(F, A_1) & \xrightarrow{\lambda_1} & H^2(\overline{F}, A_1). \end{array} \tag{1.8}$$

От диаграмата (1.8) следва

$$\overline{c_1} = \lambda_1 c_1 = \lambda_1 \varphi_* \, c = \overline{\varphi} \lambda c = \overline{\varphi} \, \overline{c}.$$

Съгласно Теорема 1.2.1 задачата $(K/k, G, A)$ е разрешима, ако $\overline{c} = 0$. Следователно, ако $\overline{c} = 0$, то $\overline{c_1} = 0$. Получаваме, че ако задачата $(K/k, G, A)$ е разрешима, то е разрешима и задачата $(K/k, G_1, A_1)$.

Забележка. Твърдението остава вярно и за неабелови групи A и A_1.

Задачата $(K/k, G_1, A_1)$ наричаме *съпътстваща задача от първи тип* за задачата $(K/k, G, A)$.

Хомоморфизмът $\varphi : A \to A_1$ индуцира влагането

$$\widehat{A_1} = \mathrm{Hom}(A_1, K^*) \longrightarrow \widehat{A} = \mathrm{Hom}(A, K^*)$$

от което получаваме следната комутативна диаграма

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & V_1 & \longrightarrow & \mathbb{Z}[\widehat{A_1}] & \longrightarrow & \widehat{A_1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & V & \longrightarrow & \mathbb{Z}[\widehat{A}] & \longrightarrow & \widehat{A} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & V/V_1 & \longrightarrow & \mathbb{Z}[\widehat{A}]/\mathbb{Z}[\widehat{A_1}] & \longrightarrow & \widehat{A}/\widehat{A_1} & \longrightarrow & 0. \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}
\tag{1.9}
$$

Тъй като $\widehat{A_1} \subset \widehat{A}$, модулите $\mathbb{Z}[\widehat{A}]/\mathbb{Z}[\widehat{A_1}]$ и V/V_1 са свободни абелови групи. Тогава имаме следната точна редица от F-модули:

$$0 \longrightarrow \mathrm{Hom}(V/V_1, \overline{k}^*) \longrightarrow \mathrm{Hom}(V, \overline{k}^*) \xrightarrow{\mu} \mathrm{Hom}(V_1, \overline{k}^*) \longrightarrow 0.$$

Изображенията $\varphi : A \to A_1$, $\mu : \mathrm{Hom}(V, \overline{k}^*) \to \mathrm{Hom}(V_1, \overline{k}^*)$ и $\nu : \mathrm{Hom}(\mathbb{Z}[\widehat{A}], \overline{k}^*) \to \mathrm{Hom}(\mathbb{Z}[\widehat{A_1}], \overline{k}^*)$ индуцират комутативната диаграма с точни редове

$$
\begin{array}{ccccccc}
0 & \longrightarrow & H^1(\overline{F}, \mathrm{Hom}(V, \overline{k}^*)) & \xrightarrow{\beta} & H^2(\overline{F}, A) & \xrightarrow{\gamma} & H^2(\overline{F}, \mathrm{Hom}(\mathbb{Z}[\widehat{A}], \overline{k}^*)) \\
 & & \downarrow{\scriptstyle \overline{\mu}} & & \downarrow{\scriptstyle \overline{\varphi}} & & \downarrow{\scriptstyle \overline{\nu}} \\
0 & \longrightarrow & H^1(\overline{F}, \mathrm{Hom}(V_1, \overline{k}^*)) & \xrightarrow{\beta_1} & H^2(\overline{F}, A_1) & \xrightarrow{\gamma_1} & H^2(\overline{F}, \mathrm{Hom}(\mathbb{Z}[\widehat{A_1}], \overline{k}^*)).
\end{array}
\tag{1.10}
$$

От диаграмата (1.10) получаваме следната теорема.

Теорема 1.3.1. ([MZ1, Theorem 4.2]) *Нека η и ξ са съответно първото и второто препятствие за задачата $(K/k, G, A)$. Тогава $\overline{\nu}\eta$ и $\overline{\mu}\xi$ са съответно първото и второто препятствие за задачата $(K/k, G_1, A_1)$.*

Аналогично получаваме комутативна диаграма

$$
\begin{array}{ccccc}
0 & \longrightarrow & \mathrm{Ext}^1_F(V, K^*) & \longrightarrow & \mathrm{Ext}^2_F(\widehat{A}, K^*) \\
 & & \downarrow{\scriptstyle \mu^*} & & \downarrow{\scriptstyle \varphi_*} \\
0 & \longrightarrow & \mathrm{Ext}^1_F(V_1, K^*) & \longrightarrow & \mathrm{Ext}^2_F(\widehat{A_1}, K^*),
\end{array}
\tag{1.11}
$$

където μ^* и φ_* са индуцирани изображения.

Следствие 1.3.2. ([MZ1, Corollary 4.3]) *Нека първото препятствие за задачата* $(K/k, G, A)$ *е тривиално, т.е.* $\eta = 0$. *Тогава* $\varphi_* \xi$ *е второто препятствие за задачата* $(K/k, G_1, A_1)$.

1.4 Съпътстващи задачи от втори тип

Разглеждаме задачата $(K/k, G, A)$ и нека F_1 е подгрупа на $F = \mathrm{Gal}(K/k)$. Означаваме с G_1 пълния прообраз на F_1 при епиморфизма $\alpha : G \to F$, т.е. $G_1 = \alpha^{-1}(F_1)$. Нека $k_1 = K^{F_1}$, т.е. $\mathrm{Gal}(K/k_1) = F_1$. По този начин получаваме задачата $(K/k_1, G_1, A)$, която наричаме *съпътстваща задача от втори тип*.

Имаме комутативната диаграма

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & G_1 & \longrightarrow & F_1 = \mathrm{Gal}(K/k_1) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & A & \longrightarrow & G & \longrightarrow & F = \mathrm{Gal}(K/k) & \longrightarrow & 1. \end{array} \tag{1.12}$$

Вертикалните изображения са влагания на подгрупи в групи. По този начин, влагането на групата F_1 в групата F индуцира хомоморфизма на рестрикция $\mathrm{res} : H^2(F, A) \to H^2(F_1, A)$. Ако долният ред е кохомологичния цикъл c, то горния ред е $\mathrm{res}\, c = c_1$. Означаваме с $\overline{F_1}$ групата на Галоа на разширението $\overline{k}/k_1$, т.е. $\overline{F_1} = \mathrm{Gal}(\overline{k}/k_1)$. Следната диаграма е комутативна

$$\begin{array}{ccc} H^2(F, A) & \xrightarrow{\lambda} & H^2(\overline{F}, A) \\ \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} \\ H^2(F_1, A) & \xrightarrow{\lambda_1} & H^2(\overline{F_1}, A). \end{array} \tag{1.13}$$

Тогава $\overline{c_1} = \lambda_1 c_1 = \lambda_1 \mathrm{res}\, c = \mathrm{res}\, \lambda c = \mathrm{res}\, \overline{c}$. Получаваме комутативна диаграма с точни редове

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(\overline{F}, \mathrm{Hom}(V, \overline{k}^*)) & \xrightarrow{\beta} & H^2(\overline{F}, A) & \xrightarrow{\gamma} & H^2(\overline{F}, \mathrm{Hom}(\mathbb{Z}[\widehat{A}], \overline{k}^*)) \\ & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} \\ 0 & \longrightarrow & H^1(\overline{F_1}, \mathrm{Hom}(V, \overline{k}^*)) & \xrightarrow{\beta_1} & H^2(\overline{F_1}, A) & \xrightarrow{\gamma_1} & H^2(\overline{F_1}, \mathrm{Hom}(\mathbb{Z}[\widehat{A}], \overline{k}^*)). \end{array} \tag{1.14}$$

Вертикалните изображения са хомоморфизми на рестрикция (ограничение).

От (1.14) следва теорема аналогична на Теорема 1.3.1

Теорема 1.4.1. ([MZ1, Theorem 5.1]) *Ако η и ξ са съответно първото и второто препятствие за задачата $(K/k, G, A)$, то* $\mathrm{res}\, \eta$ *и* $\mathrm{res}\, \xi$ *са съответно първото и второто препятствие за задачата $(K/k_1, G_1, A)$.*

Съгласно първата теорема на Кохендорфер [ИЛФ, Теорема 3.5], задачата за вложимост с абелово ядро може да се сведе до разглеждането на задачата за вложимост с абелово p-ядро (p – просто число).

Нека A е абелова p-група и нека F_1 е силова p-подгрупа на F. Нека отново G_1 е пълният прообраз на F_1 при епиморфизма $\alpha : G \to F$. Да означим $m = |F| = p^r m_p$, $(p, m_p) = 1$ и $|F_1| = p^r$. Ще дадем едно кратко доказателство на известната втора редукционна теорема на Кохендорфер, която е доказана и от Ф. К. Фадеев [ИЛФ, Теорема 3.8].

Теорема 1.4.2. ([MZ1, Theorem 5.2]) *Задачата* $(K/k, G, A)$ *е разрешима тогава и само тогава, когато е разрешима задачата* $(K/k_1, G_1, A)$.

Доказателство: Нека е разрешима съпътстващата задача от втори тип (K/k_1, G_1, A). Тогава $\overline{c_1} = 0$ и $m_p \overline{c} = 0$, тъй като $\overline{F}$ е прокрайна група и $(\overline{F} : \overline{F_1}) = m_p$ (виж [Se, I, §2.4, Prop. 9]).

Нека F_2 е силова q-подгрупа на F, $q \neq p$. Аналогично $G_2 = \alpha^{-1}(F_2)$ и имаме груповото разширение

$$1 \longrightarrow A \longrightarrow G_2 \longrightarrow F_2 \longrightarrow 1, \tag{1.15}$$

което е разцепимо, т.е. $c_2 = 0$, където c_2 е кохомологичния клас, съответстващ на (1.15) в $H^2(F_2, A)$.

Тогава $\overline{c_2} = 0$, където $\overline{c_2}$ е инфлацията на c_2 в $H^2(\overline{F_2}, A)$. Получаваме, че рестрикцията (res) от $\overline{c} \in H^2(\overline{F}, A)$ в $H^2(\overline{F_i}, A)$ е нула за всички силови p_i-подгрупи F_i на F. Това означава, че $m_{p_i} \overline{c} = 0$ за всички прости делители p_i на m и следователно $\overline{c} = 0$, т.е. задачата $(K/k, G, A)$ е разрешима. □

Двете теореми на Кохендорфер позволяват задачата за вложимост с абелово ядро да се сведе до задача за вложимост с p-групи.

1.5 Брауеровата задача

Нека $A = \langle a \rangle$ е циклична група от ред n и $\zeta \in K$ е примитивен n-ти корен на единицата. Тогава $\zeta^{\rho} = \zeta^{k_\rho}$, където $\rho \in F$ и k_ρ е естествено число по $\bmod n$. Когато $a^{\rho} = \overline{\rho}^{-1} a \overline{\rho} = a^{k_\rho}$ ($\overline{\rho}$ е прообраз на ρ в G), то задачата $(K/k, G, A)$ наричаме *брауерова*.

Като приложение на изложението в т.1 ще дадем едно кратко доказателство на [ИЛФ, Теорема 3.1].

Теорема 1.5.1. ([MZ1, Theorem 3.1]) *Ако за брауеровата задача е изпълнено условието за съгласуваност, то тя е разрешима.*

Доказателство: Нека $\chi \in \widehat{A}$ и $\chi(\rho) = \zeta$. Тогава $\chi^{\rho}(a) = \chi(a^{\rho})^{\rho^{-1}} = \chi(a^{k_\rho})^{\rho^{-1}} = \zeta^{k_\rho . k_{\rho^{-1}}} = \zeta$. Следователно $\widehat{A} = \langle \chi \rangle$, $\mathbb{Z}[\widehat{A}]$ и V са модули, на които F действа тривиално. Групата $\mathrm{Hom}\,(V, K^*)$ е директно произведение на няколко множителя K^* и по теоремата на Шпайзер [Sp] е изпълнено $H^1(F, \mathrm{Hom}(V, K^*)) = 0$. Това означава, че елементът ξ (второто препятствие) е нула. Но тъй като и първото препятствие се анулира, то задачата е разрешима. □

В доказателството на горната теорема отбелязахме, че $\widehat{A}$ е тривиален F-модул. Това ни дава възможност да изкажем по-общата дефиниция на брауерова задача, когато A е абелова група. Именно, задачата за вложимост $(K/k, G, A)$ с абелово ядро A наричаме *брауерова*, ако $\widehat{A}$ е тривиален F-модул.

Сега ще изложим едно обобщение на теорема 1.5.1, което ще играе важна роля в глава 6.

Теорема 1.5.2. ([Mi12, Theorem 3.2]) *Нека A е абелова група от ред n, нека полето K съдържа примитивен n-ти корен на единицата, и нека m е цяло число такова, че $m^2 \equiv 1 \pmod{n}$. Да предположим още, че $(K/k, G, A)$ е задача за вложимост, за която действието на $F = G/A$ върху $\widehat{A}$ удовлетворява следното изискване: за произволно $\rho \in F$ имаме, че или $\chi^{\rho} = \chi^m$ за всяко $\chi \in \widehat{A}$, или $\chi^{\rho} = \chi$ за всяко $\chi \in \widehat{A}$. Тогава условието за съгласуваност е необходимо и достатъчно за слабата разрешимост на задачата за вложимост $(K/k, G, A)$.*

Доказателство: От точната редица (1.6) следва, че е достатачно да покажем, че $H^1(F, \mathrm{Hom}(V, K^*)) = 0$.

Да изберем и фиксираме произволно $\rho \in F$ такова, че $\chi^{\rho} = \chi^m$ за всяко $\chi \in \widehat{A}$. Дефинираме $U = \{u \in V : \ u^{\rho} = u\}$. Очевидно, U е свободна абелова група и

тривиален F-модул. Оттук получаваме, че групата $\mathrm{Hom}(U, K^*)$ е директно произведение на няколко копия на K^*, така че според теоремата на Шпайзер [Sp] имаме $H^1(F, \mathrm{Hom}(U, K^*)) = 0$.

Според лема 1.2.3, модулът V има $\mathbb{Z}$-базис, който се състои от елементи от вида $e_\psi + e_\varphi - e_{\psi\varphi}$ за някои $\psi, \varphi \in \widehat{A}$. Лесно може да се провери, че някои от тези базисни елементи не са в U, значи $U \neq V$. Нека $v \in V \setminus U$. Тъй като $m^2 \equiv 1 \pmod{n}$, елементът $v + v^\rho$ е в U. Следователно, $v^\rho \equiv -v \pmod{U}$.

Да предположим сега, че $\alpha v \in U$ за някое $\alpha \in \mathbb{Z}^*$. Нека $v^\rho = -v + u$ за някое $u \in U$. Тъй като U е тривиален F-модул, получаваме $(\alpha v)^\rho = -\alpha v + \alpha u = \alpha v$, значи $u = 2v$. Оттук $v^\rho = v$, което е противоречие. Следователно, $V/U \cong \sum \mathbb{Z}\overline{v}$, където $\overline{v} = v + U$. Да отбележим, че дефинираният по-горе модул U не зависи от избора на $\rho \in F$ такова, че $\chi^\rho = \chi^m$ за всяко $\chi \in \widehat{A}$. По този начин получаваме, че за всяко $\tau \in F$ имаме $v^\tau \equiv \pm v \pmod{U}$, откъдето $(\mathbb{Z}\overline{v})^\tau = \mathbb{Z}\overline{v}$. Следователно, $\mathrm{Hom}(V/U, K^*)$ е директно произведение на няколко копия на K^*, значи $H^1(F, \mathrm{Hom}(V/U, K^*)) = 0$.

Тъй като V/U е свободна абелова група, имаме, че $V = (V/U) \oplus U$ и $\mathrm{Hom}(V, K^*) = \mathrm{Hom}(V/U, K^*) \oplus \mathrm{Hom}(U, K^*)$. Така получаваме точната редица

$$0 = H^1(F, \mathrm{Hom}(V/U, K^*)) \longrightarrow H^1(F, \mathrm{Hom}(V, K^*)) \longrightarrow H^1(F, \mathrm{Hom}(U, K^*)) = 0,$$

която очевидно ни дава $H^1(F, \mathrm{Hom}(V, K^*)) = 0$. □

Естествено възниква въпросът дали е възможно още да се обобощи горната теорема. Ако е дадено фиксирано цяло число m такова, че $m \not\equiv 1 \pmod{n}$ и $m^2 \equiv 1 \pmod{n}$, да разгледаме следното действие на F върху $\widehat{A}$: за всяко $\rho \in F$ имаме или $\chi^\rho = \chi^m$ за всяко $\chi \in \widehat{A}$, или $\chi^\rho = \chi^l$ за всяко $\chi \in \widehat{A}$, където l е някое цяло число такова, че $l \not\equiv 1 \pmod{n}, l \not\equiv m \pmod{n}$ и $l^2 \equiv 1 \pmod{n}$. При тези предположения, обаче не можем да дефинираме подходящо F-тривиален подмодул U такъв, че $v^\rho \equiv -v \pmod{U}, \forall \rho \in F, \forall v \in V$. Нещо повече, в [ИЛФ, §3.14.3] е даден контра пример, показващ, че една конкретна задача за вложимост с циклично ядро от ред 8 не е разрешима. Там F е елементарната абелова група от ред 8 с пораждащи f_1, f_2 и f_3, които действат на пораждащия χ на $\widehat{A}$ така: $\chi^{f_1} = \chi^7, \chi^{f_2} = \chi^5, \chi^{f_3} = \chi^7$.

Следствие 1.5.3. ([MZ1, Theorem 3.2]) *Нека за абеловото ядро A имаме, че за произволно $\chi \in \widehat{A}$ и за произволно $\rho \in F$ е в сила $\chi^\rho = \chi^{\pm 1}$. Тогава условието за съгласуваност е необходимо и достатъчно за слабата разрешимост на задачата $(K/k, G, A)$.*

Доказателство: Първо ще покажем, че за произволни характери $\chi_1, \chi_2 \in \widehat{A}$ и за произволно $\rho \in F$ е изпълнено:

$$\chi_1^\rho = \chi_1, \chi_2^\rho = \chi_2, (\chi_1\chi_2)^\rho = \chi_1\chi_2 \qquad \text{или} \qquad \chi_1^\rho = \chi_1^{-1}, \chi_2^\rho = \chi_2^{-1}, (\chi_1\chi_2)^\rho = \chi_1^{-1}\chi_2^{-1}.$$

Да допуснем, че $\chi_1^\rho = \chi_1^{-1}$ и $\chi_2^\rho = \chi_2$. Тогава имаме два случая. В първия случай $(\chi_1\chi_2)^\rho = \chi_1^{-1}\chi_2 = \chi_1\chi_2$, откъдето $\chi_1^2 = 1$, т.е. $\chi_1^\rho = \chi_1^{-1} = \chi_1$. Във втория случай $(\chi_1\chi_2)^\rho = \chi_1^{-1}\chi_2 = \chi_1^{-1}\chi_2^{-1}$, откъдето $\chi_2^2 = 1$, т.е. $\chi_2^\rho = \chi_2 = \chi_2^{-1}$. Това доказва твърдението.

Да означим сега с U свободната абелова група породена от елементите $e_\chi + e_{\chi^{-1}} \in \widehat{A}$. Групата F действа на U тривиално, защото $(e_\chi + e_{\chi^{-1}})^\rho = e_\chi + e_{\chi^{-1}}$, $x \in \widehat{A}$, $\rho \in F$. Тогава групата $\mathrm{Hom}(U, K^*)$ е директно произведение на няколко множителя K^* и от теоремата на Шпайзер следва, че $H^1(F, \mathrm{Hom}(U, K^*)) = 0$.

По-нататък $e_{\chi^{-1}} = -e_\chi + e_\chi + e_{\chi^{-1}}$, откъдето $e_\chi^\rho = e_{\chi^\rho} \equiv \pm e_\chi \pmod U$. Според доказаното по-горе, за произволен пораждащ елемент $v = e_{\chi_1} + e_{\chi_2} - e_{\chi_1\chi_2}$ на V имаме

$$v^\rho = e_{\chi_1^\rho} + e_{\chi_2^\rho} - e_{(\chi_1\chi_2)^\rho} \equiv \pm v \pmod U.$$

За да завършим доказателството, трябва само да приложим същите разсъждения, както в теорема 1.5.2. □

Следствие 1.5.4. ([ИЛФ, §3.4.1],[MZ1, Corollary 3.3]) *Задачата за вложимост* $(K/k, G, A)$ *с циклично ядро от четвърти ред е разрешима тогава и само тогава, когато е изпълнено условието за съгласуваност.*

Доказателство: Групата на характерите $\widehat{A}$ също е циклична група от ред 4. Нека $\widehat{A} = \langle\chi\rangle$. Тогава за всяко $\rho \in F$ имаме $\chi^\rho = \chi^{\pm 1}$, $(\chi^2)^\rho = \chi^2$. □

Сега ще изложим една от формите на условието за съгласуваност (виж [ИЛФ, §3.3]). Нека $(K/k, G, A)$ е произволна задача за вложимост с абелово ядро. Въвеждаме следните означения: $F_\chi = \{\rho \in F : \ \chi^\rho = \chi\}$ – подгрупата на F, която действа на даден характер $\chi \in \widehat{A}$ тривиално; $B_\chi = \mathrm{Ker}\chi$ – ядрото на χ; $A_\chi = A/B_\chi, H_\chi = \pi^{-1}(F_\chi), G_\chi = H_\chi/B_\chi$ и K_χ – неподвижното подполе на F_χ. Може да се покаже, че A_χ е циклична група изоморфна на групата от стойности на χ. Характерът χ е пораждащ на групата на характерите на A_χ. Задачата $(K/K_\chi, G_\chi, A_\chi)$ очевидно е брауерова с циклично ядро. Тогава условието за съгласуваност за задачата $(K/k, G, A)$ е в сила

тогава и само тогава, когато всички съпътстващи задачи $(K/K_\chi, G_\chi, A_\chi)$ свързани с груповите разширения

$$1 \to A_\chi \to G_\chi \stackrel{\pi_\chi}{\to} F_\chi \to 1 \tag{1.16}$$

са разрешими за всички характери $\chi \in \widehat{A}$.

Тъй като характерът χ индуцира хомоморфизъм $\overline{\chi} : H^2(F_\chi, A_\chi) \to H^2(F_\chi, K^*)$, условието за съгласуваност може да се изкаже и по следния начин: $\overline{\chi}(c_\chi) = 1$ за всяко $\chi \in \widehat{A}$, където c_χ е 2-кокласът на (1.16) в $H^2(F_\chi, A_\chi)$.

В действителност, не е нужно да разглеждаме всички тези задачи. Достатъчно е да разгледаме задачите $(K/K_\chi, G_\chi, A_\chi)$, където χ пробягва множество от представители на класовете спрегнати елементи в групата $\widehat{A}$, разглеждана като F-модул.

В частност, за задачата за вложимост с циклично p-ядро за някое просто число p, е нужно само да се разгледат съпътстващите брауерови задачи от първи и втори тип с най-голямо ядро и най-голяма подгрупа F_χ, понеже останалите брауерови задачи са също така и техни съпътстващи задачи. Наистина, ако A е циклична p-група и A_1, A_2 са фактор-групи на A такива, че редът на A_1 е по-голям от реда на A_2, то съществува епиморфизъм $\varphi : A_1 \to A_2$. Аналогично, ако $F_2 \leq F_1$ са подгрупи на F, то задачата съответстваща на някое групово разширение на F_2 е съпътстваща от втори тип на задачата, съответстваща на някое групово разширение на F_1.

За брауеровата задача с циклично ядро всички характери са степени на дадено $\chi, F_\chi = F$ и $K_\chi = k$, така че условието за съгласуваност придобива вида: $\overline{\chi}(c) = 1$, където c е класът на (1.16) в $H^2(F, A)$. Тъй като $H^2(F, K^*)$ е изоморфна на относителната група на Брауер $\mathrm{Br}(K/k)$, можем да считаме препятствието $\overline{\chi}(c)$ като елемент на абсолютната група на Брауер $\mathrm{Br}(k)$. Нека $\Gamma = (K, F, c)$ е алгебрата на кръстосаното произведение, отговаряща на груповото разширение (1.16). Тогава класът на еквивалентност $[\Gamma] = [K, F, c] \in \mathrm{Br}(k)$ е равен на елемента $\overline{\chi}(c)$.

1.6 Задачата за вложимост с циклично 2-ядро

Нека първо да разгледаме задачата за вложимост $(K/k, G, A)$ с ядро $A = C_4$ – цикличната група от ред 4, породена от елемента a, и нека $i \in K$ е примитивен 4-ти корен на единицата. Тогава $\widehat{A}$ е породена от елемент χ такъв, че $\chi(a) = i$. Ако задачата $(K/k, G, C_4)$ не е брауерова, тогава съществува $\kappa \in F$ такова, че $\chi^\kappa = \chi^{-1}$, значи $N = F_\chi$ е подгрупа на F с индекс 2. Виждаме, че $\mathrm{Ker}\chi = \{1\}, A_\chi = C_4, G_\chi = H_\chi = \pi^{-1}(N), \mathrm{Ker}\chi^2 = \{1, a^2\} \cong C_2, A_{\chi^2} \cong C_2, F_{\chi^2} \cong F$ и $G_{\chi^2} \cong G/C_2$. Класовете спрегнати елементи в $\widehat{A}$ са: $\{1\}, \{\chi, \chi^{-1}\}$ и $\{\chi^2\}$. Да означим с $k_1 = K_\chi$ неподвижното подполе на N. Нека още полето k има характеристика различна от 2.

Според обясненията в края на предния параграф, условието за съгласуваност се изпълнява тогава и само тогава, когато съпътстващите задачи за вложимост $(K/k_1, \pi^{-1}(N), C_4)$ и $(K/k, G/C_2, C_2)$, съответстващи на груповите разширения

$$1 \to C_4 \to \pi^{-1}(N) \underset{\pi}{\to} N \to 1,$$

и съответно

$$1 \to C_2 \to G/C_2 \underset{\pi}{\to} F \to 1$$

са разрешими. Според следствие 1.5.4, условието за съгласуваност за задачи за вложимос с циклично ядро от ред 4 е достатъчно за разрешимостта им. Дефинираме хомоморфизми e, f и g от F в $\{+1, -1\}$ чрез: $a^\sigma = a^{e_\sigma}, \sigma i = i^{f_\sigma}$ и $g_\sigma = e_\sigma f_\sigma$. Тогава $N = \{\sigma \in F, g_\sigma = 1\}$, така че получаваме от друга гледна точка резултата на Ледет [Le2, Theorem 1.1].

Нека сега $A = C_{2^n}$ – цикличната група от ред $2^n (n \geq 2)$, породена от елемент a. Нека K съдържа примитивен 2^n-ти корен на единицата ζ, и нека $\chi : C_{2^n} \to K^*$ е пораждащият на $\widehat{C}_{2^n}$. Да означим $\mu_{2^n} = \langle\zeta\rangle \subset K^*$. Ако задачата $(K/k, G, A)$ е брауерова, можем да отъждествим A с μ_{2^n} като F-модули.

За нечетно m ще имаме $F_\chi = F_{\chi^m}$ и $\mathrm{Ker}\chi = \mathrm{Ker}\chi^m = \{1\}$. Нека още F_χ има индекс 2 в F. Тогава от $F_\chi \subset F_{\chi^{2m}}$ следва, че $F_\chi = F_{\chi^{2m}}$ или $F = F_{\chi^{2m}}$.

Ако $F_\chi = F_{\chi^{2m}}$, получаваме брауеровата задача $(K/K_\chi, \pi^{-1}(F_\chi)/B_{2m}, C_{2^n}/B_{2m})$, която е съпътстваща задача от първи тип на задачата $(K/K_\chi, \pi^{-1}(F_\chi), C_{2^n})$. Тук за краткост пишем $B_{2m} = B_{\chi^{2m}}$.

Ако $F = F_{\chi^{2m}}$, получаваме брауеровата задача $(K/k, G/B_{2m}, C_{2^n}/B_{2m})$. От този вид задачи се нуждаем само от тази с най-голямо ядро. Именно, нека $\chi^\sigma = \chi^{m_\sigma}, m_\sigma \in$

$\mathbb{N}$, и понеже F_χ има индекс 2, имаме $m_\sigma \in \{1, l\}$, където l е нечетно такова, че $l^2 \equiv 1 \pmod{2^n}$. Оттук $(\chi^{2m})^\sigma = \chi^{2m}$ за всяко $\sigma \in F$, тогава и само тогава, когато $2ml \equiv 2m \pmod{2^n}$, т.е. $ml \equiv m \pmod{2^{n-1}}$.

Нека сега m_0 е най-малкото естествено число такова, че $1 \leq m_0 \leq 2^{n-2}$ и $m_0 l \equiv m_0 \pmod{2^{n-1}}$. Ако m е такова, че $F = F_{\chi^{2m}}$, то $B_{2m_0} \subset B_{2m}$. Така получаваме изоморфизмите $(C_{2^n}/B_{2m_0})/(B_{2m}/B_{2m_0}) \cong C_{2^n}/B_{2m}$ и $(G/B_{2m_0})/(B_{2m}/B_{2m_0}) \cong G/B_{2m}$. Следователно задачата за вложимост $(K/k, G/B_{2m}, C_{2^n}/B_{2m})$ е съпътстваща задача от първи тип на задачата $(K/k, G/B_{2m_0}, C_{2^n}/B_{2m_0})$. По този начин условието за съгласуваност на задачата $(K/k, G, C_{2^n})$ е еквивалентно на разрешимостта на двете задачи $(K/K_\chi, \pi^{-1}(F_\chi), C_{2^n})$ и $(K/k, G/B_{2m_0}, C_{2^n}/B_{2m_0})$.

Имаме два важни случая: Ако $l \equiv 1 \pmod{2^{n-1}}$, то $m_0 = 1$ и $B_2 \cong C_2$, така че последната задача е еквивалентна на $(K/k, G/C_2, C_{2^{n-1}})$. Ако $l \equiv -1 \pmod{4}$, то $m_0 = 2^{n-2}$ и $B_{2^{n-1}} \cong C_{2^{n-1}}$, така че задачата става еквивалентна на $(K/k, G/C_{2^{n-1}}, C_2)$. По този начин получаваме следната теорема.

Теорема 1.6.1. ([Mi1, Theorem 2.1]) *Нека K/k е крайно разширение на Галоа с група на Галоа F, и нека $\zeta \in K$ е примитивен 2^n-ти корен на единицата $(n > 1)$. Да разгледаме груповото разширение*

$$1 \to C_{2^n} \to G \underset{\pi}{\to} F \to 1, \tag{1.17}$$

такова, че $e_\sigma, f_\sigma \in \{+1, -1\}$ за всяко $\sigma \in F$. Нека k_1 е неподвижното подполе на $N = \mathrm{Ker} g$. Задачата за вложимост $(K/k, G, C_{2^n})$ е разрешима, тогава и само тогава, когато задачите за вложимост $(K/k_1, \pi^{-1}(N), \mu_{2^n})$ и $(K/k, G/C_{2^{n-1}}, \mu_2)$ са разрешими.

Следващият резултат може да се получи директно от горната теорема, но ние ще представим друго доказателство, което не се базира на разсъжденията от този параграф.

Следствие 1.6.2. ([Mi2, Theorem 1.1]) *Нека K/k е крайно разширение на Галоа с група на Галоа H, и нека $\zeta \in K$ е примитивен 2^n-ти корен на единицата $(n > 1)$ такъв, че $\zeta + \zeta^{-1} \in k$ и $i(\zeta - \zeta^{-1}) \in k$. Нека $N = \mathrm{Gal}(K/k(i))$ и H действат тривиално върху C_{2^n}. Тогава задачата за вложимост $(K/k, G, C_{2^n})$ зададена с груповото разширение*

$$1 \to C_{2^n} \to G \underset{\pi}{\to} H \to 1, \tag{1.18}$$

е разрешима тогава и само тогава, когато задачите за вложимост $(K/k(i), \pi^{-1}(N), \mu_{2^n})$ *и* $(K/k, G/C_{2^{n-1}}, \mu_2)$, *зададени с*

$$1 \to \mu_{2^n} \to \pi^{-1}(N) \underset{\pi}{\to} N \to 1, \tag{1.19}$$

и, съответно, с

$$1 \to \mu_2 \to G/C_{2^{n-1}} \underset{\pi'}{\to} H \to 1, \tag{1.20}$$

са разрешими.

Доказателство: Нека $\overline{k}$ е алгебричната сепарабелна обвивки на k с про-крайна група на Галоа $\overline{H}$. Означаваме с $c \in H^2(H, C_{2^n}), c_1 \in H^2(N, \mu_{2^n})$ и $c_2 \in H^2(H, \mu_2)$ кохомологичните класове съответно на (1.18), (1.19) и (1.20). Означаваме също с $\overline{c} \in H^2(\overline{H}, C_{2^n}), \overline{c}_1 \in H^2(\overline{N}, \mu_{2^n})$ и $\overline{c}_2 \in H^2(\overline{H}, \mu_2)$ инфлациите на c, c_1 и c_2, съответно, където $\overline{H} = \mathrm{Gal}(\overline{k}/k), \overline{N} = \mathrm{Gal}(\overline{k}/k(i))$.

Да предположим сега, че задачите (които са брауерови) $(K/k(i), \pi^{-1}(N), \mu_{2^n})$ и $(K/k, G/C_{2^{n-1}}, \mu_2)$ са разрешими. Тогава $\overline{c}_1 = 1$ и $\overline{c}_2 = 1$. От параграфи 1.3 и 1.4 следва, че $\overline{c}_1 = \mu\overline{c}$ и $\overline{c}_2 = \nu\overline{c}$, където $\mu : H^2(\overline{H}, C_{2^n}) \to H^2(\overline{N}, \mu_{2^n})$ е хомоморфизъм на рестрикция, а хомоморфизма $\nu : H^2(\overline{H}, C_{2^n}) \to H^2(\overline{H}, \mu_2)$ се индуцира от епиморфизма $C_{2^n} \to C_2$. Остава да приложим [AFSS, Lemma 2], за да получим $\overline{c} = 1$, което означава, че задачата $(K/k, G, C_{2^n})$ е разрешима. □

Следствие 1.6.3. ([Mi1, Corollary 2.2]) *Нека* K/k *е крайно разширение на Галоа с група на Галоа* F, *и нека* ζ *е примитивен* 2^n*-ти корен на единицата* $(n > 1)$ *такъв, че* $\zeta + \zeta^{-1} \in k, i(\zeta - \zeta^{-1}) \in k$ *и* $i \notin K$. *Нека*

$$1 \to C_{2^n} \to G \underset{\pi}{\to} F \to 1 \tag{1.21}$$

е групово разширение. Продължаваме автоморфизмите $\sigma \in F$ *върху* $K(i)$ *чрез* $\sigma i = i$, *и нека* κ *е пораждащият на* $\mathrm{Gal}(K(i)/K)$. *Нека* $k(\sqrt{b})$ *е неподвижното подполе на* $N = \mathrm{Ker}g$ *и да означим* $k_1 = k(i\sqrt{b})$. *Тогава* $\mathrm{Gal}(K(i)/k_1) \cong F$, *и задачата за вложимост* $(K/k, G, C_{2^n})$ *е разрешима тогава и само тогава, когато задачите* $(K(i)/k_1, G, \mu_{2^n})$ *и* $(K/k, G/C_{2^{n-1}}, \mu_2)$ *са разрешими.*

Глава 2
Кохомологични критерии за задачата за вложимост с циклично ядро от прост ред

Тази глава е посветена на разработените в работите [Mi2, Mi3, Mi4, Mi5, Mi6] теоретични кохомологични критерии за задачата за вложимост с циклично ядро от прост ред. Тези критерии позволяват прецизното пресмятане на препятствията на редица задачи за вложимост касаещи p-групи, които ще разгледаме в следващите глави.

В параграф 2.2 доказваме няколко критерия, позволяващи пресмятане на препятствието на някои задачи за вложимост, касаещи p-групи със специфични фактор-групи. В параграф 2.3 излагаме метод използващ хомоморфизма на квадратичната корестрикция, който разширява значително кръга от p-групи, чиито препятствия могат да бъдат пресметнати. В параграфи 2.4, 2.5 и 2.6 използваме един съвременен и бързо развиващ се подход към задачата за вложимост - теорията на ортогоналните представяния на крайни групи. Считаме, че получените от нас резултати в тези параграфи са особено съществени и потенциално приложими в други области на математиката, използващи алгебри и групи на Клифорд, както и производните им групи Pin и Spin.

2.1 Предварителни сведения

Нека p е просто число и нека k е произволно поле с характеристика различна от p, което съдържа примитивен p-ти корен на единицата ζ. Да означим с μ_p цикличната подгрупа в k^*, породена от ζ. Нека K е разширение на Галоа на k с група на Галоа

p-групата H. Да разгледаме груповото разширение

$$1 \longrightarrow \langle\varepsilon\rangle \cong \mu_p \longrightarrow G \longrightarrow H \longrightarrow 1, \tag{2.1}$$

където ε е централен елемент от ред p в G. Ние можем да отъждествим групите $\langle\varepsilon\rangle$ и $\langle\zeta\rangle$, тъй като те са изоморфни като H-модули. Тогава мономорфизмът $\mu_p \hookrightarrow K^*$, индуцира хомоморфизма $i : H^2(H, \mu_p) \to H^2(H, K^*)$. В сила е следният известен критерий за решимост на задачата за вложимост зададена чрез K/k и груповото разширение (2.1).

Теорема 2.1.1. ([Ki]) *Нека $\gamma \neq 0$ е 2-кокласът в $H^2(H, \mu_p)$, съответстващ на неразцепимото групово разширение* (2.1)*. Тогава задачата за вложимост $(K/k, G, \mu_p)$ е подходящо разрешима тогава и само тогава, когато $i(\gamma) = 0$. Ако $K(\sqrt[p]{\beta})/k$ е решение на задачата за вложимост за някое $\beta \in K^*$, то всички решения са от вида $K(\sqrt[p]{r\beta})/k$, за $r \in k^*$.*

Елементът $i(\gamma)$ ще наричаме *препятствие* за решимост на задачата за вложимост (или за реализирането на групата G като група на Галоа над k). Тъй като задачата $(K/k, G, \mu_p)$ е брауерова, препятствието $i(\gamma)$ съвпада с първото препятствие (условието за съгласуваност) дефинирано в Глава 1.

Нека $c \in Z^2(H, \mu_2)$ представя γ. Известно е, че $H^2(H, K^*)$ е изоморфна на относителната група на Брауер $\mathrm{Br}(K/k)$ чрез изоморфизма $i(\gamma) \mapsto [K, H, c]$, където $[K, H, c] \in \mathrm{Br}(K/k)$ е класът на еквивалентност на кръстосаното произведение (K, H, c), т.е. (K, H, c) е централна проста алгебра над k, породена от K и елементите u_σ със съотношенията $u_1 = c_{1,1}, u_\sigma u_\tau = c_{\sigma,\tau} u_{\sigma\tau}$ и $u_\sigma x = \sigma(x) u_\sigma$, за $\sigma, \tau \in H$ и $x \in K$.

Абсолютната група на Брауер $\mathrm{Br}(k)$ е изоморфна на индуктивната (директна) граница $\varinjlim \mathrm{Br}(K/k)$, където K/k пробягва всички крайни разширения на Галоа. Тъй като γ е елемент от ред p, препятствието $i(\gamma)$ лежи в p-торзията на групата на Брауер $\mathrm{Br}(k)$. Според теоремата на Меркуриев-Суслин [MeS], препятствието може да бъде разложено като произведение на p-циклични алгебри (които ще наричаме обобщени алгебри на кватернионите). Нашата цел е да намерим това разлагане за всяка група, която ще разглеждаме.

Определение 2.1.2. *Обобщена кватернионна алгебра* от степен p ще наричаме централната проста алгебра над k, породена от елементи i и j такива, че $i^p = a, j^p = b$

и $ji = \zeta ij$ $(a, b \in k^*)$. Ще я бележим с $(a, b; \zeta)$. Когато $p = 2$, това е стандартната кватернионна алгебра, която ще бележим с (a, b).

Ние няма да правим разграничение между кватернионната алгебра и нейния клас на еквивалентност в групата на Брауер. Повече информация за свойствата на тези алгебри може да бъде намерена в [Pi, Гл. 15]. Тук ще изложим само най-често използваните свойства на кватернионните алгебри:

- $(a, b; \zeta) = (b, a; \zeta^{-1})$;
- $(a, b; \zeta)^{-1} = (b, a; \zeta)$;
- $(a, bc; \zeta) = (a, b; \zeta)(a, c; \zeta)$;
- $(ab, c; \zeta) = (a, c; \zeta)(b, c; \zeta)$;
- $(a, b; \zeta) = 1 \in \mathrm{Br}(k) \iff a \in N_{k(\sqrt[p]{b})/k}(k(\sqrt[p]{b})^*) \iff$
  $b \in N_{k(\sqrt[p]{a})/k}(k(\sqrt[p]{a})^*)$, където чрез $N_{K/k}$ означаваме нормата $N : K \to k$;
- $(a^p, b; \zeta) = 1$;
- Ако $a + b \in k^p$, то $(a, b; \zeta) = 1$. В частност $(a, -a; \zeta) = (a, 1 - a; \zeta) = 1$.

$(\forall a, b, c \in k^*.)$

Другата цел, която можем да си поставим е да опишем всички разширения на Галоа, които решават задачата за вложимост $(K/k, G, \mu_p)$. Това може да се постигне по следния начин. Да приемем, че препятствието се разпада, т.е. $i(\gamma) = 1$. Тогава $c \in B^2(H, K^*)$, т.е. съществува изображение $a : H \to K^*$ такова, че $c_{\sigma,\tau} = a_\sigma \sigma a_\tau a_{\sigma\tau}^{-1}, \forall \sigma, \tau \in H$. Тъй като $c_{\sigma,\tau}$ е в μ_p, имаме, че $\sigma \mapsto a_\sigma^p$ е кръстосан хомоморфизъм $H \longrightarrow K^*$. Тогава според теорема 90 на Хилберт, съществува $\omega \in K^*$ такова, че $\sigma\omega/\omega = a_\sigma^p, \forall \sigma \in H$.

В светлината на тези наблюдения, можем да процедираме по следната схема, когато търсим елемента ω:

1. Проверяваме дали $\sigma\omega/\omega$ е в $K^{*p}, \forall \sigma \in H$. Това ще гарантира, че $K(\sqrt[p]{r\omega})/k$ е разширение на Галоа. За тази цел е достатъчно да разгледаме минимално пораждащо множество на групата H.

2. Избираме произволни про-образи на пораждащото множество в групата $\mathrm{Gal}(K(\sqrt[p]{r\omega})/k)$. Проверяваме дали те удовлетворяват дефиниционните релации

на групата G. Това е напълно достатъчно, както се вижда от обясненията в увода на статията [Le3]. Например, ако $\sigma \in H$ е от ред n, про-образът на σ, да речем $\widetilde{\sigma} \in \mathrm{Gal}(K(\sqrt[p]{r\omega})/k)$, ще има ред n или pn. Можем да положим $\widetilde{\sigma}\sqrt[p]{r\omega} = \sqrt[p]{r\omega}a_\sigma$, откъдето $\widetilde{\sigma}^n\sqrt[p]{r\omega} = \sqrt[p]{r\omega}a_\sigma\sigma a_\sigma \cdots \sigma^{n-1}a_\sigma$. Следователно, $\widetilde{\sigma}$ е от ред n $\iff$ $a_\sigma\sigma a_\sigma \cdots \sigma^{n-1}a_\sigma = 1$ и е от ред pn $\iff$ $a_\sigma\sigma a_\sigma \cdots \sigma^{n-1}a_\sigma = \zeta^s \neq 1$.

Разлагането на препятствието в произведение на кватернионни алгебри може също така да послужи за конструиране на разширенията на Галоа, които са решения на дадената задача за вложимост.

Като начало нека да разгледаме една задача за вложимост, касаеща цикличната група C_{p^2}. Нека $H = C_p$ и нека $K = k(\sqrt[p]{a})$, където $a \in k^* \setminus k^{*p}$. Означаваме със σ пораждащия елемент на H такъв, че $\sigma(\sqrt[p]{a})/\sqrt[p]{a} = \zeta$. Да образуваме задачата за вложимост $(K/k, C_{p^2}, \mu_p)$ зададена чрез K/k и груповото разширение:

$$1 \longrightarrow \langle\varepsilon\rangle \cong \mu_p \longrightarrow C_{p^2} \longrightarrow H \longrightarrow 1. \tag{2.2}$$

Означаваме с Γ кръстосаното произведение, съответстващо на (2.2). Тогава Γ се поражда от елементите $\sqrt[p]{a}$ и u, където $(\sqrt[p]{a})^p = a, u\sqrt[p]{a} = \zeta\sqrt[p]{a}u$ и $u^p = \zeta$. Следователно $[\Gamma] = (a, \zeta; \zeta)$, така че $[\Gamma] = 1$ тогава и само тогава, когато $\zeta \in N_{K/k}(K^*)$. Сега ние можем лесно да опишем семейството от разширения на Галоа, които реализират C_{p^2} като група на Галоа над k. Нека задачата $(K/k, C_{p^2}, \mu_p)$ е разрешима, т.е. съществува $\alpha \in K^*$ такова, че $N_{K/k}(\alpha) = \zeta$. За $\beta = \sqrt[p]{a}(\alpha^{p-1}\sigma(\alpha)^{p-2}\cdots\sigma^{p-2}(\alpha))^{-1}$ ние имаме $\sigma(\beta)/\beta = \alpha^p$, следователно $K(\sqrt[p]{\beta})/k$ е разширение на Галоа. Можем да предполагаме, че про-образът $\overline{\sigma}$ на σ в групата $\mathrm{Gal}(K(\sqrt[p]{\beta})/k)$ действа по този начин: $\overline{\sigma}(\sqrt[p]{\beta}) = \sqrt[p]{\beta}\alpha$. От $\overline{\sigma}^p(\sqrt[p]{\beta}) = \sqrt[p]{\beta}N_{K/k}(\alpha) = \sqrt[p]{\beta}\zeta$ следва, че редът на $\overline{\sigma}$ е p^2.

Можем също така да разгледаме следния частен случай на задачата $(K/k, C_{p^2}, \mu_p)$, който ще използваме по-нататък при реализирането на p-групи като групи на Галоа. Нека p е нечетно просто число и нека $a = \zeta \notin k^{*p}$. Тогава ще имаме, че $(a, \zeta; \zeta) = 1$ и $\sigma(\sqrt[p]{\zeta})/\sqrt[p]{\zeta} = \zeta = (\sqrt[p]{\zeta})^p$. Можем да положим $\alpha = \sqrt[p]{\zeta} = \zeta_{p^2}$ и $\beta = \alpha$, откъдето $N_{K/k}(\alpha) = \alpha^p = \zeta$ и $\sigma(\beta)/\beta = \sigma(\alpha)/\alpha = \zeta = \alpha^p$. Следователно едно решение на задачата е $K(\sqrt[p]{\beta})/k = k(\zeta_{p^3})/k$, а всички решения са $K(\sqrt[p]{f\zeta_{p^2}})/k, f \in k^*$.

2.2 Пресмятане на препятствието на някои задачи за вложимост с ядро μ_p

Нека H е p-група и нека

$$1 \longrightarrow C_p \cong \langle \zeta \rangle \longrightarrow G \underset{\pi}{\longrightarrow} H \times C_p \longrightarrow 1 \tag{2.3}$$

е неразцепимо централно групово разширение с характеристичен 2-коклас $\gamma \in H^2(H \times C_p, C_p)$. Чрез $res_H\gamma$ означаваме 2-кокласът на груповото разширение

$$1 \longrightarrow C_p \longrightarrow \pi^{-1}(H) \underset{\pi}{\longrightarrow} H \longrightarrow 1.$$

Нека $\sigma_1, \sigma_2, \ldots, \sigma_m$ е минимално пораждащо множество на максималната елементарна абелова факторгрупа на H; и нека τ е пораждащият елемент на директния множител C_p. Нека $s_1, s_2, \ldots, s_m, t \in G$ са про-образи на $\sigma_1, \sigma_2, \ldots, \sigma_m, \tau$ такива, че $t^p = \zeta^j$ и $ts_i = \zeta^{d_i} s_i t$, където $i \in \{1, 2, \ldots, m\}; j, d_i \in \{0, 1, \ldots, p-1\}$.

Теорема 2.2.1. ([Mi2, Theorem 4.1],[Mi3, Theorem 2.1]) *Нека K/k е разширение на Галоа с група на Галоа H и нека $L/k = K(\sqrt[p]{b})/k$ е разширение на Галоа с група на Галоа $H \times C_p$ ($b \in k^* \setminus k^{*p}$). Да изберем $a_1, a_2, \ldots, a_m \in k^*$ такива, че $\sigma_k \sqrt[p]{a_i} = \zeta^{\delta_{ik}} \sqrt[p]{a_i}$ (δ_{ik} е делтата на Кронекер). Тогава препятствието на задачата за вложимост $(L/k, G, \mu_p)$ зададена чрез L/k и груповото разширение* (2.3) *е*

$$[K, H, res_H\gamma]\left(b, b^j \zeta^{j(1+p(p-1)/2)} \prod_{i=1}^{m} a_i^{d_i}; \zeta\right).$$

Доказателство: Алгебрата на кръстосаното произведение $B = (K, H, \zeta)$ се съдържа в $A = (L, H \times C_p, \zeta)$, следователно A е тензорно произведение на B и централизатора на B в A : $A = B \otimes_k C_A(B)$. Нека сега да разгледаме подалгебрата $k[\sqrt[p]{b}, \sqrt[p]{b}^j \prod_{i=1}^{m} \sqrt[p]{a_i}^{d_i} t]$ in A. Тъй като $t^p = \zeta^j$ и $t\sqrt[p]{b} = \zeta \sqrt[p]{b} t$, имаме, че

$$\left(\sqrt[p]{b}^j \prod_{i=1}^{m} \sqrt[p]{a_i}^{d_i} t\right)^p = b^j \zeta^j \zeta^{jp(p-1)/2} \prod_{i=1}^{m} a_i^{d_i}.$$

Ще покажем, че кватернионната алгебра $k[\sqrt[p]{b}, \sqrt[p]{b}^j \prod_{i=1}^{m} \sqrt[p]{a_i}^{d_i} t]$ е точно централизатора $C_A(B)$. Наистина, степента на $C_A(B)$ е p и от $s_\kappa \sqrt[p]{b} = \sqrt[p]{b} s_\kappa$ за всяко κ следва,

че $\sqrt[p]{b}$ се съдържа в $C_A(B)$. Накрая,

$$s_\kappa\left(\sqrt[p]{b}^j\prod_{i=1}^m\sqrt[p]{a_i}^{d_i}t\right)=\sqrt[p]{b}^j\prod_{i=1}^m(\zeta^{\delta_{i\kappa}}\sqrt[p]{a_i})^{d_i}s_\kappa t=\sqrt[p]{b}^j\prod_{i=1}^m(\zeta^{\delta_{i\kappa}}\sqrt[p]{a_i})^{d_i}\zeta^{-d_\kappa}ts_\kappa$$
$$=\zeta^{-d_\kappa}\prod_{i=1}^m\zeta^{\delta_{i\kappa}d_i}\sqrt[p]{b}^j\prod_{i=1}^m\sqrt[p]{a_i}^{d_i}ts_\kappa=\left(\sqrt[p]{b}^j\prod_{i=1}^m\sqrt[p]{a_i}^{d_i}t\right)s_\kappa,$$

понеже $\sum_{i=1}^m\delta_{i\kappa}d_i=d_\kappa$. □

Оттук можем да получим критерия за $(p,p,\ldots,p)$ централни разширения, който е намерен също така в [Sw].

Следствие 2.2.2. ([Mi3, Corollary 2.2]) *Нека* $L/k=k(\sqrt[p]{a_1},\sqrt[p]{a_2},\ldots,\sqrt[p]{a_n})/k$ *е* C_p^n *разширение, и нека* $\sigma_1,\sigma_2,\ldots,\sigma_n\in\mathrm{Gal}(L/k)$ *се задават чрез* $\sigma_i(\sqrt[p]{a_j})/\sqrt[p]{a_j}=\zeta^{\delta_{ij}}$ *(*δ_{ij} *е делтата на Кронекер). Нека*

$$1\longrightarrow\mu_p\longrightarrow G\longrightarrow C_p^n=\mathrm{Gal}(L/k)\longrightarrow 1$$

е неразцепимо централно групово разширение, и да изберем про-образи $s_1,s_2,\ldots,s_n\in G$ *на* $\sigma_1,\sigma_2,\ldots,\sigma_n$. *Дефинираме* $d_{ij}(i\le j)$ *чрез* $s_i^p=\zeta^{d_{ii}}$ *и* $s_is_j=\zeta^{d_{ij}}s_js_i(i<j)$. *Тогава препятствието на задачата за вложимост* $(L/k,G,\mu_p)$ *е*

$$\prod_{i=1}^n(a_i,\zeta;\zeta)^{d_{ii}}\prod_{i<k}(a_i,a_k;\zeta)^{d_{ik}}.$$

Доказателство: Прилагаме математическа индукция по n. За $n=1$ групата G е изоморфна на C_{p^2}, така че препятствието е $(a_1,\zeta;\zeta)$. Нека сега за $n-1$ препятствието има формата, дадена в условието. Означаваме с H групата на Галоа на $K/k=k(\sqrt[p]{a_1},\ldots,\sqrt[p]{a_{n-1}})/k$. По индукционното допускане $[K,H,res\gamma]=\prod_{i=1}^{n-1}(a_i,\zeta;\zeta)^{d_{ii}}\prod_{i<k}(a_i,a_k;\zeta)^{d_{ik}}$, където за второто произведение k пробягва множеството $\{1,2,\ldots,n-1\}$. Тогава според теорема 2.2.1 препятствието на първоначалната задача е

$$[K,H,res\gamma]\left(a_n,a_n^{d_{nn}}\zeta^{d_{nn}(1+p(p-1)/2)}\prod_{i=1}^{n-1}a_i^{-d_{in}};\zeta\right).$$

Тъй като $(a_n,a_n;\zeta)=1$ при нечетно p, $(a_n,a_n;\zeta)=(a_n,-1)$ при $p=2$, и $(a_n,a_i^{-d_{in}};\zeta)=(a_i,a_n;\zeta)^{d_{in}}$, получаваме накрая препятствието

$$\prod_{i=1}^n(a_i,\zeta;\zeta)^{d_{ii}}\prod_{i<k}(a_i,a_k;\zeta)^{d_{ik}}.$$

□

Да разгледаме сега следната ситуация. Нека G е крайна група и нека $\{\sigma_1, \ldots, \sigma_\kappa\}$ е фиксирано (не непременно минимално) пораждащо множество на G със следните свойства: $|\sigma_1| = p^{n-1}$ за $n > 1$, подгрупата H породена от $\sigma_2, \ldots, \sigma_\kappa$ е нормална в G, и факторгрупата G/H е изоморфна на цикличната група $C_{p^{n-1}}$, т.е. $\sigma_1^i \notin H, 1 \leq i < p^{n-1}$. Да вземем две произволни групови разширения

$$1 \longrightarrow \mu_p \longrightarrow G_1 \underset{\varphi}{\longrightarrow} G \longrightarrow 1 \tag{2.4}$$

и

$$1 \longrightarrow \mu_p \longrightarrow G_2 \underset{\psi}{\longrightarrow} G \longrightarrow 1. \tag{2.5}$$

Да означим с $\widetilde{\sigma}_i = \varphi^{-1}(\sigma_i)$ произволен про-образ на σ_i в G_1 и с $\overline{\sigma}_i = \psi^{-1}(\sigma_i)$ произволен про-образ на σ_i в G_2, $i = 1, \ldots \kappa$.

Определение 2.2.3. Пишем $G_2 = G_1^{(p^n, \sigma_1)}$, ако

1. $|\widetilde{\sigma}_1| = p^{n-1}$;
2. $\overline{\sigma}_1^{p^{n-1}} \in \mu_p, \overline{\sigma}_1^{p^{n-1}} \neq 1$; и
3. всички останали съотношения между пораждащите на групите G_1 и G_2 са идентични, т.е. $\widetilde{\sigma}_i^{\alpha_i} = \zeta^l \prod_{j \neq 1} \widetilde{\sigma}_j^{\beta_j} \iff \overline{\sigma}_i^{\alpha_i} = \zeta^l \prod_{j \neq 1} \overline{\sigma}_j^{\beta_j}$ за $i = 2, 3, \ldots, \kappa$; $l, \alpha_i, \beta_j \in \mathbb{Z}$; и $[\widetilde{\sigma}_i, \widetilde{\sigma}_j] = \zeta^l \prod_{s \neq 1} \widetilde{\sigma}_s^{\varepsilon_s} \iff [\overline{\sigma}_i, \overline{\sigma}_j] = \zeta^l \prod_{s \neq 1} \overline{\sigma}_s^{\varepsilon_s}$ for $i, j = 1, 2, \ldots, \kappa; l, \varepsilon_s \in \mathbb{Z}$.

Сега ще докажем следния резултат, даващ ни връзката между препятствията на задачите зададени с груповите разширения (2.4) и (2.5).

Теорема 2.2.4. ([Mi5, Theorem 2.7]) *Нека L/k е крайно разширение на Галоа с група на Галоа $G = \mathrm{Gal}(L/k)$ според описанието по-горе, нека $K = L^H$ е неподвижното подполе на H, и нека групите G_1 и G_2 от (2.4) и (2.5) са такива, че $G_2 = G_1^{(p^n, \sigma_1)}$. Да означим с $O_{G_1} \in \mathrm{Br}_p(k)$ – препятствието на задачата за вложимост $(L/k, G_1, \mu_p)$, с $O_{G_2} \in \mathrm{Br}_p(k)$ – препятствието на задачата за вложимост $(L/k, G_2, \mu_p)$, и с $O_{C_{p^n}} \in \mathrm{Br}_p(k)$ – препятствието на задачата за вложимост $(K/k, C_{p^n}, \mu_p)$ зададена с груповото разширение*

$$1 \longrightarrow \mu_p \longrightarrow C_{p^n} \longrightarrow G/H \cong C_{p^{n-1}} \longrightarrow 1.$$

Тогава връзката между тези препятствия се дава чрез следното равенство:

$$O_{G_2} = O_{G_1} O_{C_{p^n}} \in \mathrm{Br}_p(k).$$

Доказателство: Да означим с $\Gamma_1 = (L, G, f_1)$ кръстосаното произведение съответстващо на препятствието O_{G_1}, и с $\Gamma_2 = (L, G, f_2)$ ръстосаното произведение съответстващо на препятствието O_{G_2}. Както отбелязахме след теорема 2.1.1, Γ_1 се поражда над k от елементите на L и $\{u_\sigma\}_{\sigma\in G}$, където $u_1 = f_1(1,1) = 1, u_\sigma x = \sigma x u_\sigma$ и $u_\sigma u_\tau = u_{\sigma\tau} f_1(\sigma, \tau)$. Да отбележим, че структурата на G_1 определя структурата на Γ_1, така например ако $[\widetilde{\sigma}_i, \widetilde{\sigma}_j] = \zeta\widetilde{\sigma}_s$ то $[u_{\sigma_i}, u_{\sigma_j}] = \zeta u_{\sigma_s}$. Цикличната алгебра A породена от елементите на K и елементите $u^i_{\sigma_1} = u_{\sigma_1^i}, i = 1, \ldots, p^{n-1}$, се съдържа в Γ_1 и $u^{p^{n-1}}_{\sigma_1} = u_1 = 1$. Тогава $\Gamma_1 = A \otimes_k C_{\Gamma_1}(A)$. Ще покажем, че u_{σ_1} и неговите степени не участват в произведенията, които пораждат централизатора $C_{\Gamma_1}(A)$.

Да отбележим първо, че всеки елемент на G се записва по единствен начин във вида $\sigma_1^i\sigma$, където $\sigma \in H = \langle\sigma_2, \ldots, \sigma_\kappa\rangle$ и $i = 1, \ldots, p^{n-1}$. Тогава $u_{\sigma_1^i\sigma} = u_{\sigma_1^i} u_\sigma f_1^{-1}(\sigma_1^i, \sigma)$, така че за произволен елемент $\alpha \in C_{\Gamma_1}(A)$ можем да напишем

$$\alpha = \sum_{\sigma\in H, i} x_{\sigma,i} u_{\sigma_1^i\sigma} = \sum_{\sigma\in H, i} y_{\sigma,i} u^i_{\sigma_1} u_\sigma,$$

където $x_{\sigma,i} \in L^*$ и $y_{\sigma,i} = x_{\sigma,i} f_1^{-1}(\sigma_1^i, \sigma) \in L^*$. Да предположим, че $y_{\sigma,i} \neq 0$ за някое i, което е взаимно просто с p. Тъй като K съдържа елемент от вида $\sqrt[p]{a}$ за $a \in k^* \setminus k^{*p}$, така че $\sigma_1\sqrt[p]{a} = \sqrt[p]{a}\zeta$, имаме следните равенства: $u^i_{\sigma_1}\sqrt[p]{a} = \sigma_1^i\sqrt[p]{a}u^i_{\sigma_1} = \sqrt[p]{a}\zeta^i u^i_{\sigma_1}$ и $u^j_{\sigma_1}\sqrt[p]{a} = \sqrt[p]{a}u^j_{\sigma_1}$ за всяко j такова, че p дели j. Отчитайки, че $\sigma\sqrt[p]{a} = \sqrt[p]{a}$ за всяко $\sigma \in H$, получаваме

$$\alpha\sqrt[p]{a} = \sqrt[p]{a}\left(\sum_{(i,p)=1} y_{\sigma,i}\zeta^i u^i_{\sigma_1} u_\sigma + \sum_{p|i} y_{\sigma,i} u^i_{\sigma_1} u_\sigma\right) = \sqrt[p]{a}\alpha,$$

където $\zeta^i \neq 1$ за i такова, че $(i,p) = 1$. Така достигаме до противоречие с линейната независимост на елементите $\{u_\sigma\}_{\sigma\in G}$. Нека сега да допуснем, че всяка участваща степен на u_{σ_1} се дели на p, откъдето можем да приемем, че α има вида

$$\alpha = \sum_{j>0, \sigma\in H} y_{\sigma,j} u^{p^j k_j}_{\sigma_1} u_\sigma,$$

където $(p, k_j) = 1$. Нека j_0 е най-малкото число такова, че $y_{\sigma_0,j_0} \neq 0$ за някое $\sigma_0 \in H$. Груповите разширения

$$1 \longrightarrow C_p \longrightarrow C_{p^j} \longrightarrow C_{p^{j-1}} \longrightarrow 1$$

$(j = 2, \ldots, n-1)$ дават следното свойство на цикличните разширения, което прилагаме за j_0: съществува $\sqrt[p]{\omega} \in K$, така че $\sigma_1^{p^{j_0}k_{j_0}}\sqrt[p]{\omega} = \sqrt[p]{\omega}\zeta$ и $\sigma_1^{p^j k_j}\sqrt[p]{\omega} = \sqrt[p]{\omega}$ за всяко

$j > j_0$. За простота можем да считаме, че останалите елементи y_{σ,j_0} в сумата са 0. Тогава от

$$\alpha\sqrt[p]{\omega} = \sqrt[p]{\omega}\left(y_{\sigma_0,j_0}\zeta u_{\sigma_1}^{p^{j_0}k_{j_0}}u_\sigma + \sum_{j>j_0,\sigma\in H} y_{\sigma,j}u_{\sigma_1}^{p^j k_j}u_\sigma\right) = \sqrt[p]{\omega}\alpha$$

отново достигаме до противоречие. Следователно, всеки елемент $\alpha \in C_{\Gamma_1}(A)$ наистина е от вида: $\sum_{\sigma\in H} x_\sigma u_\sigma$, където $x_\sigma \in L$.

По-нататък, Γ_2 се поражда над k от елементите на L и $\{v_\sigma\}_{\sigma\in G}$, където $v_1 = f_2(1,1) = 1, v_\sigma x = \sigma x v_\sigma$ и $v_\sigma v_\tau = v_{\sigma\tau}f_2(\sigma,\tau)$. Цикличната алгебра B породена от елементите на K и елементите $v_{\sigma_1}^i = v_{\sigma_1^i}, i = 1,\ldots,p^{n-1}-1$, се съдържа в Γ_2. Тук обаче, $v_{\sigma_1}^{p^{n-1}} = \zeta^l$, където $\overline{\sigma}_1^{p^{n-1}} = \zeta^l$. Тогава аналогично с Γ_1, имаме $\Gamma_2 = B \otimes_k C_{\Gamma_2}(B)$, където v_{σ_1} и неговите степени не участват в произведенията, които пораждат централизатора $C_{\Gamma_2}(B)$. Да дефенираме изображение $\theta : \Gamma_1 \to \Gamma_2$ чрез $x \mapsto x$ и $u_\sigma \mapsto v_\sigma$ за всяко $x \in L$ всяко $\sigma \in G$. От полученото за структурата на централизатора следва, че θ изобразява $C_{\Gamma_1}(A)$ върху $C_{\Gamma_2}(B)$ и че рестрикцията $\theta : C_{\Gamma_1}(A) \to C_{\Gamma_2}(B)$ е изоморфизъм.

Остава да се съобрази, че алгебрата A се разпада. Оттук $O_{G_1} = [\Gamma_1] = [A][C_{\Gamma_1}(A)] = [C_{\Gamma_1}(A)]$. Накрая, $[B] = O_{C_{p^n}}$, така че $O_{G_2} = [B][C_{\Gamma_2}(B)] = O_{C_{p^n}}O_{G_1}$. □

Пример 2.2.5. Нека $G = D_{2^{n-1}}$ – диедралната група от ред 2^{n-1} породена от два елемента σ_1 и σ_2 със съотношенията $\sigma_1^2 = 1, \sigma_2^{2^{n-2}} = 1$ и $[\sigma_1,\sigma_2] = \sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2 = \sigma_2^2$; $G_1 = D_{2^n}$ – диедралната група от ред 2^n породена от $\widetilde{\sigma}_1$ и $\widetilde{\sigma}_2$ със съотношенията $\widetilde{\sigma}_1^2 = 1, \widetilde{\sigma}_2^{2^{n-2}} = -1$ и $[\widetilde{\sigma}_1,\widetilde{\sigma}_2] = \widetilde{\sigma}_2^2$; и $G_2 = Q_{2^n}$ – кватернионната група от ред 2^n породена от $\overline{\sigma}_1$ и $\overline{\sigma}_2$ със съотношенията $\overline{\sigma}_1^2 = \overline{\sigma}_2^{2^{n-2}} = -1$ и $[\overline{\sigma}_1,\overline{\sigma}_2] = \overline{\sigma}_2^2$. Лесно се вижда сега, че $Q_{2^n} = D_{2^n}^{(4,\sigma_1)}$.

Нека сега $L = K(\sqrt{b})/k$ е $D_{2^{n-1}}$ разширение такова, че $\sigma_2\sqrt{b} = \sqrt{b}$ и $\sigma_1\sqrt{b} = -\sqrt{b}$. Задачата за вложимост $(k(\sqrt{b})/k, C_4, \mu_2)$ има препятствие $(b,-1)$, както е добре известно. Тогава според теорема 2.2.4 е в сила следната връзка между препятствията на задачите $(L/k, D_{2^n}, \mu_2)$ и $(L/k, Q_{2^n}, \mu_2)$: $O_{Q_{2^n}} = O_{D_{2^n}}(b,-1)$. □

В следващите два параграфа ще изложим още два метода за решаване на задачи за вложимост с циклично ядро от ред 2 - квадратичната корестрикция и ортогоналните представяния.

2.3 Хомоморфизъм на квадратичната корестрикция. Лема на Шапиро

В този параграф ще разгледаме лемата на Шапиро в следнака конкретна ситуация: нека G е про-крайна 2-група, нека H е затворена подгрупа с индекс $(G : H) = 2$, и нека $\mu_2 = \{\pm 1\}$ е тривиален H-модул.

Определение 2.3.1. [Se1, Ch. I, §2.5] Нека A е H-модул. Дефинираме *индуциран* модул (*коиндуциран* в означенията на [Se2]) $A^* = M_G^H(A)$ като множеството на всички непрекъснати изображения $a^* : G \to A$ такива, че $a^*(hx) = ha^*(x)$, където $h \in H$ и $x \in G$. Можем да дадем G-модулна структура на A^* чрез $(ga^*)(x) = a^*(xg)$ за всяко $g \in G$.

В нашата ситуация можем лесно да дадем явно описание на модула μ_2^*: Избираме елемент $g \in G$ такъв, че $g \notin H$, т.е. H и Hg са двата десни съседни класа на H в G. Дефиницията ни дава, че $a^*(h) = a^*(1)$ и $a^*(hg) = a^*(g)$ за всяко $h \in H$. Следователно, μ_2^* е елементарната абелова група от ред 4, която ще записваме мултипликативно. Ще означаваме елементите на μ_2^* по този начин: $a_1^* = (1,1), a_2^* = (1,-1), a_3^* = (-1,1)$ и $a_4^* = (-1,-1)$, където a_1^* изобразява G в 1; a_2^* изобразява H в 1 и Hg в -1; a_3^* изобразява H в -1 и Hg в 1; a_4^* изобразява G в -1. Действието на G върху μ_2^* тогава се задава чрез $ha^* = a^*$ за всяко $h \in H$ и $a^* \in \mu_2^*$; $ga_1^* = a_1^*, ga_2^* = a_3^*, ga_3^* = a_2^*$ и $ga_4^* = a_4^*$.

Нека сега да дефинираме изображение $\varphi : \mu_2^* \to \mu_2$ чрез $\varphi(a^*) = a^*(1)$. Очевидно, φ е епиморфизъм, който е съвместим с естественото включване на H в G. По-нататък, $\ker(\varphi) = \{a_1^*, a_2^*\}$ и φ индуцира хомоморфизъм $H^2(G, \mu_2^*) \to H^2(H, \mu_2)$. Този хомоморфизъм се явява изоморфизъм според лемата на Шапиро [Se1, Ch. I, Prop. 10]. Следвайки отново [Se1], дефинираме изображение $\pi : \mu_2^* \to \mu_2$ чрез

$$\pi(a^*) = \prod_{x \in G/H} xa^*(x^{-1}),$$

където трябва да отбележим, че под $xa^*(x^{-1})$ се разбира действието на x върху $a^*(x^{-1}) \in \mu_2$. Тъй като μ_2 е тривиален G-модул, имаме, че $\pi(a^*) = a^*(1)a^*(g)$. Изображението π е коректно дефинирано и се явява G-епиморфизъм, който индуцира хомоморфизма на *корестрикция* (*трансфер*):

$$\mathrm{cor}_{G/H} : H^q(H, \mu_2) \cong H^q(G, \mu_2^*) \longrightarrow H^q(G, \mu_2), \tag{2.6}$$

където лявото изображение е изоморфизма (който занапред ще наричаме накратко *изоморфизма на Шапиро*) дефиниран в доказателството на лемата на Шапиро в [Se1]. Да забележим също, че $\ker(\pi) = \{a_1^*, a_4^*\}$ е тривиален G-модул.

Да разгледаме следната конкретна ситуация: Нека $\mathcal{G}$ е про-крайна 2-група и нека E_4 е затворена нормална подгрупа на $\mathcal{G}$, изоморфна на елементарната абелова група от ред 4 с пораждащи σ и τ. Нека да съществува затворена подгрупа $\mathcal{H}$ в $\mathcal{G}$ такава, че E_4 е нормална подгрупа в $\mathcal{H}$, още $\mathcal{H}$ се съдържа в централизатора $C_{\mathcal{G}}(E_4)$ на E_4 в $\mathcal{G}$, и индекса на $\mathcal{H}$ в $\mathcal{G}$ е 2. По-нататък, да изберем и фиксираме $g_1 \in \mathcal{G} \setminus \mathcal{H}$, и да приемем, че $g_1 \sigma g_1^{-1} = \sigma$ и $g_1 \tau g_1^{-1} = \sigma\tau$. Тогава за $H = \mathcal{H}/E_4$ и $G = \mathcal{G}/E_4$ имаме изоморфизма $G/H \cong \mathcal{G}/\mathcal{H}$. Накрая, да изберем и да фиксираме $g \in G \setminus H$, така че да имаме G-действие на E_4, зададено чрез $c^h = c$ за всяко $c \in E_4$ и $h \in H$; $\sigma^g = \sigma$ и $\tau^g = \sigma\tau$. В тези означения е в сила

Лема 2.3.2. ([Mi5, Lemma 3.2]) *Нека $\varphi_1, \varphi_2 \in \mathrm{Hom}_H(E_4, \mu_2)$ са такива, че $\ker(\varphi_1) = \{1, \tau\}$ и $\ker(\varphi_2) = \{1, \sigma\tau\}$. Тогава φ_1 и φ_2 индуцират съответно хомоморфизмите $\varphi_1'', \varphi_2'' : H^2(H, E_4) \longrightarrow H^2(H, \mu_2)$ такива, че композициите*

$$\psi_i : H^2(G, E_4) \xrightarrow{\text{res}} H^2(H, E_4) \xrightarrow{\varphi_i''} H^2(H, \mu_2)$$

са изоморфизми за $i = 1, 2$.

Доказателство: Можем да дефинираме G-изоморфизъм $E_4 \cong \mu_2^*$ чрез $\sigma \mapsto a_4^*, \tau \mapsto a_2^*, \sigma\tau \mapsto a_3^*$. По този начин, можем да приемем, че хомоморфизмите зададени в условието, са в $\mathrm{Hom}_H(\mu_2^*, \mu_2)$, и имат ядра $\ker(\varphi_1) = \{a_1^*, a_2^*\}$ и $\ker(\varphi_2) = \{a_1^*, a_3^*\}$. Тогава за произволен G-модул B, хомоморфизмите φ_i индуцират хомоморфизми $\varphi_i' : \mathrm{Hom}_H(B, \mu_2^*) \to \mathrm{Hom}_H(B, \mu_2)$ за $i = 1, 2$. Включването $H \hookrightarrow G$ ни дава композицията

$$\theta_1 : \mathrm{Hom}_G(B, \mu_2^*) \xrightarrow{\text{res}} \mathrm{Hom}_H(B, \mu_2^*) \xrightarrow{\varphi_1'} \mathrm{Hom}_H(B, \mu_2),$$

където $\theta_1(f)(b) = f(b)(1)$ за $f \in \mathrm{Hom}_G(B, \mu_2^*)$ и $b \in B$. Според [Se1], θ_1 е изоморфизъм, който индуцира изоморфизма на Шапиро. Тъй като два кохомологични функтора, които са идентични в нулевата степен трябва да са идентични на всякъде, получаваме, че ψ_1 е изоморфизъм.

Нека сега да дефинираме изображение $\xi : \mu_2^* \to \mu_2^*$ чрез $a_1^* \mapsto a_1^*, a_2^* \mapsto a_3^*, a_3^* \mapsto a_2^*$ и $a_4^* \mapsto a_4^*$. Очевидно, ξ е G-автоморфизъм на μ_2^*, който индуцира автоморфизъм $\xi' : \mathrm{Hom}_G(B, \mu_2^*) \to \mathrm{Hom}_G(B, \mu_2^*)$. Тогава за композицията

$$\theta_2 : \mathrm{Hom}_G(B, \mu_2^*) \xrightarrow{\text{res}} \mathrm{Hom}_H(B, \mu_2^*) \xrightarrow{\varphi_2'} \mathrm{Hom}_H(B, \mu_2)$$

ще имаме, че $\theta_2 = \theta_1\xi'$. Следователно θ_2 и ψ_2 също са изоморфизми. $\square$

Запазвайки означенията от лема 2.3.2, ще докажем следната

Теорема 2.3.3. ([Mi5, Theorem 3.3]) *Нека L/k е крайно разширение на Галоа с група на Галоа G и нека $K = L^H$ е неподвижното подполе на H. Тогава задачата за вложимост $(L/k, \mathcal{G}, E_4)$ е слабо разрешима тогава и само тогава, когато задачата за вложимост $(L/K, \mathcal{H}/\langle\tau\rangle, E_4/\langle\tau\rangle)$ е слабо разрешима.*

Доказателство: 'Необходимост'. Задачата за вложимост $(L/K, \mathcal{H}/\langle\tau\rangle, E_4/\langle\tau\rangle)$ може да се достигне като първо образуваме съпътстващата задача от втори тип $(L/K, \mathcal{H}, E_4)$ и след това съпътстващата задача от първи тип $(L/K, \mathcal{H}/\langle\tau\rangle, E_4/\langle\tau\rangle)$. Да припомним, че слабата решимост на първоначалната задача за вложимост $(L/k, \mathcal{G}, E_4)$ влече слабата решимост на съпътстващите задачи за вложимост.

'Достатъчност'. Нека φ_i и ψ_i $(i = 1, 2)$ са дефинираните в лема 2.3.2 хомоморфизми. Ако разгледаме групите на Галоа Ω_k и Ω_K на сепарабелната обвивка k_s над k и K, съответно, хомоморфизмите φ_i индуцират също хомоморфизми $\overline{\psi}_i : H^2(\Omega_k, E_4) \to H^2(\Omega_K, \mu_2)$. За така зададените ψ_i и $\overline{\psi}_i$ имаме следните комутативни диаграми:

$$\begin{array}{ccc} H^2(G, E_4) & \xrightarrow{\psi_i} & H^2(H, \mu_2) \\ \downarrow \inf_G^{\Omega_k} & & \downarrow \inf_H^{\Omega_K} \\ H^2(\Omega_k, E_4) & \xrightarrow{\overline{\psi}_i} & H^2(\Omega_K, \mu_2) \end{array}$$

$(i = 1, 2)$.

Нека сега да предположим, че задачата за вложимост $(L/K, \mathcal{H}/\langle\tau\rangle, E_4/\langle\tau\rangle)$ е слабо разрешима и да означим с c 2-кокласа на груповото разширение

$$1 \longrightarrow E_4 \longrightarrow \mathcal{G} \longrightarrow G \longrightarrow 1$$

в $H^2(G, E_4)$. Тъй като 2-кокласът $\psi_1(c)$ се представя от груповото разширение

$$1 \longrightarrow E_4/\langle\tau\rangle \longrightarrow \mathcal{H}/\langle\tau\rangle \longrightarrow H \longrightarrow 1,$$

имаме, че $\inf_H^{\Omega_K}(\psi_1(c)) = 0$. Комутативната диаграма за $i = 1$ тогава показва, че $\overline{\psi}_1 \inf_G^{\Omega_k}(c) = 0$. Тъй като $\overline{\psi}_1$ е изоморфизъм, то $\inf_G^{\Omega_k}(c) = 0$, откъдето задачата за вложимост $(L/k, \mathcal{G}, E_4)$ е слабо разрешима. $\square$

Както лема 2.3.2 показва, няма значение дали ще изберем τ или $\sigma\tau$ в условието на теорема 2.3.3. В тази връзка, условието за съгласуваност се свежда до проверката само на една Брауерова задача за вложимост.

Известно е, че за да бъде една слабо разрешима задача $(E/k, Y, X)$ подходящо разрешима е достатъчно ядрото X да се съдържа в подгрупата на Фратини $\Phi(Y)$ на Y (виж [ИЛФ, §1.6, Следствие 5]). Следните свойства на подгрупата на Фратини ни дават едно достатъчно условие ядрото X да се съдържа във $\Phi(Y)$.

Лема 2.3.4. ([Be, Cor. 5.3.2]) *Нека X и Y са крайни групи, нека X е нормална в Y и нека $X \leq \Phi(Y)$. Тогава $\Phi(Y)/X = \Phi(Y/X)$.*

Лема 2.3.5. ([Be, Ex. 5.3.8]) *Нека X и Y са крайни p-групи и $X \leq Y$. Тогава $\Phi(X) \leq \Phi(Y)$.*

Лема 2.3.6. ([ИЛФ, Предложение 4.1.2]) *Нека $1 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 1$ е крайно p-групово разширение и нека $X_0 = X \cap \Phi(Y)$. Тогава груповото разширение $1 \longrightarrow X/X_0 \longrightarrow Y/Y_0 \longrightarrow Z \longrightarrow 1$ е разцепимо.*

Теорема 2.3.7. ([Mi5, Proposition 3.7]) *В означенията на лема 2.3.2, нека $\mathcal{G}$ е крайна 2-група и нека груповите разширения $1 \longrightarrow E_4/\langle\rho\rangle \longrightarrow \mathcal{H}/\langle\rho\rangle \longrightarrow H \longrightarrow 1$ са неразцепими за всяко $\rho \in E_4$. Тогава $E_4 \leq \Phi(\mathcal{G})$.*

Доказателство: Да допуснем, че E_4 не се съдържа във $\Phi(\mathcal{H})$. Тогава групата $E_0 = E_4 \cap \Phi(\mathcal{H})$ има ред ≤ 2, така че груповото разширение $1 \longrightarrow E_4/E_0 \longrightarrow \mathcal{H}/E_0 \longrightarrow H \longrightarrow 1$ е разцепимо според лема 2.3.6, което е противоречие. Оттук $E_4 \leq \Phi(\mathcal{H}) \leq \Phi(\mathcal{G})$, според лема 2.3.5. □

Запазвайки означенията дадени непосредствено преди лема 2.3.2, ние сме готови да докажем основния резултат на този параграф.

Теорема 2.3.8. ([Mi5, Theorem 3.8]) *Нека $c_1 \in H^2(G, \mu_2)$ е 2-кокласът, съответстващ на груповото разширение $1 \longrightarrow E_4/\langle\sigma\rangle \cong \mu_2 \longrightarrow \mathcal{G}/\langle\sigma\rangle \longrightarrow G \longrightarrow 1$, нека $c_2 \in H^2(H, \mu_2)$ е 2-кокласът, съответстващ на груповото разширение $1 \longrightarrow E_4/\langle\tau\rangle \cong \mu_2 \longrightarrow \mathcal{H}/\langle\tau\rangle \longrightarrow H \longrightarrow 1$, и нека $c_3 \in H^2(H, \mu_2)$ е 2-кокласът, съответстващ на груповото разширение $1 \longrightarrow E_4/\langle\sigma\tau\rangle \cong \mu_2 \longrightarrow \mathcal{H}/\langle\sigma\tau\rangle \longrightarrow H \longrightarrow 1$. Тогава $\mathrm{cor}_{G/H}(c_2) = \mathrm{cor}_{G/H}(c_3) = c_1$.*

Доказателство: Да припомним, че хомоморфизмът $\pi : \mu_2^* \to \mu_2$, зададен чрез $\pi(a^*) = a^*(1)a^*(g)$ индуцира хомоморфизма на корестрикция (виж (2.6)):

$$\mathrm{cor}_{G/H} : H^2(H, \mu_2) \longrightarrow H^2(G, \mu_2^*) \xrightarrow{\pi'} H^2(G, \mu_2),$$

където лявото изображение е изоморфизма на Шапиро, а дясното е индуцирано от π. Да въведем следните означения: нека $c \in H^2(G, E_4)$ е 2-кокласът, съответстващ на груповото разширение $1 \longrightarrow E_4 \longrightarrow \mathcal{G} \longrightarrow G \longrightarrow 1$, нека $\xi_1 : E_4 \to \mu_2^*$ е G-изоморфизъм, дефиниран чрез $\xi_1(\sigma) = a_4^*, \xi_1(\tau) = a_2^*, \xi_1(\sigma\tau) = a_3^*$ и нека $\xi_1' : H^2(G, E_4) \to H^2(G, \mu_2^*)$ е индуцирания изоморфизъм. По същия начин, нека $\xi_2 : E_4 \to \mu_2^*$ е G-изоморфизъм, дефиниран чрез $\xi_2(\sigma) = a_4^*, \xi_2(\tau) = a_3^*, \xi_2(\sigma\tau) = a_2^*$ и нека $\xi_2' : H^2(G, E_4) \to H^2(G, \mu_2^*)$ е индуцирания изоморфизъм.

От лема 2.3.2 сега следва, че $c_2 = \psi_1(c)$, където ψ_1 е изоморфизъм. По-нататък, $c_1 = \pi'\xi_1'(c)$ и $c_1 = \pi'\xi_1'\psi_1^{-1}(c_2)$, където $\xi_1'\psi_1^{-1}$ е точно изоморфизма на Шапиро. Аналогично, имаме $c_3 = \psi_2(c)$ и $c_1 = \pi'\xi_2'(c)$, понеже $\pi(a_2^*) = \pi(a_3^*) = -1$. Следователно $c_1 = \pi'\xi_2'\psi_2^{-1}(c_3)$. Дефинициите на ψ_1 и ψ_2 в лема 2.3.2 показват, че имаме комутативната диаграма:

$$\begin{array}{ccc} H^2(G, E_4) & \xrightarrow{\psi_1} & H^2(H, \mu_2) \\ \uparrow{\scriptstyle \xi_1'^{-1}} & & \uparrow{\scriptstyle \psi_2} \\ H^2(G, \mu_2^*) & \xrightarrow{\xi_2'^{-1}} & H^2(G, E_4) \end{array}$$

откъдето получаваме $\xi_1'\psi_1^{-1} = \xi_2'\psi_2^{-1}$ – изоморфизма на Шапиро. Следователно, $c_1 = \mathrm{cor}_{G/H}(c_2) = \mathrm{cor}_{G/H}(c_3)$. □

Хомоморфизмът на корестрикция приема множество форми. Ще изложим и една класическа формула на Тейт [Та], която ни дава възможност за явни пресмятания. Нека G е крайна група, и нека H е собствена подгрупа на G. Разлагаме G на съседни класове ρ по отношение на H: $G = \cup_\rho \rho = \cup_\rho H\overline{\rho}$ с дадена дясна трансверзала $R = \{\overline{\rho}\}$. Нека A е тривиален H-модул и да изберем 2-коцикъл $\overline{f} \in Z^2(H, A)$, съответстващ на дадено групово разширение

$$1 \longrightarrow A \longrightarrow G_0 \underset{\varphi}{\longrightarrow} H \longrightarrow 1.$$

Теорема 2.3.9. *В горните означения, хомоморфизмът на корестрикция* $\mathrm{cor}_{G/H}$: $H^2(H,A) \to H^2(G,A)$ *се задава със следната явна формула:*

$$\mathrm{cor}_{G/H}\overline{f}(g_1,g_2) = \prod_{\overline{\rho}\in R} \overline{f}(r_0 g_1 r_1^{-1}, r_1 g_2 r_2^{-1}),$$

където r_0, r_1 *и* r_2 *се дефинират така:* $r_0 = \overline{\rho}, r_1 \in Hr_0g_1$ *и* $r_2 \in Hr_1g_2$.

Доказателство: Първо, да припомним дефиницията на *обобщеното сплитане*, дадена в [ИЛФ, §3.7]. Нека $\widetilde{G}$ е множеството от наредени двойки (g,ψ_g), където $g \in G$ и ψ_g са функции дефинирани върху съседните класове ρ със стойности в групата G_0. Нека стойностите на ψ_g удовлетворяват условието $\varphi(\psi_g(\rho)) = \overline{\rho g^{-1}} g \overline{\rho}^{-1}$. По-нататък, да дефинираме действие на G върху ψ_g чрез $\psi_g^{g_1}(\rho) = \psi_g(\rho g_1^{-1})$. Сега можем да превърнем $\widetilde{G}$ в група чрез следното мултипликативно правило:

$$(g_1,\psi_{g_1})(g_2,\psi_{g_2}) = (g_1g_2, \psi_{g_1}^{g_2}\psi_{g_2}).$$

Изображението $\widetilde{\varphi}$, което праща (g,ψ_g) в $g \in G$ е епиморфизъм с ядро

$$\widetilde{A} = \ker\widetilde{\varphi} = \{(1,\psi_1) \mid \psi_1(\rho) \in A\}.$$

По този начин, получаваме груповото разширение

$$1 \longrightarrow \widetilde{A} \longrightarrow \widetilde{G} \underset{\widetilde{\varphi}}{\longrightarrow} G \longrightarrow 1,$$

където $\widetilde{A}$ е абелова и нейния ред е $|A|^{(G:H)}$. Следователно, можем да асоциираме с горното групово разширение определен 2-коклас $\widetilde{f} \in Z^2(G,\widetilde{A})$.

От друга страна, $\widetilde{A}$ съвпада с индуцирания G-модул $M_G^H(A)$. Според [Se1, §2.5], имаме изоморфизма $H^2(G,\widetilde{A}) \cong H^2(H,A)$ зададен чрез $[\widetilde{f}] \mapsto [\overline{f}]$.

Можем да дефинираме изображение $\pi : \widetilde{A} \to A$ чрез $\pi(1,\psi_1) = \prod_\rho \psi_1(\rho)$. Тогава π е G-епиморфизъм, който индуцира груповото разширение

$$1 \longrightarrow A \cong \widetilde{A}/\ker\pi \longrightarrow G_1 \cong \widetilde{G}/\ker\pi \underset{\widetilde{\varphi}}{\longrightarrow} G \longrightarrow 1.$$

Ако означим с f 2-коцикъла от $Z^2(G,A)$ съответстващ на горното групово разширение, то $[f] = \mathrm{cor}_{G/H}[\overline{f}]$, според [Se1].

Да означим с $[g,\psi_g]$ класа $(g,\psi_g)/\ker\pi$ в G_1, и да положим $v_g = [g,\psi_g]$ за $g \in G$. Така, $\{v_g\}$ е система от представители за $f = \mathrm{cor}_{G/H}\overline{f}$:

$$\begin{aligned} f(g_1,g_2) &= v_{g_1}v_{g_2}v_{g_1g_2}^{-1} = [g_1,\psi_{g_1}][g_2,\psi_{g_2}][g_1g_2,\psi_{g_1g_2}]^{-1} \\ &= [1, \psi_{g_1}^{g_1^{-1}}\psi_{g_2}^{g_2^{-1}g_1^{-1}}\psi_{g_2^{-1}g_1^{-1}}]. \end{aligned}$$

Нататък, да изберем система от представители $\{u_h\}_{h\in H}$ за $\overline{f}$, т.е. $\overline{f}(h_1,h_2) = u_{h_1}u_{h_2}u_{h_1h_2}^{-1}$. Вземайки образите под действието на φ, получаваме съотношенията:

$$\begin{aligned}
\psi_{g_1}^{g_1^{-1}}(\rho) &= u_{\overline{\rho}g_1\overline{\rho g_1}^{-1}}a_{g_1}(\rho),\\
\psi_{g_2}^{g_2^{-1}g_1^{-1}}(\rho) &= u_{\overline{\rho g_1}g_2\overline{\rho g_1 g_2}^{-1}}a_{g_2}(\rho g_1),\ \text{и}\\
\psi_{g_2^{-1}g_1^{-1}}(\rho) &= u^{-1}_{\overline{\rho}g_1g_2\overline{\rho g_1 g_2}^{-1}}a^{-1}_{g_1g_2}(\rho g_2^{-1}g_1^{-1}),
\end{aligned}$$

където $a_g(\rho)\in A$. Полагаме $a_g = \prod_\rho a_g(\rho)$. Тогава

$$\begin{aligned}
&[1, \psi_{g_1}^{g_1^{-1}}\psi_{g_2}^{g_2^{-1}g_1^{-1}}\psi_{g_2^{-1}g_1^{-1}}]\\
&= \prod_\rho \psi_{g_1}^{g_1^{-1}}\psi_{g_2}^{g_2^{-1}g_1^{-1}}\psi_{g_2^{-1}g_1^{-1}}(\rho)\\
&= \prod_\rho u_{\overline{\rho}g_1\overline{\rho g_1}^{-1}}u_{\overline{\rho g_1}g_2\overline{\rho g_1 g_2}^{-1}}u^{-1}_{\overline{\rho}g_1g_2\overline{\rho g_1 g_2}^{-1}}a_{g_1}(\rho)a_{g_2}(\rho g_1)a^{-1}_{g_1g_2}(\rho g_2^{-1}g_1^{-1})\\
&= a_{g_1}a_{g_2}a^{-1}_{g_1g_2}\cdot\prod_\rho \overline{f}(\overline{\rho}g_1\overline{\rho g_1}^{-1}, \overline{\rho g_1}g_2\overline{\rho g_1 g_2}^{-1}).
\end{aligned}$$

□

Ще предполагаме оттук до края на този параграф, че полето k има характеристика различна от 2, $a\in k^*\setminus k^{*2}$, $K = k(\sqrt{a})$ и $\mathrm{Gal}(K/k) = \langle\sigma\rangle \cong C_2$. Тъй като $\mathrm{Br}_2(k)\cong H^2(\Omega_k,\mu_2)$, имаме хомоморфизма на корестрикция $\mathrm{cor}_{\Omega_k/\Omega_K}:\mathrm{Br}_2(K)\to\mathrm{Br}_2(k)$. За $b\in k^*$ и $\alpha\in K$, проекционната формула гласи, че $\mathrm{cor}_{\Omega_k/\Omega_K}(\alpha,b)_K = (N_{K/k}(\alpha),b)_k$, където $N_{K/k}$ е норменото изображение. Тази формула може да се извлече от упражненията в [Se2, XIV §1,§2].

С помощта на проекционната формула, можем да докажем директно следната лема, която се явява аналог на [ST, Pr. 4].

Лема 2.3.10. *Нека $a\in k^*, K = k(\sqrt{a}), \alpha_0 = a_0 + b_0\sqrt{a}$ и $\alpha_1 = a_1 + b_1\sqrt{a}$ $(a_i,b_i\in k)$. Тогава*

1. *Ако $b_{1-i} = 0$, то $\mathrm{cor}_{\Omega_k/\Omega_K}(\alpha_0,\alpha_1)_K = (a_{1-i}, a_i^2 - ab_i^2)_k$;*

2. *Ако $a_{1-i}b_i - a_ib_{1-i} = 0$, то $\mathrm{cor}_{\Omega_k/\Omega_K}(\alpha_0,\alpha_1)_K = (-a_ia_{1-i}, a_i^2 - ab_i^2)_k$;*

3. *Иначе,*
   $\mathrm{cor}_{\Omega_k/\Omega_K}(\alpha_0,\alpha_1)_K = (a_0^2 - ab_0^2, b_0(a_1b_0 - a_0b_1))_k(a_1^2 - ab_1^2, b_1(a_0b_1 - a_1b_0))_k$.

Доказателство: (1) Следва от проекционната формула.

(2) Имаме $a_1b_0 = a_0b_1$ и $a_i, b_i \neq 0$, така че $a_1/a_0 = b_1/b_0 = x \in k^*$. Следователно, $(\alpha_0, \alpha_1)_K = (\alpha_0, \alpha_0 x)_K = (\alpha_0, -x)_K = (\alpha_0, -a_0a_1)_K$ и остава да се приложи проекционната формула.

(3) Нека $b_1, b_2 \neq 0$. Да положим $\Delta = a_0b_1 - b_0a_1 \neq 0$ и $y = -\Delta b_0/b_1 \neq 0$. Тогава са в сила равенствата: $-\alpha_1 y = \Delta a_1 b_0/b_1 + b_0\Delta\sqrt{a} = \Delta a_1 b_0/b_1 - a_0\Delta + \alpha_0\Delta = -\Delta^2/b_1 + \alpha_0\Delta$, откъдето $b_1\alpha_1 y = \Delta^2 - \alpha_0 b_1\Delta$. Следователно $(\alpha_0 b_1\Delta, -\alpha_1 b_0\Delta)_K = 1 \in \mathrm{Br}_2(K)$, затова $(\alpha_0 b_1\Delta, -b_0\Delta)_K(\alpha_0 b_1\Delta, \alpha_1)_K = 1$ или, еквивалентно, $(\alpha_0, \alpha_1)_K = (\alpha_0 b_1\Delta, -b_0\Delta)_K(\alpha_1, b_1\Delta)_K = (\alpha_0, -b_0\Delta)_K(\alpha_1, b_1\Delta)_K(b_1\Delta, -b_0\Delta)_K$. Тъй като $b_i\Delta \in k^*$, можем отново да приложим проекционната формула за да получим желания резултат. □

Нека R е централна проста K-алгебра, и нека R^σ е пръстена R снабден с усукана структура на K-алгебра зададена чрез $\lambda \cdot a = \sigma(\lambda)a, a \in R^\sigma, \lambda \in K$. Да конструираме сега алгебрата на тензорното произведение $A = R \otimes_K R^\sigma$ и да дефинираме действие $\widetilde{\sigma} : A \to A$ чрез $\widetilde{\sigma}(a \otimes b) = b \otimes a$.

Определение 2.3.11. ([Ri],[Sc]) Корестрикцията на R е k-алгебрата на $\widetilde{\sigma}$ - инвариантите: $\mathrm{cor}_{K/k}(R) = A^{\langle\widetilde{\sigma}\rangle}$.

Ние няма да се спираме на по-сложната обща дефиниция на алгебрата на корестрикция, дадена в [Ri] или [Ti]. Даже в нашия частен случай, обаче, структурата на тази алгебра е трудна за изясняване. Шарлау доказва в [Sc], че каноничното изображение $\psi : K \times \mathrm{cor}_{K/k}(R) \to A$ зададено чрез $(\alpha, x) \mapsto \alpha x$ е k-билинейно, мултипликативно и индуцира каноничен изоморфизъм на K-алгебри $K \otimes_k \mathrm{cor}_{K/k}(R) \cong A$. Оттук виждаме, че $\mathrm{cor}_{K/k}(R)$ е централна проста k-алгебра и $\dim_k \mathrm{cor}_{K/k}(R) = \dim_K A$. За забележим, че $\mathrm{cor}_{K/k}(R)$ не съдържа K, нещо, което може да причини затруднения в някои ситуации. Това, обаче, може да се поправи по следния начин: Дефинираме $S = A \oplus Ae_\sigma$ като k-векторно пространство и да превърнем S в алгебра чрез $e_\sigma^2 = 1, e_\sigma x = \widetilde{\sigma}(x)e_\sigma$ за всяко $x \in A$. Тогава S е централна проста k-алгебра такава, че K се съдържа в S, да речем чрез влагането $\lambda \mapsto \lambda \otimes 1$. Очевидно $\dim_k S = 4\dim_K A = 4\dim_k \mathrm{cor}_{K/k}(R)$. Кватернионната алгебра S_1 породена от $\sqrt{a}$ и e_σ се съдържа в S, откъдето $S = S_1 \otimes_k C_S(S_1)$. Тъй като S_1 се разцепва и $C_S(S_1) \cong \mathrm{cor}_{K/k}(R)$, получаваме, че S е подобна на $\mathrm{cor}_{K/k}(R)$.

Друг полезен резултат, който може лесно да бъде доказан, е че ако R е кватер-

нионна алгебра $(d, e/K)$, то $R^\sigma = (\sigma(d), \sigma(e)/K)$.

Оказва се, че проекционната формула е валидна за хомоморфизма на корестрикция на алгебри, дефиниран току що. Тиньол доказва тази формула в [Ti]. Тъй като в доказателството на лема 2.3.10 използвахме само проекционната формула, в сила е нейния аналог за корестрикция на алгебри.

Нека отново L/k е разширение на Галоа с група на Галоа G, $H < G, (G : H) = 2, H = \mathrm{Gal}(L/K)$ и $\overline{f} \in Z^2(H, \mu_2)$ е 2-коцикълът съответстващ на дадено групово разширение $1 \longrightarrow \mu_2 \longrightarrow H_2 \longrightarrow H \longrightarrow 1$. Да означим $f = \mathrm{cor}(\overline{f})$, т.е. $[f] = \mathrm{cor}_{G/H}([\overline{f}]) \in H^2(G, \mu_2)$, и нека груповото разширение $1 \longrightarrow \mu_2 \longrightarrow \mathcal{G} \longrightarrow G \longrightarrow 1$ се представя чрез f. По този начин получаваме задачите за вложимост $(L/K, H, \mu_2)$ и $(L/k, G, \mu_2)$, които имат препятствия $[L, H, \overline{f}] \in \mathrm{Br}_2(K)$ и $[L, G, f] \in \mathrm{Br}_2(k)$, съответно. Тогава имаме следната

Теорема 2.3.12. ([ST, Proposition 2]) *При горните предположения е в сила формулата* $\mathrm{cor}_{K/k}([L, H, \overline{f}]) = [L, G, f]$.

За да бъде доказана тази теорема е достатъчно да се покаже комутативността на следната диаграма:

$$\begin{array}{ccccc} H^2(H, \mu_2) & \xrightarrow{\inf_H^{\Omega_K}} & H^2(\Omega_K, \mu_2) & = & \mathrm{Br}_2(K) \\ \downarrow{\scriptstyle \mathrm{cor}_{G/H}} & & \downarrow{\scriptstyle \mathrm{cor}_{\Omega_k/\Omega_K}} & & \downarrow{\scriptstyle \mathrm{cor}_{K/k}} \\ H^2(G, \mu_2) & \xrightarrow{\inf_G^{\Omega_k}} & H^2(\Omega_k, \mu_2) & = & \mathrm{Br}_2(k) \end{array}$$

Трябва да отбележим, че комутативността на десния квадрат не е очевидна, за разлика от левия квадрат. За комутативността на десния квадрат не са достатъчни функториалните свойства на функтора H^2. Рием, обаче, доказва в [Ri, Th. 11] този изключително важен резултат с помощта на неабеловите кохомологии.

2.4 Алгебри и групи на Клифорд. Точни редици

Ще започнем с някои предварителни сведения относно ортогоналните представяния. Нека k е поле с характеристика $\neq 2$, нека V е крайномерно k-векторно пространство, и нека (V, q) е квадратично пространство, където q е квадратична форма. Изометриите $(V, q) \mapsto (V, q)$ образуват подгрупа $O(q)$ на $\mathrm{GL}_k(V)$, наречена *ортогоналната група* на q. *Ортогонално представяне* на крайна група G ще наричаме хомоморфизма $\mu : G \to O(q)$ на G в ортогоналната група за някоя квадратична форма q. Отсега нататък, под ортогонално представяне ще разбираме влагане $\mu : G \hookrightarrow O(q)$.

Сега ще припомним дефиницията на *алгебра на Клифорд*.

Определение 2.4.1. В тензорното произведение

$$T(V) = K \oplus V \oplus (V \otimes_k V) \oplus (V \otimes_k V \otimes_k V) \oplus \cdots$$

разглеждаме идеала $I(q)$ породен от всички елементи $\mathbf{v} \otimes \mathbf{v} - q(\mathbf{v})$ за $\mathbf{v} \in V$. Факторалгебрата $C(q) = T(V)/I(q)$ ще наричаме *алгебра на Клифорд* на квадратичната форма q.

Тъй като $I(q) \cap V = 0$, можем да считаме, че V е подпространство на $C(q)$ и $\mathbf{v}^2 = q(\mathbf{v})$ за $\mathbf{v} \in V$. Следователно $\mathbf{uv} + \mathbf{vu} = 2B(\mathbf{u}, \mathbf{v})$ за $\mathbf{u}, \mathbf{v} \in V, B$ – билинейната форма асоциирана с q. Също, ако запишем

$$T(V) = T_0(V) \oplus T_1(V),$$

където

$$T_0(V) = K \oplus (V \otimes_k V) \oplus (V \otimes_k V \otimes_k V \otimes_k V) \oplus \cdots$$

и

$$T_1(V) = V \oplus (V \otimes_k V \otimes_k V) \oplus \cdots$$

ще имаме, че

$$I(q) = (I(q) \cap T_0(V)) \oplus (I(q) \cap T_1(V)).$$

Оттук получаваме

$$C(q) = C_0(q) \oplus C_1(q),$$

където

$$C_i(q) = (T_i(V) + I(q))/I(q).$$

$C_0(q)$ е подалгебра на $C(q)$, която се нарича четна алгебра на Клифорд. Ако $x \in C_i(q)$, ще записваме $\partial x = i$.

Ако $\mathbf{v}_1, \ldots, \mathbf{v}_n$ е ортогонален базис на V, то елементите $\mathbf{v}_1^{\epsilon_1} \cdots \mathbf{v}_n^{\epsilon_n}$ за $\epsilon_i = 0, 1$ образуват базис на $C(q)$ като k-векторно пространство. Правилата за умножение се задават чрез равенствата: $\mathbf{v}_i^2 = q(\mathbf{v}_i)$ и $\mathbf{v}_i\mathbf{v}_j = -\mathbf{v}_j\mathbf{v}_i$ за $i \neq j$.

Да дефинираме сега групата на Клифорд $C^*(q)$ като подгрупата на $C(q)^*$, състояща се от онези обратими елементи x, за които $xVx^{-1} = V$. Анизотропните вектори на V са в $C^*(q)$ и $\mathbf{vuv}^{-1} = -T_{\mathbf{v}}(\mathbf{u})$ за $\mathbf{u}, \mathbf{v} \in V$, където $\mathbf{v}$ е анизотропен и $T_{\mathbf{v}}$ е рефлексията на хиперравнината $\mathbf{v}^{\perp}$, зададена така:

$$T_{\mathbf{v}}(\mathbf{u}) = \mathbf{u} - 2\frac{B(\mathbf{u}, \mathbf{v})}{q(\mathbf{v})}\mathbf{v}, \quad \mathbf{u} \in V.$$

В сила са следните свойства на рефлексиите: $T_{\mathbf{v}}$ е линейно изображение, $T_{\mathbf{v}}|_{\mathbf{v}^{\perp}} = 1_{\mathbf{v}^{\perp}}, T_{\mathbf{v}}(\mathbf{v}) = -\mathbf{v}, T_{\mathbf{v}}^2 = 1_V$ и $T_{\mathbf{v}} \in O(q)$.

Да дефинираме изображение r чрез $r_x : \mathbf{u} \mapsto (-1)^{\partial x} x\mathbf{u}x^{-1}$, за $x \in C^*(q)$ и $\mathbf{u} \in V$. От равенствата $q(r_x(\mathbf{u})) = r_x(\mathbf{u})^2 = x\mathbf{u}^2x^{-1} = q(\mathbf{u})$ следва, че r_x е изометрия и понеже $r_{xy} = r_x \cdot r_y$, r е хомоморфизъм. Освен това r е сюрективно, тъй като $T_{\mathbf{v}} = r_{\mathbf{v}}$ и всяка изометрия е произведение на рефлексии (виж [La, Le4]).

Така получаваме точната редица

$$1 \longrightarrow k^* \longrightarrow C^*(q) \xrightarrow{r} O(q) \longrightarrow 1,$$

В частност, за $C_0^*(q) = C^*(q) \cap C_0(q)$ получаваме друга точна редица

$$1 \longrightarrow k^* \longrightarrow C_0^*(q) \xrightarrow{r} SO(q) \longrightarrow 1.$$

Тензорната алгебра $T(V)$ притежава анти-инволюция ι зададена чрез $\iota(\mathbf{u}_1 \otimes \cdots \otimes \mathbf{u}_r) = \mathbf{u}_r \otimes \cdots \otimes \mathbf{u}_1$. Тя запазва идеала $I(q)$, и затова индуцира анти-инволюция в $C(q)$, която ще наричаме *главна инволюция*. Тя запазва скаларите, сумите и векторите, и обръща произведенията. Означаваме с $N : C^*(q) \to k^*$ нормата зададена чрез $N(x) = x\iota(x)$. Може да се покаже, че това е хомоморфизъм и че нормите на два прообраза на една изометрия се различават само с множител, който е квадрат. По този начин можем коректно да дефинираме хомоморфизъм $sp : O(q) \to k^*/k^{*2}$, наречен *спинорна норма*, чрез равенството $sp(\prod T_{\mathbf{v}}) = \prod \overline{q(\mathbf{v})}$. Тук използваме факта, че всяка изометрия е произведение на рефлексии $T_{\mathbf{v}}$ за някои анизотропни вектори $\mathbf{v}$.

Като положим сега $\mathrm{Pin}(q) = \ker(N)$ и $\mathrm{Spin}(q) = \mathrm{Pin}(q) \cap C_0^*(q)$, получаваме дългите точни редици

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Pin}(q) \xrightarrow{r} O(q) \xrightarrow{sp} k^*/2$$

и

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Spin}(q) \xrightarrow{r} SO(q) \xrightarrow{sp} k^*/2.$$

Ако вземем сепарабелната обвивка $\overline{k}_{sep}$ на k, получаваме кратките точни редици

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Pin}(\overline{q}) \xrightarrow{r} O(\overline{q}) \longrightarrow 1 \tag{2.7}$$

и

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Spin}(\overline{q}) \xrightarrow{r} SO(\overline{q}) \longrightarrow 1. \tag{2.8}$$

В тази връзка, ще разгледаме следното приложения на теорема 2.2.4 при $p = 2$.

Теорема 2.4.2. *Нека групите G и $H \leq G$ са както в предположенията на определение 2.2.3 при $p = 2$. Именно, нека $\{\sigma_1, \ldots, \sigma_\kappa\}$ е фиксирано пораждащо множество на G със следните свойства: $|\sigma_1| = 2^{n-1}$ за $n > 1$, подгрупата H породена от $\sigma_2, \ldots, \sigma_\kappa$ е нормална в G, и факторгрупата G/H е изоморфна на цикличната група $C_{2^{n-1}}$. Нека $\varphi : G/H \to \overline{k}_{sep}^*$ е хомоморфизъм индуциран от изоморфизма $G/H \cong \langle \zeta_{2^{n-1}} \rangle$ и от включването $\langle \zeta_{2^{n-1}} \rangle \hookrightarrow \overline{k}_{sep}^*$, където $\zeta_{2^{n-1}}$ е примитивен корен на единицата от степен 2^{n-1}. Да предположим още, че е дадено ортогонално представяне $G \hookrightarrow O(q)$, и да образуваме ограничението (рестрикцията) $1 \longrightarrow \mu_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$ на точната редица $1 \longrightarrow \mu_2 \longrightarrow \mathrm{Pin}(\overline{q}) \longrightarrow O(\overline{q}) \longrightarrow 1$. Тогава съществува подгрупа $\overline{G}$ на $C^*(\overline{q})$ такава, че*

(i) *Диаграмата*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_2 & \longrightarrow & \overline{G} & \xrightarrow{r'} & G & \longrightarrow & 1 \\ & & \downarrow N & & \downarrow N & & \downarrow \varphi & & \\ 1 & \longrightarrow & 1 & \longrightarrow & \overline{k}_{sep}^* & = & \overline{k}_{sep}^* & \longrightarrow & 1 \end{array}$$

е комутативна с точни редове, където N е нормата, а r' е ограничението на $r : C^*(\overline{q}) \to O(\overline{q})$ върху $\overline{G}$;

(ii) *Или $\overline{G} = \widetilde{G}^{(2^n, \sigma_1)}$, или $\widetilde{G} = \overline{G}^{(2^n, \sigma_1)}$.*

Доказателство: Да изберем и да фиксираме про-образи $\widetilde{\sigma}_1, \ldots, \widetilde{\sigma}_\kappa \in \widetilde{G}$ на пораждащите $\sigma_1, \ldots, \sigma_\kappa$ на G. Нека $\overline{G}$ е подгрупата на $C^*(\overline{q})$, породена от елементите $\overline{\sigma}_1 = \widetilde{\sigma}_1\zeta_{2^n}, \overline{\sigma}_2 = \widetilde{\sigma}_2, \ldots, \overline{\sigma}_\kappa = \widetilde{\sigma}_\kappa$. Ще покажем, че $\overline{G}$ удовлетворява условията **(i)** и **(ii)**.

Първо, ще проверим, че $\ker(r') \cong \mu_2$. Да изберем произволно x от $\ker(r')$, т.е. $x = \prod \overline{\sigma}_1^{i_1}\overline{\sigma}_2^{i_2}\cdots\overline{\sigma}_\kappa^{i_\kappa}$ и $r'(x) = \prod \sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_\kappa^{i_\kappa} = 1$. Тъй като $\sigma_1^{i_1} \notin H$ за $1 \leq i_1 < 2^{n-1}$, получаваме $i_1 \equiv 0 \pmod{2^{n-1}}$. Оттук следва, че $x = \pm\overline{\sigma}_2^{i_2}\cdots\overline{\sigma}_\kappa^{i_\kappa} = \pm\widetilde{\sigma}_2^{i_2}\cdots\widetilde{\sigma}_\kappa^{i_\kappa} \in \ker(r) \cong \mu_2$, където с r означаваме още и ограничението на r върху $\mathrm{Pin}(\overline{q})$.

По-нататък, $N(\overline{\sigma}_1) = N(\widetilde{\sigma}_1)\zeta_{2^n}^2 = \zeta_{2^{n-1}} = \varphi r'(\overline{\sigma}_1)$ и $N(\overline{\sigma}_i) = \varphi r'(\overline{\sigma}_i) = 1$ за $i = 2, \ldots, \kappa$. Следователно, диаграмата в условието наистина е комутативна и е с точни редове.

Накрая, имаме или $|\widetilde{\sigma}_1| = 2^{n-1}$, или $\widetilde{\sigma}_1^{2^{n-1}} = -1$. Ако $|\widetilde{\sigma}_1| = 2^{n-1}$, то имаме $\overline{\sigma}_1^{2^{n-1}} = \zeta_{2^n}^{2^{n-1}} = -1$, и понеже останалите съотношения между пораждащите на $\widetilde{G}$, съответно на $\overline{G}$, са идентични, установяваме, че $\overline{G} = \widetilde{G}^{(2^n,\sigma_1)}$. Ако $\widetilde{\sigma}_1^{2^{n-1}} = -1$, имаме, че $\overline{\sigma}_1^{2^{n-1}} = 1$, значи $\widetilde{G} = \overline{G}^{(2^n,\sigma_1)}$. □

Сега ще се спрем на двойните обвивки на симетричната група S_n, следвайки означенията на Ледет [Le4]. Нека L/k е разширение на Галоа с група на Галоа G, и да предположим, че L е полето на разлагане над k на неразложимия полином $f(x) \in k[x]$ от степен n. Тогава можем да вложим транзитивно G в S_n, считайки елементите на G като пермутации на корените на $f(x)$. Да разгледаме т. нар. 'положителна' двойна обвивка

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{S}_n^+ \longrightarrow S_n \longrightarrow 1,$$

за която транспозициите се повдигат до елементи от ред 2, и 'отрицателната' двойна обвивка

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{S}_n^- \longrightarrow S_n \longrightarrow 1,$$

за която транспозициите се повдигат до елементи от ред 4 (и в двата случая произведението на две независими транспозиции се повдига до елементи от ред 4). Да образуваме сега ограниченията

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{G}^+ \longrightarrow G \longrightarrow 1,$$

и

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{G}^- \longrightarrow G \longrightarrow 1,$$

на позитивната и, съответно, отрицателната двойна обвивка на S_n.

Следствие 2.4.3. *В горните означения да предположим, че G съдържа транспозиция. Тогава $\widetilde{G}^- = \widetilde{G}^{+(4,\sigma_1)}$ и връзката между препятствията на съответните задачи за вложимост е $O_{\widetilde{G}^-} = (-1, d_f)O_{\widetilde{G}^+}$, където d_f е дискриминантата на $f(x)$.*

Доказателство: Да означим със σ_1 някоя транспозиция на G, и с H подгрупата $G \cap A_n$ на G. Да изберем множество от пораждащи $\sigma_2, \ldots, \sigma_k$ за H, откъдето $\sigma_1, \sigma_2, \ldots, \sigma_k$ са пораждащи на G. Да изберем техни про-образи $\widetilde{\sigma}_1, \widetilde{\sigma}_2, \ldots, \widetilde{\sigma}_k$ в $\widetilde{G}^+$. Тъй като $\widetilde{G}^+$ е в $\mathrm{Pin}_n(\overline{k}_{sep})$ (виж [Le4]) и $\sigma_1^2 = \widetilde{\sigma}_1^2 = 1$, можем да използваме теорема 2.4.2. По този начин можем да дефинираме подгрупа $\overline{G} = \widetilde{G}^{+(4,\sigma_1)}$ на $C_n^*(\overline{k}_{sep})$, породена от $\overline{\sigma}_1 = \widetilde{\sigma}_1 i, \overline{\sigma}_2 = \widetilde{\sigma}_2, \ldots, \overline{\sigma}_k = \widetilde{\sigma}_k$ (i е имагинерната единица). Сега, от $\overline{\sigma}_1^2 = -1$ следва, че всяка транспозиция от G се повдига до елемент от ред 4 в $\overline{G}$. Наистина, ако σ е друга транспозиция в G, то $\sigma = \sigma_1\tau$ за $\tau \in H$, така че можем да изберем про-образ $\overline{\sigma} = \overline{\sigma}_1\overline{\tau} = i\widetilde{\sigma}_1\overline{\tau} \in \overline{G}$, където $\overline{\tau}$ също е в $\widetilde{G}^+$, и $|\widetilde{\sigma}_1\overline{\tau}| = 2$. Следователно, $\overline{\sigma}^2 = -1$ и $\overline{G} \cong \widetilde{G}^-$.

Накрая, от $\sigma_1(\sqrt{d_f}) = -\sqrt{d_f}$ получаваме връзката между препятствията, дадена в условието. □

Сега ще припомним дефиницията на усукването на Галоа, която използва съществуването на първа кохомологична група $H^1(G, \mathcal{G})$, където $\mathcal{G}$ е неабелова група с G-действие. Нека отново (V, q) е квадратично пространство над k, и нека K/k е разширение на Галоа с група на Галоа G. Тогава можем да разширим полето на скаларите и да получим квадратично пространство (V_K, q_K). Полу-линейното действие на G тогава ни дава равенството $q_K(\sigma u) = \sigma q_K(u)$. Обратно, ако (W, Q) е квадратично пространство над K снабдено с полу-линейно действие такова, че $Q(\sigma u) = \sigma Q(u)$, получаваме квадратично пространство (W^G, Q^G) над k чрез вземане на неподвижните елементи и ограничаване на Q. Тези две действия (разширяване на скаларите и неподвижните елементи) запазват регулярността и са взаимно обратни. Също, $O(Q)$ е G-група чрез спрягането: $(\sigma\varphi)(u) = \sigma\varphi(\sigma^{-1}u)$.

По-нататък, нека $f : G \to O(q_K)$ е кръстосан хомоморфизъм. Тогава можем да дефинираме полу-линейно действие чрез ${}^\sigma u = f_\sigma(\sigma u)$ и да получим индуцираното квадратично пространство $(V_f, q_f) = ((V_K)^G, (q_K)^G)$ над k. Освен това, ако g е еквивалентен с f, т.е. $g_\sigma = \varphi f_\sigma \sigma \varphi^{-1}$ за някое $\varphi \in O(q_K)$, то $V_g = \varphi(V_f)$ и следователно (V_f, q_f) и (V_g, q_g) са еквивалентни. По този начин с всеки елемент от $H^1(G, O(q))$ можем да асоциираме клас на еквивалетност на квадратични пространства над k.

Определение 2.4.4. Казваме, че квадратичното пространство (V_f, q_f) е образувано от (V, q) чрез *усукване на Галоа* с помощта на f.

Важна роля при пресмятане на препятствията на задачи за вложимост, произтичащи от точните редици (2.7) и (2.8) играе така наречената *инварианта на Хасе-Вит* или *втори клас на Стийфел-Уитни* на q.

Определение 2.4.5. *Инварианта на Хасе-Вит* наричаме следното произведение на кватернионни алгебри

$$\mathrm{hw}(q) = \prod_{i<j} (a_i, a_j) \in \mathrm{Br}(k),$$

където $a_i = q(u_i)$ за някакъв каноничен ортогонален базис $u_1, \ldots, u_n$ на q.

Препятствията на задачите за вложимост тогава се пресмятат по формулата, която е изложена в следната

Теорема 2.4.6. ([Fr, Le4]) *Нека L/k е крайно разширение на Галоа с група на Галоа $G = \mathrm{Gal}(L/k)$ и нека $G \hookrightarrow O(q)$ за някоя регулярна квадратична форма q над k. Нека $e : \mathrm{Gal}(\overline{k}/k) \to O(q)$ е индуцираният кръстосан хомоморфизъм, и нека q_e е квадратичната форма, получена от q чрез усукването на Галоа с помощта на e. Също, нека*

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$$

е групово разширение индуцирано от влагането $G \hookrightarrow O(q)$ и точната редица

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Pin}(\overline{q}) \xrightarrow{r} O(\overline{q}) \longrightarrow 1.$$

Нека $K/k = k(\sqrt{a_1}, \ldots, \sqrt{a_r})/k$ е максималното елементарно абелово 2-подразширение на L/k и нека $\rho_1, \ldots, \rho_r \in G$ са такива, че $\rho_i(\sqrt{a_j}) = (-1)^{\delta_{ij}} \cdot \sqrt{a_j}$. Тогава препятствието на задачата за вложимост $(L/k, \widetilde{G}, \mu_2)$ е

$$\mathrm{hw}(q)\mathrm{hw}(q_e)(d, -d_e) \prod_{i=1}^{r} (a_i, sp(\rho_i)) \in \mathrm{Br}(k),$$

където d и d_e са дискриминантите съответно на q и q_e.

2.5 Индуцирани ортогонални представяния на групи на Галоа

Нека сега L/k е крайно разширение на Галоа с група на Галоа G, нека H е подгрупа на G с неподвижно поле $K = L^H$, и нека $\mu : H \hookrightarrow O(q)$ е ортогонално представяне над k. Тогава, според [Fr, FM], можем да конструираме *индуцираното ортогонално представяне* $\mathrm{ind}\mu : G \hookrightarrow O(q_{\mathrm{ind}\mu})$, където $\mathrm{ind}\mu$ има като прилежащ модул индуцирания G-модул на H-модула V_q : $V_{\mathrm{ind}\mu} = \oplus(V_q \otimes \sigma) = V_q \otimes_{kH} kG$, σ пробягва дадена дясна трансверзала R на H в G. Да отбележим, че $V_q \subset V_{\mathrm{ind}\mu}$ е подпространство, което е H-инвариантно. Не е трудно да се покаже, че ако е дадено ортогонално представяне $\mu : H \hookrightarrow O(q)$, такова $V_{\mathrm{ind}\mu}$ съществува и е единствено с точност до изоморфизъм (виж например [FH, §3.3]). Нещо повече, действието на G може да бъде явно зададено: всеки елемент $v \in V_{\mathrm{ind}\mu}$ има единствено представяне $v = \sum w_\sigma \otimes \sigma$ за някои елементи w_σ във V_q. За дадено $g \in G$, действието се задава чрез

$$g \cdot (w_\sigma \otimes \sigma) = hw_\sigma \otimes \tau \quad \text{ако } g\sigma = \tau h \ (\tau \in R). \tag{2.9}$$

Нататък, нека ни е дадено специално ортогонално представяне $\mu : H \hookrightarrow SO(q)$ над k. Означаваме отново с $\overline{k}_{sep}$ сепарабелната обвивка на k, и с $\overline{q}$ разширената форма на q върху $\overline{k}_{sep}$. Тогава имаме следната диаграма

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_2 & \longrightarrow & \widetilde{H} & \longrightarrow & H & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \mathrm{Spin}(\overline{q}) & \longrightarrow & SO(\overline{q}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \overline{k}^*_{sep} & \longrightarrow & C^*_0(\overline{q}) & \longrightarrow & SO(\overline{q}) & \longrightarrow & 1,
\end{array}$$

първият ред на която е ограничението на $1 \longrightarrow \mu_2 \longrightarrow \mathrm{Spin}(\overline{q}) \longrightarrow SO(\overline{q}) \longrightarrow 1$. Индуцираното ортогонално представяне $\mathrm{ind}\mu : G \hookrightarrow O(q_{\mathrm{ind}\mu})$ на свой ред дава комутативната диаграма

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_2 & \longrightarrow & \widetilde{G} & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & \mathrm{Pin}(\overline{q}_{\mathrm{ind}\mu}) & \longrightarrow & O(\overline{q}_{\mathrm{ind}\mu}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \overline{k}^*_{sep} & \longrightarrow & C^*(\overline{q}_{\mathrm{ind}\mu}) & \longrightarrow & O(\overline{q}_{\mathrm{ind}\mu}) & \longrightarrow & 1.
\end{array}$$

Преди да формулираме нашата основна теорема, ще докажем следната кохомологична

Лема 2.5.1. ([Mi4, Lemma 2.3]) *Нека G е про-крайна група, нека H е затворена подгрупа с индекс 2 в G, нека $R = \{1, g\}$ е дясна трансверзала на H в G, т.е. $G = H \cup Hg$, и да положим $h_0 = g^2$. Нека $1 \longrightarrow \mu_2 \longrightarrow H_1 \longrightarrow H \longrightarrow 1$ е групово разширение и да изберем про-образ $\overline{u}_h \in H_1$ на всяко $h \in H$. Системата $\{\overline{u}_h\}_{h\in H}$ задава 2-коцикъл $\overline{f} \in Z^2(H, \mu_2)$ чрез $\overline{f}(s_1, s_2) = \overline{u}^{-1}_{s_1 s_2}\overline{u}_{s_1}\overline{u}_{s_2}$. Да означим с $\delta : H \to \{0, 1\}$ изображението, зададено с $\overline{u}_{h_0}\overline{u}_h\overline{u}^{-1}_{h_0} = (-1)^{\delta(h)}\overline{u}_{h_0 h h_0^{-1}}$. Нека също $1 \longrightarrow \mu_2 \longrightarrow G_1 \longrightarrow G \longrightarrow 1$ е групово разширение и да изберем про-образи $u_{hg^i} \in G_1$ на всеки елемент $hg^i \in G, i = 0, 1$. Системата $\{u_{hg^i}\}$ тогава задава 2-коцикъл $f \in Z^2(G, \mu_2)$, и ако следните три условия:*

(i) $f(s_1, s_2) = u^{-1}_{s_1 s_2}u_{s_1}u_{s_2} = \overline{f}(s_1, s_2)\overline{f}(gs_1g^{-1}, gs_2g^{-1}), \forall s_1, s_2 \in H;$

(ii) $u_g u_h u_g^{-1} = (-1)^{\delta(h)}u_{ghg^{-1}}, \forall h \in H;$ *u*

(iii) $u_g^2 = u_{h_0}$

са изпълнени, то $[f] = \mathrm{cor}_{G/H}([\overline{f}])$.

Доказателство: От теорема 2.3.9 имаме, че

$$(\mathrm{cor}_{G/H}(\overline{f}))(s_1, s_2) = \begin{cases} \overline{f}(s_1, s_2)\overline{f}(gs_1g^{-1}, gs_2g^{-1}), & (s_1, s_2) \in H \times H \\ \overline{f}(s_1g^{-1}, gs_2g^{-1})\overline{f}(gs_1, s_2), & (s_1, s_2) \in Hg \times H \\ \overline{f}(s_1, s_2g^{-1})\overline{f}(gs_1g^{-1}, gs_2), & (s_1, s_2) \in H \times Hg \\ \overline{f}(s_1g^{-1}, gs_2)\overline{f}(gs_1, s_2g^{-1}), & (s_1, s_2) \in Hg \times Hg. \end{cases}$$

Тъй като изборът на u_{gh} за $h \neq 1$ не влияе на условията (i)-(iii), можем да считаме, че $u_{gh} = u_g u_h \overline{f}(h_0, h)$. Тогава $f(g, h) = u^{-1}_{gh}u_g u_h = \overline{f}(h_0, h)$, което удовлетворява формулата за корестрикцията.

Нататък,

$$u_{hg} = u_{g(g^{-1}hg)} = (-1)^{\delta(g^{-1}hg)}u_h u_g \overline{f}(h_0, g^{-1}hg),$$

понеже $u_g^{-1}u_h u_g = (-1)^{\delta(g^{-1}hg)}u_{g^{-1}hg}$. Следователно,

$$f(h, g) = u^{-1}_{hg}u_h u_g = (-1)^{\delta(g^{-1}hg)}\overline{f}(h_0, g^{-1}hg).$$

Сега, от $\overline{u}_{h_0}\overline{u}_h\overline{u}_{h_0}^{-1} = (-1)^{\delta(h)}\overline{u}_{h_0hh_0^{-1}}$ следва, че

$$\overline{u}_{h_0}\overline{u}_{g^{-1}hg}\overline{u}_{h_0}^{-1} = (-1)^{\delta(g^{-1}hg)}\overline{u}_{ghg^{-1}},$$

значи

$$\begin{aligned}\overline{f}(ghg^{-1}, h_0) &= \overline{u}_{ghg}^{-1}\overline{u}_{ghg^{-1}}\overline{u}_{h_0} = (-1)^{\delta(g^{-1}hg)}\overline{u}_{ghg}^{-1}\overline{u}_{h_0}\overline{u}_{g^{-1}hg} \\ &= (-1)^{\delta(g^{-1}hg)}\overline{f}(h_0, g^{-1}hg).\end{aligned}$$

Следователно, $f(h,g) = \overline{f}(ghg^{-1}, h_0)$, което също удовлетворява формулата за корестрикцията.

Накрая, от (iii) получаваме $f(g,g) = u_{h_0}^{-1}u_g^2 = 1$, така че за да получим останалите равенства във формулата за корестрикцията е нужно единствено да приложим стандартното кохомологично тъждество. □

Сега ще докажем следната основна

Теорема 2.5.2. ([Mi4, Theorem 2.2]) *Нека G е крайна група и нека H е подгрупа на G такава, че $|H| = 2^t m, (t, m \geq 1)$. Нека също $\mu : H \hookrightarrow SO(q)$ е специално ортогонално представяне над k с прилежащ модул V_q такъв, че $n = \dim_k V_q \equiv 0 \pmod 4$. Да означим с $\overline{f} \in Z^2(H, \mu_2)$ и с $f \in Z^2(G, \mu_2)$ 2-коциклите дадени от описаните по-горе групови разширения $1 \longrightarrow \mu_2 \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 1$ и $1 \longrightarrow \mu_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$, съответно. Тогава $[f] = \mathrm{cor}_{G/H}([\overline{f}])$, където $\mathrm{cor}_{G/H} : H^2(H, \mu_2) \to H^2(G, \mu_2)$ е хомоморфизма на корестрикция.*

Доказателство: Ще разделим доказателството на три стъпки.

I). Да предположим,че H е подгрупа с индекс 2 в G. Нека $R = \{1, g\}$ е дясна трансверзала на H в G, т.е. $G = H \cup Hg$, и да положим $h_0 = g^2$. Да дефинираме k-модул V чрез $V = V_{q_1} \oplus V_{q_2}$, където $q_1 = q_2 = q$ и $V_{q_1} = V_{q_2} = V_q$ е равенство на k-модули. Така получаваме квадратичното пространство $(V, q_1 \perp q_2)$. Според (2.9), индуцираното действие на G се задава чрез:

$$h(\mathbf{v}_1, \mathbf{v}_2) = (h\mathbf{v}_1, g^{-1}hg\mathbf{v}_2) \ \text{ и } \ hg(\mathbf{v}_1, \mathbf{v}_2) = (hh_0\mathbf{v}_2, g^{-1}hg\mathbf{v}_1),$$

за $h \in H$ и $v_i \in V_{q_i}, i = 1, 2$.

По-нататък, можем да разширим скаларите за да получим квадратично пространство $(V_{\overline{k}_{sep}}, \overline{q}_1 \perp \overline{q}_2)$, където $\overline{q}_i$ е скаларното разширение на q_i. По този начин,

специалното ортогонално представяне $\mu : H \hookrightarrow SO(q) \hookrightarrow SO(\overline{q})$ индуцира ортогонално представяне $\mathrm{ind}\mu : G \hookrightarrow O(q_1 \perp q_2) \hookrightarrow O(\overline{q}_1 \perp \overline{q}_2)$.

Да дефинираме сега изометрии $h\oplus 1$ и $1\oplus g^{-1}hg$ в $O(\overline{q}_1 \perp \overline{q}_2)$ чрез $(h\oplus 1)(\mathbf{v}_1, \mathbf{v}_2) = (h\mathbf{v}_1, \mathbf{v}_2)$ и $(1 \oplus g^{-1}hg)(\mathbf{v}_1, \mathbf{v}_2) = (\mathbf{v}_1, g^{-1}hg\mathbf{v}_2)$. Оттук получаваме, че $h = (h \oplus 1)(1 \oplus g^{-1}hg) \in O(\overline{q}_1 \perp \overline{q}_2)$ за всяко $h \in H$. Тъй като h е в $SO(\overline{q})$, можем да изберем и фиксираме про-образ $u_h \in \mathrm{Spin}(\overline{q}_1) \subset C_0^*(\overline{q}_1)$ на $h \oplus 1 \in O(\overline{q}_1 \perp \overline{q}_2)$. Можем също така да изберем про-образ $v_h \in C_0^*(\overline{q}_2)$ на $1 \oplus g^{-1}hg \in O(\overline{q}_1 \perp \overline{q}_2)$ за всяко $h \in H$. Ние, обаче, ще фиксираме избора на елементите v_h малко по-късно.

От [Fr, p. 119] е известно, че за елементите $x_i \in C^*(q_i) \subset C^*(q_1 \perp q_2), i = 1, 2$ е в сила правилото за комутиране $x_1x_2 = (-1)^{\partial x_1 \partial x_2}x_2x_1$, и че то определя подгрупата на $C^*(q_1 \perp q_2)$ породена от $C^*(q_i), i = 1, 2$. Тъй като в нашия случай $\partial u_h = \partial v_h = 0$, имаме, че $u_{h_1}v_{h_2} = v_{h_2}u_{h_1}, \forall h_1, h_2 \in H$. Нататък, от равенствата $g(h \oplus 1)(\mathbf{v}_1, \mathbf{v}_2) = (h_0\mathbf{v}_2, h\mathbf{v}_1) = (1 \oplus ghg^{-1})g(\mathbf{v}_1, \mathbf{v}_2)$, получаваме $g(h \oplus 1)g^{-1} = 1 \oplus ghg^{-1}$, така че ако изберем про-образ $w_g \in \mathrm{Pin}(\overline{q}_1 \perp \overline{q}_2)$ на g, ще получим, че $w_g u_h w_g^{-1} = \pm v_{ghg^{-1}}$. Очевидно, можем да считаме, че $u_{h_0}u_h u_{h_0}^{-1} = (-1)^{\delta(h)}u_{h_0hh_0^{-1}}$ за някое изображение $\delta : H \to \{0, 1\}$. Да положим сега

$$v_{ghg^{-1}} = (-1)^{\delta(h)}w_g u_h w_g^{-1} \quad \text{и} \quad w_h = u_h v_h.$$

Тогава $w_g^2 = \pm u_{h_0}$ и $v_h = w_g^{-1}u_{ghg^{-1}}w_g$. Тъй като про-образите $\{u_h\}_{h\in H}$ определят 2-коцикъла $\overline{f} \in Z^2(H, \mu_2)$, даден в условието, получаваме

$$f(h_1, h_2) = w_{h_1h_2}^{-1}w_{h_1}w_{h_2} = \overline{f}(h_1, h_2)\overline{f}(gh_1g^{-1}, gh_2g^{-1}),\ \forall h_1, h_2 \in H.$$

Така се убеждаваме, че условието (i) на лема 2.5.1 е удовлетворено. Условието (ii) също се изпълнява, както се вижда от

$$w_g w_h w_g^{-1} = w_g u_h w_g^{-1} w_g v_h w_g^{-1} = (-1)^{\delta(h)}v_{ghg^{-1}}u_{ghg^{-1}} = (-1)^{\delta(h)}w_{ghg^{-1}}.$$

По този начин, остава само да се провери равенството $w_g^2 = w_{h_0}$. Нека $e_1, \ldots, e_n$ е ортогонален базис на $V_{\overline{q}}$ над $\overline{k}_{sep}$, където $n = \dim_k V_q = \dim_{\overline{k}_{sep}} V_{\overline{q}}$. Очевидно, векторите $e'_1 = (e_1, 0), \ldots, e'_n = (e_n, 0), e'_{n+1} = (0, e_1), \ldots, e'_{2n} = (0, e_n)$ образуват ортогонален базис на $V_{\overline{k}_{sep}} = V_{\overline{q}_1} \oplus V_{\overline{q}_2}$ над $\overline{k}_{sep}$. Да отбележим, че $\overline{q}_1(e'_i) = \overline{q}_2(e'_{n+i}) = q(e_i) = a_i \in k^*$ за $i = 1, \ldots, n$. Не е трудно да се провери, че рефлексията $T_{(e'_i - e'_{n+i})/\sqrt{a_i}}$ разменя e'_i и e'_{n+i}, оставяйки другите e'_k инвариантни. Като про-образ на $T_{(e'_i - e'_{n+i})/\sqrt{a_i}}$ в $\mathrm{Pin}(\overline{q}_1 \perp \overline{q}_2)$ можем да изберем $x_i = (e'_i - e'_{n+i})/\sqrt{2a_i}, i = 1, \ldots, n$. Тогава $x_i^2 = 1, x_ix_j = -x_jx_i$ и $(x_ix_j)^2 = -1$, ако $i \neq j$. Нататък, да дефинираме изометрия $\varphi \in O(\overline{q}_1 \perp \overline{q}_2)$ чрез

$\varphi(\mathbf{v}_1, \mathbf{v}_2) = (\mathbf{v}_2, \mathbf{v}_1)$ за $v_i \in V_{\overline{q}_i}$. φ също може да бъде записано като произведение на рефлексии:

$$\varphi = T_{(e'_1 - e'_{n+1})/\sqrt{a_1}} T_{(e'_2 - e'_{n+2})/\sqrt{a_2}} \cdots T_{(e'_n - e'_{2n})/\sqrt{a_n}},$$

така че можем да изберем про-образ $x = x_1 x_2 \cdots x_n \in \mathrm{Pin}(\overline{q}_1 \perp \overline{q}_2)$ на φ. Тъй като $n \equiv 0 \pmod 4$ и $(x_i x_j x_k x_l)^2 = 1$, за четири различни индекса $i, j, k, l \leq n$, получаваме $x^2 = 1$. От друга страна, от равенството $(h_0^{-1} \oplus 1)g(\mathbf{v}_1, \mathbf{v}_2) = (\mathbf{v}_2, \mathbf{v}_1)$ следва, че $\varphi = (h_0^{-1} \oplus 1)g$. Тогава $u_{h_0}^{-1} w_g$ е про-образ на φ в $\mathrm{Pin}(\overline{q}_1 \perp \overline{q}_2)$, значи $u_{h_0}^{-1} w_g = \pm x$ има ред 2. Следователно, $w_g^2 = u_{h_0} w_g^{-1} u_{h_0} w_g = u_{h_0} v_{h_0} = w_{h_0}$, и доказателството на тази стъпка е завършено.

II). Нека G е 2-група. Тази стъпка следва от стъпка I) и от транзитивността както на индуцираните ортогонални представяния, така и на хомоморфизмите на корестрикция.

III). Общият случай: $|H| = 2^t m, (t, m \geq 1)$. Нека $\mathcal{H}$ е силова 2-подгрупа на H, и да изберем също една силова 2-подгрупа $\mathcal{G}$ на G. Тогава имаме груповите разширения:

$$\overline{f} : 1 \longrightarrow \mu_2 \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 1,\ \overline{f}_1 : 1 \longrightarrow \mu_2 \longrightarrow \widetilde{\mathcal{H}} \longrightarrow \mathcal{H} \longrightarrow 1,$$
$$f : 1 \longrightarrow \mu_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1,\ f_1 : 1 \longrightarrow \mu_2 \longrightarrow \widetilde{\mathcal{G}} \longrightarrow \mathcal{G} \longrightarrow 1,$$

където $[\overline{f}_1] = \mathrm{res}_{H/\mathcal{H}}([\overline{f}])$ и $[f_1] = \mathrm{res}_{G/\mathcal{G}}([f])$. Според предишната стъпка, имаме също, че $[f_1] = \mathrm{cor}_{\mathcal{G}/\mathcal{H}}([\overline{f}_1])$. Комутативната диаграма:

$$\begin{array}{ccc} H^2(H, \mu_2) & \xrightarrow{\mathrm{cor}} & H^2(G, \mu_2) \\ \big\downarrow \mathrm{res} & & \big\downarrow \mathrm{res} \\ H^2(\mathcal{H}, \mu_2) & \xrightarrow{\mathrm{cor}} & H^2(\mathcal{G}, \mu_2) \end{array}$$

тогава ни дава $\mathrm{cor}_{\mathcal{G}/\mathcal{H}} \cdot \mathrm{res}_{H/\mathcal{H}}([\overline{f}]) = [f_1] = \mathrm{res}_{G/\mathcal{G}} \cdot \mathrm{cor}_{G/H}([\overline{f}]) = \mathrm{res}_{G/\mathcal{G}}([f])$, и вземайки предвид, че вертикалните изображения са инективни (виж [Se1, §2.4]), получаваме това, което трябваше да се докаже. □

Нека отново да предположим, че L/k е нормално разширение с крайна група G. Можем винаги да намерим примитивен елемент θ такъв, че $L = k(\theta)$. Нека $f(x) \in k[x]$ е минималният полином на θ от степен $n = [L : k]$, и нека $\theta = \theta_1, \theta_2, \ldots, \theta_n$ са спрегнатите на θ. Тогава $G = G(f)$ се влага транзитивно в симетричната група S_n.

За дадена собствена подгрупа H на G, да положим $m = |H|$ и $k = (G : H) = n/m$. Очевидно, θ също така е примитивен елемент на разширението L/K, където $K = L^H$. Тъй като минималният полином на θ над K дели $f(x)$, можем да считаме, че $\theta = \theta_1, \theta_2, \ldots, \theta_m$ за $1 < m = [L : K] < n$ са спрегнатите на θ над K. H се влага транзитивно в S_m, така че можем да образуваме груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 1, \tag{2.10}$$

което представлява ограничението на груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{S}_m \longrightarrow S_m \longrightarrow 1,$$

където $\widetilde{S}_m$ е положителната двойна обвивка на S_m.

Нататък, да припомним, че за квадратичната форма $q_1 = \langle 1, \ldots, 1 \rangle$ върху $V_1 = k^m$ имаме, че S_m се влага в $O_m(k) = O(q_1)$, откъдето получаваме ортогонално представяне $H \hookrightarrow O_m(k)$. Да положим $q = q_1 \perp q_2 \perp \cdots \perp q_s$ и $V = V_1 \oplus V_2 \oplus \cdots \oplus V_s$, където $q_1 = q_2 = \cdots = q_s$ и $V_1 = V_2 = \ldots V_s$. По този начин получаваме индуцирано ортогонално представяне $G \hookrightarrow O_n(k)$, което е идентично с транзитивното влагане на $G = G(f)$ в S_n. Да вземем сега груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1, \tag{2.11}$$

което се явява ограничението на груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{S}_n \longrightarrow S_n \longrightarrow 1.$$

Да означим с $\overline{f} \in Z^2(H, \mu_2)$ 2-кокласа представящ (2.10) и с $f \in Z^2(G, \mu_2)$ 2-кокласа представящ (2.11), т.е. $\overline{f} = \mathrm{res}(s_m)$ и $f = \mathrm{res}(s_n)$. От теорема 2.5.2 сега следва, че $[f] = \mathrm{cor}_{G/H}([\overline{f}])$, при допълнителното предположения $H \hookrightarrow SO_m(k)$ и $m \equiv 0 \pmod 4$.

Забележка 2.5.3. Транзитивното влагане, за което става дума тук е частен случай на влагането описано в [Le4, Ch. 6, S. 2] и [Se3, p. 653], където е взет елемент θ, който не е непременно примитивен. Така че ако θ не е примитивен, т.е. $l = \deg \theta < n$, можем да получим транзитивно влагане на G в S_l. В пример 4.3.14 ще илюстрираме разликата между груповите разширения, получени чрез двата вида транзитивни влагания на модулярната 2-група.

2.6 Специални диедрални представяния

Нека $char(k) \neq 2$ и нека k съдържа примитивен n-ти корен на единицата η за n-четно. Нека $H \cong D_{2n}$ е диедралната група от ред $2n$, породена от елементи h_0 и h_1 със съотношения $h_0^n = h_1^2 = 1, h_1 h_0 = h_0^{-1} h_1$.

Според [Fr] можем да конструираме диедрално ортогонално представяне (което не е специално) $H \hookrightarrow O(q_1)$, където (V_1, q_1) е квадратично пространство такова, че квадратичната форма q_1 е асоциирана с билинейната форма $b_1(x, y)$ зададена чрез $b_1(\mathbf{u}, \mathbf{v}) = 1, b_1(\mathbf{u}, \mathbf{u}) = b_1(\mathbf{v}, \mathbf{v}) = 0$ за някакъв базис $\mathbf{u}, \mathbf{v}$ на V_1. Действието на H върху V_1 се задава чрез

$$h_0(\mathbf{u}) = \mathbf{u}\eta, h_0(\mathbf{v}) = \mathbf{v}\eta^{-1}, h_1(\mathbf{u}) = \mathbf{v}, h_1(\mathbf{v}) = \mathbf{u}.$$

Да извършим смяна на базиса на V_1. Полагаме $\mathbf{u}_1 = \mathbf{u} + \mathbf{v}$ и $\mathbf{u}_2 = \mathbf{u} - \mathbf{v}$. Получаваме $b_1(\mathbf{u}_1, \mathbf{u}_1) = 2, b_1(\mathbf{u}_2, \mathbf{u}_2) = -2, b_1(\mathbf{u}_1, \mathbf{u}_2) = 0$, т.е. $q_1 \cong < 2, -2 >$. Действието на H върху $\mathbf{u}_1$ и $\mathbf{u}_2$ тогава е

$$h_0(\mathbf{u}_1) = \frac{1}{2}\left((\eta + \eta^{-1})\mathbf{u}_1 + (\eta - \eta^{-1})\mathbf{u}_2\right), h_1(\mathbf{u}_1) = \mathbf{u}_1,$$
$$h_0(\mathbf{u}_2) = \frac{1}{2}\left((\eta - \eta^{-1})\mathbf{u}_1 + (\eta + \eta^{-1})\mathbf{u}_2\right), h_1(\mathbf{u}_2) = -\mathbf{u}_2.$$

Нататък, нека H е подгрупа на диедралната група $G \cong D_{4n}$, т.е. G се поражда от елементи g и h_1 такива, че $g^2 = h_0, h_1 g = g^{-1} h_1$. Можем да построим индуцираното ортогонално представяне $G \hookrightarrow O(q)$, където $V = V_1 \oplus V_2, q = q_1 \perp q_2 =< 2, -2, 2, -2 >$, $V_1 \equiv V_2, q_1 \equiv q_2$. Да припомним действието на G:

$$h(\mathbf{v}_1, \mathbf{v}_2) = (h\mathbf{v}_1, g^{-1}hg\mathbf{v}_2) \text{ и } hg(\mathbf{v}_1, \mathbf{v}_2) = (hh_0\mathbf{v}_2, g^{-1}hg\mathbf{v}_1),$$

за $h \in H$ и $v_i \in V_{q_i}, i = 1, 2$. Следователно, действието на G върху базиса $\mathbf{w}_1 = (\mathbf{u}_1, 0), \mathbf{w}_2 = (\mathbf{u}_2, 0), \mathbf{w}_3 = (0, \mathbf{u}_1), \mathbf{w}_4 = (0, \mathbf{u}_2) \in V$ е

$$g(\mathbf{w}_1) = \mathbf{w}_3, g(\mathbf{w}_3) = (h_0\mathbf{u}_1, 0) = \frac{1}{2}\left((\eta + \eta^{-1})\mathbf{w}_1 + (\eta - \eta^{-1})\mathbf{w}_2\right),$$
$$g(\mathbf{w}_2) = \mathbf{w}_4, g(\mathbf{w}_4) = (h_0\mathbf{u}_2, 0) = \frac{1}{2}\left((\eta - \eta^{-1})\mathbf{w}_1 + (\eta + \eta^{-1})\mathbf{w}_2\right),$$
$$h_1(\mathbf{w}_1) = \mathbf{w}_1, h_1(\mathbf{w}_3) = \frac{1}{2}\left((\eta + \eta^{-1})\mathbf{w}_3 - (\eta - \eta^{-1})\mathbf{w}_4\right),$$
$$h_1(\mathbf{w}_2) = -\mathbf{w}_2, h_1(\mathbf{w}_4) = \frac{1}{2}\left((\eta - \eta^{-1})\mathbf{w}_3 - (\eta + \eta^{-1})\mathbf{w}_4\right).$$

Лесно се проверява, че това е специално представяне. Нещо повече, ако (V_Q, Q) е квадратично пространство над k и $\mathcal{H} \hookrightarrow O(Q)$ е ортогонално представяне на подгрупа $\mathcal{H}$ на групата $\mathcal{G}$ такава, че $\mathcal{G} = \mathcal{H} \cup g\mathcal{H}$ и $g^2 = h_0 \in SO(Q)$, то индуцираното ортогонално представяне $\mathcal{G} \hookrightarrow O(Q \perp Q)$ е специално тогава и само тогава, когато $\dim(V_Q)$ е четно число. Наистина, матрицата на произволно $h \in \mathcal{H}$ като линейно изображение, действащо във $V_Q \oplus V_Q$ е

$$\mathbf{B}_h = \begin{pmatrix} \mathbf{A}_h & \mathbf{0} \\ \mathbf{0} & \mathbf{A}_{g^{-1}hg} \end{pmatrix},$$

където $\mathbf{A}_h$ е матрицата на h действащо във V_Q. Матрицата на g тогава е

$$\mathbf{B}_g = \begin{pmatrix} \mathbf{0} & \mathbf{I} \\ \mathbf{A}_{h_0} & \mathbf{0} \end{pmatrix},$$

където $\mathbf{I}$ е единичната матрица от ред $\dim(V_Q)$. Следователно, $\det(\mathbf{B}_h) = 1$ и $\det(\mathbf{B}_g) = (-1)^{\dim(V_Q)}$.

Нека сега да опишем подгрупата $\widetilde{G}$ на $\mathrm{Spin}(\overline{q})$. Пресмятанията показват, че трансформацията g се получава чрез спрягане с елемента

$$z = \left(\frac{1}{2}(1-\eta)\mathbf{w}_1\mathbf{w}_2 + \eta + 1\right)(\mathbf{w}_1 - \mathbf{w}_3)(\mathbf{w}_2 - \mathbf{w}_4),$$

откъдето спинорната норма е $sp(g) = N(z) = -8^2\eta$. Тогава про-образа на g в $\widetilde{G}$ е $\widetilde{g} = (i/8)\mu^{-1}z$, където $\mu^2 = \eta, i^2 = -1$. Нататък,

$$\widetilde{g}^4 = \frac{\eta^{-2}}{2}\left(\frac{1}{2}(1-\eta^4)\mathbf{w}_1\mathbf{w}_2 + \eta^4 + 1\right),$$

откъдето

$$\widetilde{g}^{2n} = \widetilde{g}^{4\cdot n/2} = \frac{\eta^{-n}}{2^{n/2}}\left(\frac{1}{2}(1-\eta^{2n})\mathbf{w}_1\mathbf{w}_2 + \eta^{2n} + 1\right)\cdot 2^{n/2-1} = 1.$$

Трансформацията h_1, на свой ред, се получава чрез спрягане с елемента

$$y = \left(\frac{1}{2}(1-\eta)\mathbf{w}_3\mathbf{w}_4 - (\eta+1)\right)\mathbf{w}_2\mathbf{w}_4,$$

откъдето $sp(h_1) = N(y) = 16\eta$. Тогава про-образа на h_1 в $\widetilde{G}$ е $\widetilde{h}_1 = (\mu^{-1}/4)y$ и

$$\begin{aligned} \widetilde{h}_1^2 &= \frac{\eta^{-1}}{16}\left(-\frac{1}{4}(1-\eta)^2(\mathbf{w}_3\mathbf{w}_4)^2 + (1+\eta)^2\right)(\mathbf{w}_2\mathbf{w}_4)^2 \\ &= -\frac{\eta^{-1}}{4}\left(-(1-\eta)^2 + (1+\eta)^2\right) = -1. \end{aligned}$$

Накрая, имаме $(\widetilde{h}_1\widetilde{g})^2 = -1$, значи $\widetilde{G}$ има представяне

$$\widetilde{G} \cong \langle \widetilde{g}, \widetilde{h}_1, \rho \mid \widetilde{g}^{2n} = \rho^2 = 1, \widetilde{h}_1^2 = \rho, \widetilde{h}_1\widetilde{g} = \widetilde{g}^{-1}\widetilde{h}_1,\ \rho\ -\ \text{централен}\rangle.$$

В частост, виждаме, че 2-кокласа съответстващ на

$$1 \longrightarrow \mu_2 \cong \langle\rho\rangle \longrightarrow \widetilde{G} \longrightarrow G \cong D_{4n} \longrightarrow 1 \tag{2.12}$$

е нетривиален, докато е известно, че корестрикцията на 2-кокласа съответстващ на

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{H} \longrightarrow H \cong D_{2n} \longrightarrow 1 \tag{2.13}$$

е тривиален.

Нека M/k е разширение на Галоа с група на Галоа $G \cong D_{4n}$, нека $K = M^H = k(\sqrt{a_1})$ е неподвижното подполе на H, и нека $L = M^{\langle g^4\rangle} = k(\sqrt{r(\alpha+\beta\sqrt{a_1})}, \sqrt{b})$ е неподвижното подполе на подгрупата $\langle g^4\rangle$, където $\alpha^2 - a_1\beta^2 = a_1 b, r, \beta \in k^*, \alpha \in k$ и $\mathrm{Gal}(L/k) \cong D_8$.

Теорема 2.6.1. ([Mi4, Proposition 5.1]) *Препятствието на задачата за вложимост* $(M/k, \widetilde{G}, \mu_2)$ *е* $(b,-1) \in \mathrm{Br}_2(k)$.

Доказателство: С помощта на [Fr, Th. 6 (i)] и [KR, Lemma 2.3] можем да пресметнем усуканата квадратична форма q_t на индуцираната квадратична форма q:

$$q_t =< 2\mathrm{tr}(a), 2\mathrm{tr}(a)N(a)a_1, -2\mathrm{tr}(a)b, -2\mathrm{tr}(a)bN(a)a_1 >,$$

където $a \in K$ е описан в [Fr, Ex. 5]. Инвариантите на Хасе-Вит за q и q_t са съответно $(-1,-1)$ и $(-1,-1)(b,-N(a)a_1)$. Според [Fr, (7.10)], препятствието на задачата за вложимост $(M/K, \widetilde{H}, \mu_2)$ е $(a,b)(\eta, r(\alpha+\beta\sqrt{a_1}))$. Да отбележим, че трябва да имаме $\mathrm{cor}_{K/k}((a,b)(\eta, r(\alpha+\beta\sqrt{a_1}))) = (N(a),b)(\eta, a_1 b) = 1$, понеже корестрикцията на 2-кокласа съответстващ на (2.13) е тривиална. Накрая, от теорема 2.4.6 получаваме, че препятствието е

$$\mathrm{hw}(q)\mathrm{hw}(q_t)(a_1, sp(g))(b, sp(h_1)) = (b,-a_1)(\eta, a_1 b)(a_1, -\eta)(b,\eta) = (b,-1).$$

Глава 3
Препятствия за реализиране на малки 2-групи като групи на Галоа

Препятствията за реализирането на групи от ред 2^n при $n \leq 4$ са изложени в работата [Ми]. За да бъдат пресметнати препятствията на групи от ред 32 и по-висок, обаче е необходимо пълното описание на разширенията на Галоа, които реализират групите от ред 16. Този проблем до голяма степен е решен в статията на Ледет [Le3], където се показва, че ако една група има препятствие, което е произведение на два кватернионни класа, то е възможно пълното описание на разширенията на Галоа, които я реализират. Тъй като кватернионната група от ред 16 има препятствие, което е произведение на три кватернионни класа, то такова описание не е възможно в общия случай. Ние, обаче сме намерили редица частни случаи, в които това описание е възможно. Първите три точки от параграф 3.1 са посветени на тези резултати, публикуване в [Mi9].

В точка 3.1.4 показваме начина, по който можем да пресметнем явно препятствията над локални полета. Тези резултати са публикувани в [Mi8].

Параграф 3.2 е посветен на реализирането на групите от ред 32 като групи на Галоа. Тези резултати са публикувани в статията [Mi5] (също така са доразвити в [Mi7]), където за първи път систематично са описани препятствията на всички неабелови групи от ред 32. Има още няколко други статии, където са пресметнати препятствията на някои групи от редове 32 и 64, например [Sm, ST, GS1, GS2].

3.1 Групи от редове 8 и 16 като групи на Галоа

Добре известно е, че съществуват 2 неабелови групи и 3 абелови групи от ред 8. Диедралната група D_8 от ред 8 (означавана още с D_4) се поражда от елементи σ и

τ със съотношения $\sigma^4 = \tau^2 = 1$ и $\tau\sigma = \sigma^3\tau$. Множеството от всички D_8 разширения се описва така: Нека a и b са квадратично независими над k такива, че $(a, ab) = 1 \in \mathrm{Br}(k)$, и нека за $\alpha_1 \in k$ и $\alpha_2 \in k^*$ имаме $ab = \alpha_1^2 - a\alpha_2^2$. Тогава

$$K/k = k(\sqrt{r(\alpha_1 - \alpha_2\sqrt{a})}, \sqrt{b})/k$$

е разширение на Галоа с група на Галоа D_8, за всяко $r \in k^*$. Полагаме $\alpha = \alpha_1 - \alpha_2\sqrt{a}$ и $\alpha' = \alpha_1 + \alpha_2\sqrt{a}$. Тогава можем да считаме, че σ и τ действат по следния начин:

$$\begin{aligned} \sigma &: \sqrt{r\alpha} \mapsto \sqrt{r\alpha'},\ \sqrt{r\alpha'} \mapsto -\sqrt{r\alpha},\ \sqrt{b} \mapsto \sqrt{b}; \\ \tau &: \sqrt{r\alpha} \mapsto \sqrt{r\alpha},\ \sqrt{r\alpha'} \mapsto -\sqrt{r\alpha'},\ \sqrt{b} \mapsto -\sqrt{b}. \end{aligned}$$

Кватернионната група Q_8 от ред 8 се поражда от елементи σ и τ такива, че $\sigma^4 = \tau^4 = 1, \sigma^2 = \tau^2$ и $\tau\sigma = \sigma^3\tau$. На нас няма да ни е нужно описанието на Q_8 разширения, така че ще го пропуснем. Това описание може да бъде намерено в [Wi].

Групата $C_4 \times C_2$ се поражда от два елемента, да речем ρ_1 и ρ_2 със съотношения $\rho_1^4 = \rho_2^2 = 1$ и $\rho_1\rho_2 = \rho_2\rho_1$. Множеството от всички $C_4 \times C_2$ разширения се описва така: Нека a и b са квадратично независими над k такива, че $(a, a) = 1 \in \mathrm{Br}(k)$ и нека $c \in k^*$ е такова, че $a = 1 + c^2$. Тогава

$$K/k = k(\sqrt{r(a + \sqrt{a})}, \sqrt{b})/k$$

е $C_4 \times C_2$ разширение, за всяко $r \in k^*$. Можем да считаме, че ρ_1 и ρ_2 действат по следния начин:

$$\begin{aligned} \rho_1 &: \sqrt{r(a + \sqrt{a})} \mapsto \sqrt{r(a - \sqrt{a})},\ \sqrt{b} \mapsto \sqrt{b}; \\ \rho_2 &: \sqrt{r(a + \sqrt{a})} \mapsto \sqrt{r(a + \sqrt{a})},\ \sqrt{b} \mapsto -\sqrt{b}. \end{aligned}$$

Останалите две абелови групи от ред 8 са цикличната група C_8 и елементарната абелова група C_2^3.

Неабеловите групи от ред 16 са 9 на брой: M_{16}-*модулярната* група, SD_{16}-*полудиедралната (квазидиедралната)* група (означавана в различните източници още с SD_8 и QD_8), D_{16}-*диедралната* група (означавана още с D_8), Q_{16}-*кватернионната* група, $Q \curlywedge C$-*пулбекът (директно произведение с обединена факторгрупа)* на хомоморфизмите $Q_8 \mapsto C_2$ и $C_4 \mapsto C_2$, $D \curlywedge C$- пулбекът на хомоморфизмите $D_8 \mapsto C_2$ и

$C_4 \mapsto C_2$, *DC-централното произведение* на D_8 и C_4, $D_8 \times C_2$ и $Q_8 \times C_2$. Техните представяния чрез пораждащи са:

$$M_{16} \cong \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \tau\sigma = \sigma^5\tau \rangle,$$
$$SD_{16} \cong \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle,$$
$$D_{16} \cong \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle,$$
$$Q_{16} \cong \langle \sigma, \tau \mid \sigma^8 = 1, \tau^2 = \sigma^4, \tau\sigma = \sigma^{-1}\tau \rangle,$$
$$Q \leftthreetimes C \cong \langle \sigma, \tau \mid \sigma^4 = \tau^4 = 1, \tau\sigma = \sigma^3\tau \rangle,$$
$$D \leftthreetimes C \cong \langle \sigma, \tau, \rho \mid \sigma^4 = \tau^2 = \rho^2 = 1, \tau\sigma = \sigma^3\tau\rho, [\sigma, \rho] = [\tau, \rho] = 1 \rangle,$$
$$DC \cong \langle \sigma, \tau, \rho \mid \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau, \sigma^2 = \rho^2, [\sigma, \rho] = [\tau, \rho] = 1 \rangle.$$

3.1.1 Разширения на Галоа, реализиращи групата $D \leftthreetimes C$

Нека k е поле с характеристика различна от 2, нека a и b са квадратично независими над k. Нека $(a, a) = 1 \in \mathrm{Br}(k)$ и да предположим, че $\alpha_1, \alpha_2 \in k$ са такива, че $\alpha_1^2 - a\alpha_2^2 = a$. Полагаме $\alpha = \alpha_1 - \alpha_2\sqrt{a}$ и $\alpha' = \alpha_1 + \alpha_2\sqrt{a}$. Тогава $\alpha\alpha' = a$ и $K_1/k = k(\sqrt{r\alpha}, \sqrt{b})/k$ е $C_4 \times C_2$ разширение за всяко $r \in k^*$. Обратно, всички $C_4 \times C_2$ се описват по този начин. Групата $C_4 \times C_2$ се поражда от елементи σ и τ такива, че $\sigma^4 = \tau^2 = 1$ и техните действия са:

$$\begin{aligned} \sigma &: \sqrt{r\alpha} \mapsto \sqrt{r\alpha'},\ \sqrt{r\alpha'} \mapsto -\sqrt{r\alpha},\ \sqrt{b} \mapsto \sqrt{b}; \\ \tau &: \sqrt{r\alpha} \mapsto \sqrt{r\alpha},\ \sqrt{r\alpha'} \mapsto \sqrt{r\alpha'},\ \sqrt{b} \mapsto -\sqrt{b}. \end{aligned}$$

Тогава препятствието на задачата за вложимост $(K_1/k, D \leftthreetimes C, \mu_2)$ зададена с разширението K_1/k и груповото разширение

$$1 \longrightarrow \langle z \rangle \longrightarrow D \leftthreetimes C \underset{\substack{x \mapsto \sigma \\ y \mapsto \tau}}{\longrightarrow} C_4 \times C_2 \longrightarrow 1$$

е $(a, b) \in \mathrm{Br}(k)$. Да предположим, че $(a, b) = 1$, така че съществуват $\beta_1, \beta_2 \in k$, за които $a = \beta_1^2 - b\beta_2^2$. Полагаме $\beta = \beta_1 - \beta_2\sqrt{b}$ и $\beta' = \beta_1 + \beta_2\sqrt{b}$. Тогава $\beta\beta' = a$ и $K_2/k = k(\sqrt{s\beta}, \sqrt{ab})/k$ е D_8 разширение за всяко $s \in k^*$. Групата D_8 се поражда от елементи σ_1 и τ_1 със съотношения $\sigma_1^2 = \tau_1^2 = 1, |\sigma_1\tau_1| = 4$, и техните действия са:

$$\begin{aligned} \sigma_1 &: \sqrt{s\beta} \mapsto -\sqrt{s\beta},\ \sqrt{s\beta'} \mapsto \sqrt{s\beta'},\ \sqrt{ab} \mapsto -\sqrt{ab}; \\ \tau_1 &: \sqrt{s\beta} \mapsto \sqrt{s\beta'},\ \sqrt{s\beta'} \mapsto \sqrt{s\beta},\ \sqrt{ab} \mapsto -\sqrt{ab}; \\ \sigma_1\tau_1 &: \sqrt{s\beta} \mapsto \sqrt{s\beta'},\ \sqrt{s\beta'} \mapsto -\sqrt{s\beta},\ \sqrt{ab} \mapsto \sqrt{ab}. \end{aligned}$$

Препятствието на задачата за вложимост зададена с K_2/k и груповото разширение

$$1 \longrightarrow \langle x^2 \rangle \longrightarrow D \leftthreetimes C \underset{\substack{x\mapsto\sigma_1\\ y\mapsto\tau_1}}{\longrightarrow} D_8 \longrightarrow 1$$

е $(a,a) \in \mathrm{Br}(k)$.

Ако ни е дадено, че $(a,a) = (a,b) = 1$, можем да построим композита $K = K_1K_2 = k(\sqrt{r\alpha}, \sqrt{b})k(\sqrt{s\beta}, \sqrt{ab})$. Ще покажем,че K/k е $D \leftthreetimes C$ разширение. Тъй като полето K зависи от r и s, по този начин ще получим описание на всички $D \leftthreetimes C$ разширения.

Очевидно, K/k е разширение на Галоа. Нека сега $x, y \in G = \mathrm{Gal}(K/k)$ са такива, че техните ограничения върху K_1 и K_2 са:

$$x|_{K_1} = \sigma, x|_{K_2} = \sigma_1; y|_{K_1} = \tau, y|_{K_2} = \tau_1.$$

Действията на x и y са:

$$\begin{aligned}
x \ &: \ \sqrt{r\alpha} \mapsto \sqrt{r\alpha'},\ \sqrt{r\alpha'} \mapsto -\sqrt{r\alpha},\ \sqrt{b} \mapsto \sqrt{b},\\
&\quad \sqrt{s\beta} \mapsto -\sqrt{s\beta},\ \sqrt{s\beta'} \mapsto \sqrt{s\beta'},\ \sqrt{ab} \mapsto -\sqrt{ab};\\
y \ &: \ \sqrt{r\alpha} \mapsto \sqrt{r\alpha},\ \sqrt{r\alpha'} \mapsto \sqrt{r\alpha'},\ \sqrt{b} \mapsto -\sqrt{b},\\
&\quad \sqrt{s\beta} \mapsto \sqrt{s\beta'},\ \sqrt{s\beta'} \mapsto \sqrt{s\beta},\ \sqrt{ab} \mapsto -\sqrt{ab}.
\end{aligned}$$

По този начин получихме това, което ни трябваше: $|x| = 4, |y| = 2$ и елементите на K_2 са неподвижни под действието на x^2. Да положим $z = [y,x]$. Действието на z е:

$$\begin{aligned}
z \ &: \ \sqrt{r\alpha} \mapsto \sqrt{r\alpha},\ \sqrt{r\alpha'} \mapsto \sqrt{r\alpha'},\ \sqrt{b} \mapsto \sqrt{b},\\
&\quad \sqrt{s\beta} \mapsto -\sqrt{s\beta},\ \sqrt{s\beta'} \mapsto -\sqrt{s\beta'},\ \sqrt{ab} \mapsto \sqrt{ab}.
\end{aligned}$$

Следователно, $|z| = 2$ и елементите на K_1 са неподвижни под действието на z. Също така, лесно е да се проверят съотношенията $[z,x] = [z,y] = 1$. Оттук получаваме, че K/k е $D \leftthreetimes C$ разширение и всички $D \leftthreetimes C$ разширения се описват по този начин.

3.1.2 Разширения на Галоа, реализиращи диедралната и полудиедралната група от ред 16

Тук ще изложим описание на разширенията на Галоа, реализиращи групите QD_{16} и D_{16}, като групи на Галоа. С QD_{16} означаваме квазидиедралната група породена от елементи u и v такива, че $u^8 = 1, v^2 = u^4$ и $vu = u^3v$. С D_{16} означаваме

диедралната група от ред 16, породена от елементи u и v със съотношения $u^8 = v^2 = 1$ и $vu = u^{-1}v$.

Нека $a, b \in k^*$ са квадратично независими, т.е. a, b и ab не са в k^2. Нека също $(a, ab) = 1 \in \mathrm{Br}(k)$, т.е. D_8 се реализира като група на Галоа. Тогава съществуват $\alpha, \beta \in k^*$, за които $\alpha^2 - a\beta^2 = ab$. Следователно, всички D_8 разширения са $\{k(\sqrt{r(\alpha + \beta\sqrt{a})}, \sqrt{b})/k,\ r \in k^*\}$. Означаваме

$$\varphi = \sqrt{r(\alpha + \beta\sqrt{a})} \text{ and } \psi = \sqrt{r(\alpha - \beta\sqrt{a})} = \frac{\alpha - \beta\sqrt{a}}{\sqrt{ab}}\varphi,$$

където D_8 е породена от два елемента σ и τ такива, че

$$\sigma : \varphi \mapsto \psi, \sqrt{b} \mapsto \sqrt{b}; \quad \tau : \varphi \mapsto \varphi, \sqrt{b} \mapsto -\sqrt{b}.$$

Да отбележим още, че

$$\sigma : \psi \mapsto -\varphi, \quad \tau : \psi \mapsto -\psi.$$

От [Le3] са известни следните теореми, даващи описание на QD_{16} и D_{16} разширенията:

Теорема 3.1.1. *Нека $\alpha \neq 0$. Задачата за вложимост зададена с $K/k = k(\varphi, \sqrt{b})/k$ и груповото разширение*

$$1 \longrightarrow \mu_2 \longrightarrow QD_{16} \underset{\substack{u \mapsto \sigma \\ v \mapsto \tau}}{\longrightarrow} D_8 \longrightarrow 1 \tag{3.1}$$

е разрешима тогава и само тогава, когато квадратичните форми $\langle b, 2r\alpha, 2br\alpha\rangle$ и $\langle a, 2, 2a\rangle$ са еквивалентни над k. Ако тази еквивалентност се изразява чрез матрицата $\mathbf{P}$:

$$\mathbf{P}^t\langle b, 2r\alpha, 2br\alpha\rangle\mathbf{P} = \langle a, 2, 2a\rangle,$$

можем да считаме, че $\det \mathbf{P} = a/br\alpha$ *и да получим всички решения*

$$K(\sqrt{s\omega_{QD}})/k = k(\sqrt{s\omega_{QD}}, \sqrt{b})/k, \quad s \in k^*,$$

където

$$\begin{aligned}\omega_{QD} = 1 &+ p_{11}\sqrt{b}/\sqrt{a} + \frac{1}{2}(p_{22} + p_{23}/\sqrt{a} - p_{32}\sqrt{b} + p_{33}\sqrt{b}/\sqrt{a})\varphi \\ &+ \frac{1}{2}(p_{22} - p_{23}/\sqrt{a} + p_{32}\sqrt{b} + p_{33}\sqrt{b}/\sqrt{a})\psi.\end{aligned}$$

Теорема 3.1.2. *Нека $\alpha \neq 0$. Задачата за вложимост зададена с $K/k = k(\varphi, \sqrt{b})/k$ и груповото разширение*

$$1 \longrightarrow \mu_2 \longrightarrow D_{16} \underset{\substack{u\mapsto\sigma \\ v\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1 \tag{3.2}$$

е разрешима тогава и само тогава, когато квадратичните форми $\langle b, r\alpha, br\alpha\rangle$ и $\langle ab, 2b, 2a\rangle$ са еквивалентни над k. Ако тази еквивалентност се изразява чрез матрицата $\mathbf{P}$:

$$\mathbf{P}^t\langle b, r\alpha, br\alpha\rangle\mathbf{P} = \langle ab, 2b, 2a\rangle,$$

можем да считаме, че $\det \mathbf{P} = 2a/r\alpha$ *и да получим всички решения*

$$K(\sqrt{s\omega_D})/k = k(\sqrt{s\omega_D}, \sqrt{b})/k, \quad s \in k^*,$$

където

$$\omega_D = 1 - p_{11}/\sqrt{a} + \frac{1}{2}(p_{32} + p_{23}/\sqrt{a})\varphi + \frac{1}{2}(p_{22}/\sqrt{b} - p_{33}\sqrt{b}/\sqrt{a})\psi.$$

Препятствията на задачата за вложимост зададени с груповите разширения (3.1) и (3.2) са, съответно, $(-b, -2r\alpha)(-a, -2) \in \mathrm{Br}(k)$ и $(-ab, -2a)(-b, -r\alpha) \in \mathrm{Br}(k)$. В частия случай $b = -1$ можем да считаме, че всички D_8 разширения са $k(\sqrt[4]{a}, i)/k$ и действието на пораждащите на D_8 е

$$\sigma : \sqrt[4]{a} \mapsto \sqrt[4]{a}i, \sigma : i \mapsto i; \quad \tau : \sqrt[4]{a} \mapsto \sqrt[4]{a}, \tau : i \mapsto -i.$$

Теорема 3.1.3. *Задачата за вложимост зададена с $K/k = k(\sqrt[4]{a}, i)/k$, имащо група на Галоа D_8, и груповото разширение*

$$1 \longrightarrow \mu_2 \longrightarrow QD_{16} \underset{\substack{u\mapsto\sigma \\ v\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1 \tag{3.1}$$

е разрешима тогава и само тогава, когато

$$\exists p, q \in k : p^2 + aq^2 = -2.$$

Решенията са:

$$K(\sqrt{r\omega_{QD}})/k = k(\sqrt{r\omega_{QD}}, i)/k, \quad r \in k^*,$$

където $\omega_{QD} = (1 + i)(p + qi\sqrt{a})\sqrt[4]{a}$.

Теорема 3.1.4. *Задачата за вложимост зададена с $K/k = k(\sqrt[4]{a}, i)/k$, имащо група на Галоа D_8, и груповото разширение*

$$1 \longrightarrow \mu_2 \longrightarrow D_{16} \underset{\substack{u\mapsto\sigma\\ v\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1 \tag{3.2}$$

е разрешима тогава и само тогава, когато

$$\exists p, q \in k : p^2 - aq^2 = 2.$$

Решенията са:

$$K(\sqrt{r\omega_D})/k = k(\sqrt{r\omega_D}, i)/k, \quad r \in k^*,$$

където $\omega_D = (p + q\sqrt{a})\sqrt[4]{a}$.

Ще продължим с описанието на полудиедралните разширения. Полудиедралната група SD_{16} от ред 16 е породена от елементи u и v със съотношения $u^8 = v^2 = 1$ и $vu = u^3v$. Разбира се, групата SD_{16} е изоморфна на квазидиедралната група QD_{16}. Груповите разширения (3.1) и (3.3), обаче не са еквивалентни, откъдето препятствията и описанието на разширенията на Галоа за тези две групи се различават съществено. Препятствието за влагането на D_8 разширение в SD_{16} разширение е $(a, -2)(-b, 2r\alpha) = (-ab, -2)(-b, -r\alpha) \in \mathrm{Br}(k)$, както е пресметнато в [Le1, Mi1].

Следователно, ако $\alpha \neq 0$, задачата за вложимост зададена с $K/k = k(\varphi, \sqrt{b})/k$ и груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow SD_{16} \underset{\substack{u\mapsto\sigma\\ v\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1 \tag{3.3}$$

е разрешима тогава и само тогава, когато формата $\langle b, r\alpha, br\alpha\rangle$ е еквивалентна на $\langle ab, 2, 2ab\rangle$ над k. Нека тази еквивалентност се изразява чрез матрицата $\mathbf{P}$:

$$\mathbf{P}^t\langle b, r\alpha, br\alpha\rangle\mathbf{P} = \langle ab, 2, 2ab\rangle,$$

и да предположим, че $\det \mathbf{P} = 2a/r\alpha$. Дефинираме матрица $\mathbf{P}'$:

$$\mathbf{P}' = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 1/2 & -1/2 \end{pmatrix} \langle\sqrt{b}, 1, \sqrt{b}\rangle\mathbf{P}\langle 1/\sqrt{b}, 1, 1/\sqrt{b}\rangle.$$

Можем да считаме, че $\det \mathbf{P}' = a/r\alpha$ и да означим $\alpha' = \alpha/\sqrt{b}, \beta' = \beta/\sqrt{b}$. Полагаме

$$\omega = 1 + p'_{11}/\sqrt{a} + \frac{1}{2}[(p'_{22} - p'_{32}) + (p'_{23} + p'_{33})/\sqrt{a}]\varphi$$
$$+ \frac{1}{2}[(p'_{22} + p'_{32}) - (p'_{23} - p'_{33})/\sqrt{a}]\frac{\alpha' - \beta'\sqrt{a}}{\sqrt{a}}\varphi,$$

където p'_{ij} са елементите на матрицата $\mathbf{P}'$. Тогава

$$\omega = 1 - p_{11}/\sqrt{a} + \frac{1}{2}[\sqrt{b}p_{32} + p_{23}/\sqrt{ab}]\varphi + \frac{1}{2}[p_{22} - p_{33}/\sqrt{a}]\frac{\alpha - \beta\sqrt{a}}{\sqrt{a}\sqrt{b}}\varphi,$$

откъдето $K(\sqrt{\omega})/k(\sqrt{b})$ е C_8 разширение. Сега можем да положим

$$\omega_{SD} = \sigma\omega = 1 + p_{11}/\sqrt{a} + \frac{1}{2}(p_{32}\sqrt{b} - p_{23}/\sqrt{ab})\psi - \frac{1}{2}[p_{22} + p_{33}/\sqrt{a}]\varphi.$$

Тогава $\tau\omega_{SD} = \omega_{SD}$, значи $K(\sqrt{\omega}_{SD})/k$ е нормално, и понеже про-образът на $\tau\sigma$ в групата на Галоа е от ред 4, тази група е точно SD_{16}. Така получаваме следната

Теорема 3.1.5. ([Mi9, Theorem 2.5]) *Нека $\alpha \neq 0$. Задачата за вложимост зададена с $K/k = k(\varphi, \sqrt{b})/k$ и груповото разширение*

$$1 \longrightarrow \mu_2 \longrightarrow SD_{16} \underset{\substack{u\mapsto\sigma \\ v\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1 \tag{3.3}$$

е разрешима тогава и само тогава, когато квадратичните форми $\langle b, r\alpha, br\alpha\rangle$ и $\langle ab, 2, 2ab\rangle$ са еквивалентни над k. Ако тази еквивалентност се изразява чрез матрицата $\mathbf{P}$:

$$\mathbf{P}^t\langle b, r\alpha, br\alpha\rangle\mathbf{P} = \langle ab, 2, 2ab\rangle,$$

можем да считаме, че $\det \mathbf{P} = 2a/r\alpha$ *и да получим всички решения*

$$K(\sqrt{s\omega_{SD}})/k = k(\sqrt{s\omega_{SD}}, \sqrt{b})/k, \quad s \in k^*,$$

където ω_{SD} е както по-горе.

За $b = -1$ имаме:

Теорема 3.1.6. ([Mi9, Theorem 2.6]) *Задачата за вложимост зададена с $K/k = k(\sqrt[4]{a}, i)/k$, имащо група на Галоа D_8, и груповото разширение*

$$1 \longrightarrow \mu_2 \longrightarrow SD_{16} \underset{\substack{u\mapsto\sigma \\ v\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1 \tag{3.3}$$

е разрешима тогава и само тогава, когато

$$\exists p, q \in k : p^2 - aq^2 = -2.$$

Решенията са:

$$K(\sqrt{r\omega_{SD}})/k = k(\sqrt{r\omega_{SD}}, i)/k, \quad r \in k^*,$$

където $\omega_{SD} = (p + q\sqrt{a})\sqrt[4]{a}$.

3.1.3 Разширения на Галоа, реализиращи кватернионната група от ред 16

В тази точка ще разгледаме три вида разширения на Галоа, имащи кватернионната група Q_{16} като група на Галоа. Нека кватернионната група е породена от елементи u и v със съотношения $u^8 = 1, v^2 = u^4$ и $vu = u^{-1}v$. Тогава задачата за вложимост зададена с $K/k = k(\varphi, \sqrt{b})/k$ и груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow Q_{16} \underset{v \mapsto \tau}{\overset{u \mapsto \sigma}{\longrightarrow}} D_8 \longrightarrow 1 \tag{3.4}$$

е разрешима тогава и само тогава, когато $(ab, 2)(b, -1)(-b, r\alpha) = 1 \in \mathrm{Br}(k)$ (виж [Le1]).

Ще разгледаме три частни случая, когато един от елементите a, b, ab е сума на два квадрата. Ще използваме следния аргумент: Ако една група от ред 16 има експонента 8 и

$$1 \longrightarrow \mu_2 \longrightarrow G \underset{v \mapsto \tau}{\overset{u \mapsto \sigma}{\longrightarrow}} D_8 \longrightarrow 1$$

е неразцепимо разширение, то G е изоморфна на една от групите QD_{16} (SD_{16}), D_{16} или Q_{16}. Нещо повече, групата G се определя еднозначно от редовете на про-образите u, v, uv на пораждащите $\sigma, \tau, \sigma\tau \in D_8$.

Теорема 3.1.7. ([Mi9, Proposition 3.1]) *Нека $(a, -1) = 1 \in \mathrm{Br}(k)$, т.е. $\exists x, y \in k$ такива, че $a = x^2 - ay^2$. Тогава всички решения на задачата за вложимост зададена с $K/k = k(\varphi, \sqrt{b})/k$ и груповото разширение* (3.4) *са*

$$K(\sqrt{s(x + y\sqrt{a})\omega_{QD}})/k = k(\sqrt{s(x + y\sqrt{a})\omega_{QD}}, \sqrt{b})/k, \quad s \in k^*,$$

където ω_{QD} е както в теорема 3.1.1 или 3.1.3.

Доказателство: Препятствието е

$$(ab, 2)(b, -1)(-b, r\alpha) = (ab, -2)(ab, -1)(b, -1)(-b, r\alpha) = (ab, -2)(-b, r\alpha) \in \mathrm{Br}(k),$$

което е точно препятствието за реализирането на QD_{16}.

Нека сега $(ab, -2)(-b, r\alpha) = 1 \in \mathrm{Br}(k)$ и ω_{QD} задава едно QD_{16} разширение. Тогава $\sigma\tau\omega_{QD} = \omega_{QD}$, и полагаме $\omega_Q = (x + y\sqrt{a})\omega_{QD}$. Имаме, че $\sigma\tau\omega_Q = a_{\sigma\tau}^2\omega_Q$, където

$$a_{\sigma\tau} = \frac{\sqrt{a}}{x + y\sqrt{a}}.$$

Оттук $K(\sqrt{\omega}_Q)/k$ е разширение на Галоа и про-образите на $\sigma\tau$ и τ в групата на Галоа G са от ред 4, понеже $a_{\sigma\tau}\sigma\tau a_{\sigma\tau} = -1$. Следователно, $K(\sqrt{s\omega_Q})/k$ е Q_{16} разширение. □

Теорема 3.1.8. ([Mi9, Proposition 3.2]) *Нека* $(b,-1) = 1 \in \mathrm{Br}(k)$, *т.е.* $\exists x, y \in k$ *такива, че* $b = x^2 - by^2$. *Тогава всички решения на задачата за вложимост зададена с* $K/k = k(\varphi, \sqrt{b})/k$ *и груповото разширение* (3.4) *са*

$$K(\sqrt{s(x+y\sqrt{b})\omega_D})/k = k(\sqrt{s(x+y\sqrt{b})\omega_D}, \sqrt{b})/k, \quad s \in k^*,$$

където ω_D *е както в теорема 3.1.2 или 3.1.4.*

Доказателство: Препятствието е

$$(ab,2)(b,-1)(-b,r\alpha) = (ab,2)(-b,r\alpha) \in \mathrm{Br}(k),$$

което съвпада с препятствието за реализирането на D_{16}.

Нека сега $(ab,2)(-b,r\alpha) = 1 \in \mathrm{Br}(k)$ и ω_D задава някое D_{16} разширение. Тук $\tau\omega_D = \omega_D, \sigma\tau\omega_D = a_{\sigma\tau}^2\omega_D$; про-образите на τ и σ в D_{16} са от ред 2, и ще положим $\omega_Q = (x+y\sqrt{b})\omega_D$. Сега имаме, че $\tau\omega_Q = a_\tau^2\omega_Q$ и $\sigma\tau\omega_Q = a'^2_{\sigma\tau}\omega_Q$, където

$$a_\tau = \frac{\sqrt{b}}{x+y\sqrt{b}}, \quad a'_{\sigma\tau} = a_\tau a_{\sigma\tau}.$$

От $a_\tau\tau a_\tau = -1, a_{\sigma\tau}\sigma\tau a_{\sigma\tau} = 1$ получаваме $a'_{\sigma\tau}\sigma\tau a'_{\sigma\tau} = a_\tau\tau a_\tau a_{\sigma\tau}\sigma\tau a_{\sigma\tau} = -1$, значи про-образите на τ и $\sigma\tau$ в G имат ред 4. Следователно, $K(\sqrt{s\omega_Q})/k$ е Q_{16} разширение. □

Теорема 3.1.9. ([Mi9, Proposition 3.3]) *Нека* $(ab,-1) = 1 \in \mathrm{Br}(k)$, *т.е.* $\exists x, y \in k$ *такива, че* $ab = x^2 - aby^2$. *Тогава всички решения на задачата за вложимост зададена с* $K/k = k(\varphi, \sqrt{b})/k$ *и груповото разширение* (3.4) *са*

$$K(\sqrt{s(x+y\sqrt{ab})\omega_{SD}})/k = k(\sqrt{s(x+y\sqrt{ab})\omega_{SD}}, \sqrt{b})/k, \quad s \in k^*,$$

където ω_{SD} *е както в теорема 3.1.5 или 3.1.6.*

Доказателство: Препятствието е

$$(-ab,-2)(ab,-1)(-1,-2)(b,-1)(-b,r\alpha) = (-ab,-2)(-b,-r\alpha) \in \mathrm{Br}(k),$$

което е точно препятствието за реализирането на SD_{16}. Нека сега $(-ab,-2)(-b,-r\alpha) = 1 \in \mathrm{Br}(k)$ и ω_{SD} задава някое SD_{16} разширение. Тук $\tau\omega_{SD} = \omega_{SD}, \sigma\tau\omega_{SD} = a_{\sigma\tau}^2\omega_{SD}$;

про-образът на τ е от ред 2 и про-образът на $\sigma\tau$ е от ред 4 (в SD_{16}), и полагаме $\omega_Q = (x + y\sqrt{ab})\omega_{SD}$. Сега имаме, че $\tau\omega_Q = a_\tau^2\omega_Q$ и $\sigma\tau\omega_Q = a_{\sigma\tau}^2\omega_Q$, където

$$a_\tau = \frac{\sqrt{ab}}{x + y\sqrt{ab}}.$$

От $a_\tau \tau a_\tau = -1$ и $a_{\sigma\tau}\sigma\tau a_{\sigma\tau} = -1$ получаваме, че про-образите на τ и $\sigma\tau$ в G имат ред 4. Следователно, $K(\sqrt{s\omega_Q})/k$ е Q_{16} разширение. □

Нека $b \in k^* \setminus (k^*)^2$, нека $L = k(\sqrt{b})$, и нека L съдържа примитивен 8-ми корен на единицата ζ. Нашата цел оттук до края на тази точка ще бъде да опишем всички разширения на Галоа M/k, които са решения на задачата за вложимост зададена чрез L/k и груповото разширение

$$1 \longrightarrow C_8 = \langle u \rangle \longrightarrow Q_{16} \longrightarrow C_2 \cong \mathrm{Gal}(L/k) \longrightarrow 1, \tag{3.5}$$

където Q_{16} се поражда от u и v със съотношенията описани в началото на тази точка.

Да предположим сега, че M е циклично разширение на L от степен 8. Тогава $M = L(\omega^{1/8})$ според Кумеровата теория. Ако $\mathrm{Gal}(L/k) = \{1, v\}$, то M е разширение на Галоа над k тогава и само тогава, когато $v(\omega) = \omega^t\beta^8$, където $\beta \in L^*$ и $t^2 \equiv 1 \pmod 8$. Това означава, че трябва да намерим явно описание на елемента ω.

Ако G е група от ред 16, която съдържа циклична подгрупа $\langle u \rangle$ от ред 8, то G се поражда от елементи u и v такива, че

1. $|u| = 8,\ v \notin \langle u \rangle$;
2. $vuv^{-1} = u^j,\ v^2 = u^l$;
3. $j^2 \equiv 1 \pmod 8,\ l(j-1) \equiv 0 \pmod 8$.

Добре известно е, че $G \cong Q_{16}$ тогава и само тогава, когато $j \equiv -1$ и $l \equiv 4 \pmod 8$. Тъй като $\zeta \in L$, имаме $v(\zeta) = \zeta^r$, където r е цяло число такова, че $\gcd(r, 8) = 1$, т.е. r е нечетно. Означаваме $\zeta = \frac{\sqrt{2}}{2}(1 + i)$, където $i = \sqrt{-1}$. Тогава са възможни следните четири случая:

1. $r \equiv 1$, т.е. $\zeta \in k$;
2. $r \equiv -1$, т.е. $\sqrt{2} \in k$ и $b =_2 -1$;
3. $r \equiv 5$, т.е. $i \in k$ и $b =_2 2$;

4. $r \equiv -5$, т.е. $\sqrt{-2} \in k$ и $b =_2 -1 =_2 2$.

Задачата за вложимост зададена с $L/k = k(\sqrt{b})/k$ и груповото разширение (3.5) е разрешима тогава и само тогава, когато съществува $a \in k$ такова, че a и b са квадратично независими над k, $(a, ab) = 1 \in Br(k)$ и $(ab, 2)(b, b)(-b, x) = 1 \in Br(k)$ за някои $x \in k$ (виж [MZ4]). Означаваме с N норменото изображение $N_{L/k} : L \to k$. Да разгледаме сега всеки от четирите случая.

Ако $r \equiv 1$, т.е. $\zeta \in k$, то задачата за вложимост зададена с L/k и (3.5) е разрешима тогава и само тогава, когато съществува a такова, че $(a, b) = 1$, т.е. $\exists \gamma \in L$, за което $a = N(\gamma)$ и b са квадратично независими. Описанието на всички Q_{16} разширения е дадено в теорема 3.1.14.

Ако $r \equiv -1$, т.е. $\sqrt{2} \in k$ и $b =_2 -1$, то задачата за вложимост е разрешима тогава и само тогава, когато съществува a такова, че a и -1 са квадратично независими и $(-1, -1) = 1$, т.е. $-1 = N(\gamma)$ за някое $\gamma \in L$. Описанието на всички Q_{16} разширения е дадено в теорема 3.1.15.

Ако $r \equiv 5$, т.е. $i \in k$ и $b =_2 2$, то задачата за вложимост е разрешима тогава и само тогава, когато съществува a такова, че $(a, 2) = 1$, още $a = N(\gamma)$ и 2 са квадратично независими. Описанието на всички Q_{16} разширения е дадено в теорема 3.1.16.

Ако $r \equiv -5$, т.е. $\sqrt{-2} \in k$ и $b =_2 -1 =_2 2$, то задачата за вложимост е разрешима тогава и само тогава, когато съществува a такова, че $(a, 2) = 1$, още $a = N(\gamma)$ и 2 са квадратично независими. Описанието на всички Q_{16} разширения е дадено в теорема 3.1.17.

Сега ще изложим няколко леми, които се явяват частни случаи на резултати, получени в [HLW].

Лема 3.1.10. *Ако $\delta, \delta' \in L^*$ и $v(\delta)/\delta = v(\delta')/\delta'$, то $\delta' = d\delta$, за някое $d \in k$.*

Лема 3.1.11. *Нека $\zeta = \frac{\sqrt{2}}{2}(1 + i) \in L$. Нека $M = L(\sqrt[8]{\omega})$, за някое $\omega \in L$ и да предположим, че $[M : L] = 8$. Тогава M/k реализира Q_{16} като група на Галоа тогава и само тогава, когато $v(\omega) = \omega^t \beta^8$, където $t \equiv -r \pmod 8$, $\omega^{(t^2-1)/8} \beta^t v(\beta) = \zeta^{l_1}$ и $l_1 \equiv 4 \pmod 8$.*

Лема 3.1.12. *Ако $b \notin -k^2$ (т.е. $L = k(\sqrt{b}) \neq k(i)$), то $k \cap L^8 = k^8 \cup b^4 k^8$ и $k \cap L^4 = k^4 \cup b^2 k^4$.*

Лема 3.1.13. *$L \neq k(i)$ (т.е. $i \in k$) тогава и само тогава, когато $r \equiv 1 \pmod 4$; $\zeta \in k$ тогава и само тогава, когато $r \equiv 1 \pmod 8$.*

С помощта на тези леми ще докажем следните теореми.

Теорема 3.1.14. ([Mi9, Theorem 4.5]) *Нека $L = k(\sqrt{b}), \omega \in L$ и нека $\zeta \in k$. Тогава $M/k = L(\sqrt[8]{\omega})/k$ е Q_{16} разширение тогава и само тогава, когато $\omega = (c\sqrt{b})^4 N(\gamma)/\gamma^2$, където $c \in k^*, \gamma \in L^*$ и $N(\gamma) \notin k^2 \cup bk^2$.*

Доказателство: Нека ω е както в условието. Тогава $\sqrt{\omega} = \pm c^2 b\sqrt{N(\gamma)}/\gamma$. Тъй като $a = N(\gamma)$ и b са квадратично независими, имаме $[L(\sqrt{\omega}) : L] = 2, L(\sqrt{\omega}) = k(\sqrt{a}, \sqrt{b})$ – биквадратично разширение над k и $[M : L] = 8$. Нататък, $N(\omega) = (c\sqrt{b})^8 = \delta^8$, където $\delta = c\sqrt{b} \in L^*$. Следователно $v(\omega) = \omega^{-1}\delta^8$, откъдето M/k е разширение на Галоа и $t = -1$. Още, $\rho = \omega^{(t^2-1)/8}\delta^t v(\delta) = v(\delta)/\delta = -1 = \zeta^{l_1}$, значи $l_1 \equiv 4$ и M/k е Q_{16} разширение.

Да предположим сега, че $M/k = L(\sqrt[8]{\omega})/k$ е Q_{16} разширение. Тогава $t = -1$ и $N(\omega) = \delta^8$ за $\delta \in L^*$. От лема 3.1.12 следва, че $\delta^8 \in k \cap L^8 = k^8 \cup b^4k^8$. Ако $\delta^8 \in k^8$, то $\delta \in k$, понеже $\zeta \in k$. В този случай, $\rho = v(\delta)/\delta = 1 = \zeta^{l_1}$, откъдето $l_1 \equiv 0$, значи M/k не е Q_{16} разширение, което е противоречие. Следователно, $\delta^8 \in b^4k^8$, т.е. $\delta = c\sqrt{b}, c \in k^*$. Тогава $\rho = v(\delta)/\delta = -1$, значи $l_1 \equiv 4$. Нататък, $(\omega/\delta^4)v(\omega/\delta^4) = N(\omega)/\delta^8 = 1$ и от теорема 90 на Хилберт следва, че $\omega/\delta^4 = v(\gamma)/\gamma$, за някое $\gamma \in L^*$. Оттук $\omega = \delta^4 v(\gamma)/\gamma = (c\sqrt{b})^4 N(\gamma)/\gamma^2$. Да предположим сега, че $u(\sqrt[8]{\omega}) = \sqrt[8]{\omega}\zeta$. Тогава $\sqrt{\omega}$ се съдържа в неподвижното подполе на u^2, което трябва да бъде биквадратично разширение на k. Следователно, $a = N(\gamma)$ и b са квадратично независими. □

Теорема 3.1.15. ([Mi9, Theorem 4.6]) *Нека $\sqrt{2} \in k, L = k(i)$ и нека $\omega \in L^*$. Тогава $M/k = L(\sqrt[8]{\omega})/k$ е Q_{16} разширение тогава и само тогава, когато*

$$\omega = \begin{cases} c_1 i, & \text{ако } c_1 \in k, -1 = \alpha^8, N(\alpha) = -1, \text{ и } c_1 \notin k^2 \cup -k^2; \\ c_2(1+\gamma^8), & \text{ако } c_2 \in k, N(\gamma) = -1, 1+\gamma^8 = d\delta^2, d \in k^*, \delta \in L^*, \text{ и} \\ & c_2 d \notin k^2 \cup -k^2. \end{cases}$$

Доказателство: Да предположим, че ω е както в условието. Ако $\omega = c_1 i$, то $\sqrt{\omega} = \pm\sqrt{c_1\alpha^4} = \pm\sqrt{c_1}\alpha^2$. Оттук $L(\sqrt{\omega}) = k(\sqrt{c_1}, \sqrt{b})$ е биквадратично над k и $[M : L] = 8$. Нататък, $v(\omega) = -\omega = \omega\alpha^8$, значи $t = 1$ и $r \equiv -1$. Също така, $\rho = \alpha v(\alpha) = N(\alpha) = -1 = \zeta^{l_1}$, значи $l_1 \equiv 4$ и M/k е Q_{16} разширение. Ако $\omega = c_2(1+\gamma^8)$, то $\sqrt{\omega} = \pm\sqrt{c_2 d}\delta$. Оттук $[M : L] = 8$. Нататък, $v(\omega) = c_2(1 + v(\gamma^8)) = \omega\beta^8$, където $\beta = v(\gamma)$. Тъй като $N(\beta) = N(\gamma) = -1 = \zeta^{l_1}$, M/k е Q_{16} разширение.

Нека сега M/k е Q_{16} разширение. Ако $v(\omega) = -\omega$, то $\omega = c_1 i, c_1 \in k$. Тъй като $r \equiv -1$, имаме $t = 1$, т.е. $v(\omega) = \omega\alpha^8, \alpha \in L^*$, значи $\alpha^8 = -1$. Също така, $\rho = \alpha v(\alpha) = N(\alpha) = -1 = \zeta^4$, понеже $l_1 \equiv 4$. Нататък, неподвижното подполе на u^2 е биквадратично над k, значи $u^2(\sqrt{\omega}) = \sqrt{\omega} = \pm\sqrt{c_1}\alpha^2$. Оттук c_1 и -1 са квадратично независими, т.е. $k(\sqrt{c_1}, i)/k$ е биквадратично разширение. Ако $v(\omega) \neq -\omega$, то $v(\omega)/\omega = \beta^8 \neq -1$, следователно $1 + v(\beta^8) \neq 0$. От $N(\beta^8) = 1$ следва, че

$$v(\omega)/\omega = \beta^8 = \frac{1+\beta^8}{1+v(\beta^8)} = \frac{v(1+v(\beta^8))}{1+v(\beta^8)},$$

и лема 3.1.10 ни дава, че $\omega = c_2(1+\gamma^8)$, където $\gamma = v(\beta)$ и $N(\gamma^8) = 1$. Сега, от $\rho = N(\beta) = -1$ следва, че $N(\gamma) = -1$. Тъй като неподвижното подполе на u^2 трябва да е биквадратично над k, получаваме, че $1 + \gamma^8 = d\delta^2$, където $d \in k^*$ и $\delta \in L^*$. Имаме тогава, че $\sqrt{\omega} = \pm\sqrt{c_2 d}\delta$, следователно $c_2 d$ и -1 трябва да са квадратично независими над k. □

Теорема 3.1.16. ([Mi9, Theorem 4.7]) *Нека $i \in k, L = k(\sqrt{2})$ и нека $\omega \in L^*$. Тогава $M/k = L(\sqrt[8]{\omega})/k$ е Q_{16} разширение тогава и само тогава, когато $\omega = c^3/\gamma^2$, където $c \in k^*, \gamma \in L^*, N(\gamma) = -c$ и $c \notin k^2 \cup 2k^2$.*

Доказателство: Да предположим, че ω е както в условието. От $c \notin k^2 \cup 2k^2$ следва, че $L(\sqrt{\omega}) = k(\sqrt{c}, \sqrt{2})$ е биквадратично над k и $[M : L] = 8$. Нататък, $v(\omega)/\omega^3 = \gamma^8/c^6 N(\gamma^2) = \beta^8$, където $\beta = \gamma/c$. Следователно $t = 3$ и $(t^2-1)/8 = 1$, значи $\rho = \omega\beta^3 v(\beta) = N(\gamma)/c = -1 = \zeta^{l_1}$. Оттук M/k е Q_{16} разширение.

Нека сега $M/k = L(\sqrt[8]{\omega})/k$ е Q_{16} разширение. Тогава $v(\omega) = \omega^3\beta^8, \beta \in L^*$, откъдето $N(\omega) = (\omega\beta^2)^4 \in L^4 \cap k$. От лема 3.1.12 следва, че $L^4 \cap k = k^4 \cup 4k^4$, откъдето $\omega\beta^2 = c$ или $\omega\beta^2 = \sqrt{2}c$ за $c \in k$. Имаме, че $N(\omega) \in k^2$. От друга страна, ако $\omega\beta^2 = \sqrt{2}c$, то $N(\omega\beta^2) = -2c^2 \in -2k^2 = 2k^2 \neq k^2$, което е противоречие. Така единствената възможност, която остава е $\omega\beta^2 = c$. Нека $\gamma = c\beta$. Тогава $\omega = c/\beta^2 = c^3/\gamma^2$ и $N(\gamma^2) = c^4 N(c/\omega) = c^2$, т.е. $N(\gamma) = \pm c$. Ако $N(\gamma) = c$, то $\rho = \omega\beta^3 v(\beta) = N(\gamma)/c = 1 = \zeta^{l_1}$, значи $l_1 \equiv 0$, което е противоречие. Следователно $N(\gamma) = -c$. Също така, c и 2 трябва да бъдат квадратично независими над k, понеже $[M : L] = 8$. □

Теорема 3.1.17. ([Mi9, Theorem 4.8]) *Нека $\sqrt{-2} \in k, L = k(\sqrt{i})$ и нека $\omega \in L^*$. Тогава $M/k = L(\sqrt[8]{\omega})/k$ е Q_{16} разширение тогава и само тогава, когато $\omega = N(\gamma)\eta^2/\gamma^4$, където $\eta \in ik, \gamma \in L^*$ и $N(\gamma) \notin k^2 \cup -k^2$.*

Доказателство: Да предположим, че ω е както в условието. От $N(\gamma) \notin k^2 \cup -k^2$ следва, че $L(\sqrt{\omega})$ е биквадратично над k и $[M : L] = 8$. Тъй като $r \equiv 3$, трябва да покажем, че $t = 5$ и $l_1 \equiv 4$. Наистина, $v(\omega)/\omega^4 = \omega\beta^8$, където $\beta = \gamma^2/v(\gamma)\eta$. Също така, $\rho = \omega^3\beta^5 v(\beta) = \eta/v(\eta) = -1$, значи $l_1 \equiv 4$. Следователно, $M/k = L(\sqrt[8]{\omega})/k$ е Q_{16} разширение.

Нека сега $M/k = L(\sqrt[8]{\omega})/k$ е Q_{16} разширение. Тогава $v(\omega) = \omega^5\beta^8$, където $\beta \in L^*$ и $l_1 \equiv 4$. Оттук $v(\omega)/\omega = (\omega\beta^2)^4$. Нека $\alpha = N(\omega\beta^2) \in k$. Тогава $\alpha^4 = N((\omega\beta^2)^4) = N(v(\omega)/\omega) = 1$. Следователно, $\alpha^2 = \pm 1$. Ако $\alpha^2 = -1$, то $\alpha = \pm i \in k$, което е противоречие. Тогава $\alpha^2 = 1$, значи $\alpha = \pm 1$. Нека $\delta = \omega\beta^2$. Ако $N(\delta) = 1$, то $\delta = \gamma/v(\gamma)$, за някое $\gamma \in L^*$. Следователно, $\omega = \gamma/v(\gamma)\beta^2 = N(\gamma)\eta^2/\gamma^4$, където $\eta = \gamma^2/v(\gamma)\beta$. Също така, $\rho = \omega^3\beta^5 v(\beta) = \eta/v(\eta) = \zeta^4 = -1$, значи $v(\eta) = -\eta$, т.е. $\eta \in ik$. Ако $\alpha = -1$, т.е. $N(\delta) = -1$, то $v(\omega\delta^2) = \omega\delta^4 v(\delta^2) = \omega\delta^2$, т.е. $\omega\delta^2 \in k$. Следователно, $N(\omega\delta^2) \in k^2$ и $N(\omega) \in k^2$. Но тогава $-1 = N(\omega\beta^2) = N(\delta) \in k^2$, което е противоречие. Така получаваме, че $\omega = N(\gamma)\eta^2/\gamma^4$, където $\eta \in ik$. Накрая, тъй като $k(\sqrt{\omega}, i)/k$ трябва да бъде биквадратично разширение, имаме, че $a = N(\gamma)$ и -1 са квадратично независими над k. □

3.1.4 Реализиране на групи от редове 8 и 16 над локални полета

В началото ще изложим някои основни изоморфизми и комутативни диаграми. Теорията на локалните полета се засяга в много монографии, като например [CF, Se2, Ив, Pi]. Означаваме с Ω максималното разширение на Галоа (сепарабелната обвивка) на локалното поле k. Тогава групата на Брауер $\mathrm{Br}(k)$ е изоморфна на $H^2(\Omega/k)$, която на свой ред е изоморфна на индуктивната (директна) граница $\varinjlim H^2(K_i/k)$, където K_i/k пробягват всички крайни разширения на Галоа. Ще използваме още означенията $F_i = \mathrm{Gal}(K_i/k)$ и $H^2(K_i/k) = H^2(F_i, k^*)$.

За всяко естествено число n съществува единствено неразклонено разширение k_n от степен n над локалното поле k. Полето k_n е полето на разлагане на полинома $x^{q^n-1} - 1$, където q е броят на елементите в полето от класове $\overline{k}$ на k.

Да разгледаме два примера на неразклонено разширение k_2.

Пример 3.1.18. Нека p е нечетно просто число, $q = p^m$ е броят на елементите в полето от класове $\overline{k}$ на k, и нека $-1 \notin k^2$. Тогава неразклоненото разширение k_2 е

полето на разлагане на полинома

$$g(x) = x^{q^2-1} - 1 = x^{p^{2m}-1} - 1$$

над k. Тъй като $4|p^{2m}-1$, имаме, че $\sqrt{-1}$ е корен на $g(x)$, следователно $k_2 = k(\sqrt{-1})$. □

Пример 3.1.19. Нека $q = 2^m$ и $-3 \notin k^2$. Тогава $3|2^{2m}-1$, значи $\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ е корен на полинома

$$h(x) = x^{2^{2m}-1} - 1,$$

следователно $k_2 = k(\sqrt{-3})$. □

За максималното неразклонено разширение k_{ur} ще имаме, че

$$k_{ur} = \bigcup_{n \geq 1} k_n.$$

Имаме още, че k_{ur} е подполе на Ω, понеже k_{ur} е абелово разширение на k. Тогава имаме точната редица

$$0 \longrightarrow H^2(k_{ur}/k) \longrightarrow \mathrm{Br}(k) \longrightarrow \mathrm{Br}(k_{ur}).$$

Ако с φ означим автоморфизмът на Фробениус за разширението k_{ur}/k, то $\varphi_n = \varphi|_{k_n}$ поражда групата $F_n = \mathrm{Gal}(k_n/k)$, която е циклична от ред n. Следователно

$$H^2(k_{ur}/k) = \varinjlim H^2(F_n, k_n^*)$$

и

$$H^2(F_n, k_n^*) \cong k^*/N(k_n/k), \tag{3.6}$$

където $N : k_n \to k$ е норменото изображение на разширението k_n/k и $N(k_n/k)$ е образът на N в k.

Ще използваме следните стандартни означения: ν е нормирането, U е групата от единици на k и π е конформният елемент на нормирането ν. Тъй като $NU(k_n/k) = U$ и $N(k_n/k) = \langle \pi^n \rangle \times U$, то регулярното нормиране ν дава изоморфизмите $k^*/U \cong \mathbb{Z}$ и $k^*/N(k_n/k) \cong \mathbb{Z}/n\mathbb{Z}$. Следователно, изображението ν/n дава изоморфизма $k^*/N(k_n/k) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Комбинирайки този изоморфизъм с изоморфизма (3.6) получаваме изоморфизма

$$inv : H^2(F_n, k_n^*) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}. \tag{3.7}$$

По-конкретно, ако ни е дадено произволно $x \in k_n^*$, можем да положим:

$$f(\varphi_n^i, \varphi_n^j) = \begin{cases} 1, & 0 \leq i, j, i+j < n \\ x, & 0 \leq i, j < n \leq i+j \end{cases} \tag{3.8}$$

Изображението $f : F_n \times F_n \to k_n^*$ е кръстосан хомоморфизъм, т.е. f се съдържа в $Z^2(F_n, k_n)$. Означаваме с $[f]$ 2-кокласът породен от f в $H^2(F_n, k_n^*)$. Тогава изоморфизмът (3.7) се задава чрез

$$inv : [f] \mapsto \frac{\nu(x)}{n} + \mathbb{Z}.$$

Ако $m|n$ то $k \subset k_m \subset k_n$ и е дефиниран хомоморфизмът на инфлация:

$$inf : H^2(F_m, k_m^*) \longrightarrow H^2(F_n, k_n^*).$$

Имаме комутативната диаграма

$$\begin{array}{ccc} H^2(F_m, k_m^*) & = & \frac{1}{m}\mathbb{Z}/\mathbb{Z} \\ \downarrow{\scriptstyle inf} & & \downarrow \\ H^2(F_n, k_n^*) & = & \frac{1}{n}\mathbb{Z}/\mathbb{Z}, \end{array}$$

където дясното вертикално изображение е инекция, понеже $\frac{1}{m}\mathbb{Z} \subset \frac{1}{n}\mathbb{Z}$. Следователно,

$$H^2(k_{ur}/k) = \varinjlim H^2(F_n, k_n) \cong \varinjlim \frac{1}{n}\mathbb{Z}/\mathbb{Z} = \mathbb{Q}/\mathbb{Z}.$$

Също така, имаме $\mathrm{Br}(k_{ur}) = 0$ и изоморфизмът

$$inf : H^2(k_{ur}/k) \cong H^2(\Omega/k) = \mathrm{Br}(k),$$

откъдето $\mathrm{Br}(k) \cong \mathbb{Q}/\mathbb{Z}$. Последният изоморфизъм означаваме отново с inv.

Нека сега K/k е крайно разширение на Галоа и $[K : k] = n$. Тогава $k \subset K \subset \Omega$ и е дефиниран хомоморфизмът на ограничение:

$$res : \mathrm{Br}(k) = H^2(\Omega/k) \longrightarrow \mathrm{Br}(K) = H^2(\Omega/K).$$

Тогава диаграмата

$$\begin{array}{ccc} \mathrm{Br}(k) & = & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle n} \\ \mathrm{Br}(K) & = & \mathbb{Q}/\mathbb{Z} \end{array}$$

е комутативна. Следователно, групата $H^2(K/k) = \mathrm{Br}(K/k)$ е ядрото на хомоморфизма $res : \mathrm{Br}(k) \to \mathrm{Br}(K)$. По този начин получаваме изоморфизмът

$$inv : H^2(K/k) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Ще продължим с приложения касаещи цикличните и кватернионните алгебри. Да означим с $\mathcal{G}(k)$ множеството на всички крайномерни централни прости алгебри над k. Нека алгебрата $A \in \mathcal{G}(k)$ е от степен n над k. Тогава $[A] = [(k_n, F_n, f)]$, където k_n, F_n и f са както по-горе, а (k_n, F_n, f) е циклична алгебра. Наистина, ако K е полето на разлагане на A и $F = \mathrm{Gal}(K/k)$, то

$$[A] \in \mathrm{Br}(K/k) = H^2(F, K^*) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong H^2(F_n, k_n^*).$$

Фактор системата f е еднозначно определена от някакъв елемент $x \in k$, според (3.8). Тогава

$$inv([A]) = \frac{\nu(x)}{n} + \mathbb{Z} \in \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Нека $A, B \in \mathcal{G}(k)$. Ето няколко свойства на изоморфизма inv:

- $A \sim B$ (т.е. $[A] = [B]$) $\iff$ $inv(A) = inv(B)$;

- $A \sim k$ (т.е. $[A] = 1$) $\iff$ $inv(A) = 0$;

- $inv(A \otimes B) = inv(A) + inv(B)$.

Нататък, да разгледаме цикличната алгебра $B = (k_n, F_n, f)$. Алгебрата B се определя напълно от следните свойства:

- $B = \bigoplus_{0 \le j < n} u^j k_n$;

- $u^{-1}du = \varphi_n(d), \forall d \in k_n$, където φ_n е автоморфизмът на Фробениус за разширението k_n/k;

- $u^n = x \in k^*$.

Системата от фактори f се задава чрез

$$u_{\varphi_n^i} u_{\varphi_n^j} = f(\varphi_n^i, \varphi_n^j) u_{\varphi_n^{i+j}}.$$

Може да се покаже, че f удовлетворява формулата (3.8). Полагаме $u_{\varphi_n} = u, u_{\varphi_n^i} = u^i, u_1 = u^n = x$.

Да разгледаме сега кватернионната алгебра Q_1, която е породена от елементи α и β такива, че $\alpha^2 = a, \beta^2 = b$ и $\alpha\beta = -\beta\alpha$ $(a, b \in k^*)$. Използваме стандартните означения: с $(a, b/k)$ означаваме алгебрата Q_1, а с (a, b) класът на еквивалентност на Q_1 в $\mathrm{Br}(k)$. Тъй като $\mathrm{Deg}(Q_1) = 2$, имаме $[Q_1] = [Q_2]$, където $Q_2 = (k_2, C_2, f)$ е кръстосаното произведение на неразклоненото разширение $k_2 = k(\sqrt{c})$ с C_2 – цикличната група от ред 2. Очевидно, Q_2 е или кватернионна алгебра с деление или матричната алгебре $\mathrm{Mat}_2(k)$. И в двата случая можем да положим $Q_2 = (c, d/k)$. Елементите γ и δ такива, че $\gamma^2 = c, \delta^2 = d$ и $\gamma\delta = -\delta\gamma$ пораждат Q_2.

Всъщност, неразклоненото разширение k_n се съдържа с точност до k - изоморфизъм във всяка алгебра $A \in \mathcal{G}(k)$ от степен n над k. Разбира се, в A неразклоненото разширение не е единствено. Всеки две от тях, обаче са взаимно спрегнати по теоремата на Ньотер-Сколем. В нашия случай имаме, че $Q_2 = k_2 \oplus \delta k_2$ и $inv([Q_1]) = inv([Q_2]) = \frac{\nu(d)}{2} + \mathbb{Z}$.

От теорията на кватернионните алгебри и квадратичните форми е известно, че $(a, b) = (c, d)$ тогава и само тогава, когато квадратичните форми $f_1(x, y, z) = ax^2 + by^2 - abz^2$ и $f_2(x, y, z) = cx^2 + dy^2 - cdz^2$ са еквивалентни. Тогава c и d се представят чрез $f_1(x, y, z) : c = ax_1^2 + by_1^2 - abz_1^2, d = ax_2^2 + by_2^2 - abz_2^2$, където $x_i, y_i, z_i \in k, i = 1, 2$. Можем да положим $\gamma = x_1\alpha + y_1\beta + z_1\alpha\beta$, откъдето $\gamma^2 = c$. Според теоремата на Ньотер-Сколем, можем да намерим елемент $\delta \in Q_1$ такъв, че $\delta\gamma\delta^{-1} = -\gamma$. Ако $\delta^2 = d \in k^*$, то $Q_1 = (a, b/k) \cong Q_2 = (c, d/k)$. По този начин виждаме как точно се съдържа неразклоненото разширение $k_2 = k(\sqrt{c})$ в Q_1.

Ще използваме локалните инварианти за да определим дали задачата за вложимост с ядро $\mu_2 = \{\pm 1\}$ е разрешима. Нека $(K/k, G, \mu_2)$ е задача за вложимост зададена с груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow G \underset{\psi}{\longrightarrow} F = \mathrm{Gal}(K/k) \longrightarrow 1 \tag{3.9}$$

и нека $c \in H^2(F, \mu_2)$ е 2-кокласът, съответстващ на (3.9). В следващия пример ще илюстрираме как можем да пресметнем дадено произведение на кватернионни алгеб-

ри. По този начин може ясно да се види кога дадено препятствия за реализирането на групи от редове 8 и 16 над локални полета се разпада (виж [Mi8] за списък на условията).

Пример 3.1.20. Нека $K/k = k(\sqrt{a_1}, \sqrt{a_1}, \ldots, \sqrt{a_n})/k$ е $C_2^n = \underbrace{C_2 \times \cdots \times C_2}_{n}$ разширение. Нека пораждащите $\rho_1, \ldots, \rho_n$ на елементарната абелова група C_2^n действат чрез $\rho_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}\sqrt{a_j}$, където δ_{ij} е делтата на Кронекер. Нека

$$1 \longrightarrow \mu_2 \longrightarrow G \underset{\psi}{\longrightarrow} C_2^n = \mathrm{Gal}(K/k) \longrightarrow 1 \tag{3.10}$$

е неразцепимо групово разширение и нека да изберем про-образи $\sigma_1, \ldots, \sigma_n \in G$ на $\rho_1, \ldots, \rho_n$. Дефинираме $d_{ij}, i \leq j$ чрез $\sigma_i^2 = (-1)^{d_{ii}}$ и $\sigma_i\sigma_j = (-1)^{d_{ij}}\sigma_j\sigma_i, i < j$. Тогава задачата за вложимост $(K/k, G, \mu_2)$, зададена с (3.10) е разрешима тогава и само тогава, когато $\prod_{i\leq j}(a_i, a_j)^{d_{ij}} = 1$ в $\mathrm{Br}(k)$ (виж [Le1]). Ако $k_2 = k(\sqrt{c})$ е неразклонимото разширение от степен 2 над k, тогава $(a_i, a_j) = (c, b_{ij})$ за някои $b_{ij} \in k^*$. Следователно, $\prod_{i\leq j}(a_i, a_j)^{d_{ij}} = (c, b)$, където $b = \prod_{i\leq j} b_{ij}^{d_{ij}}$ и

$$inv(c, b) = \frac{\nu(b)}{2} + \mathbb{Z} \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}.$$

3.2 Групи от ред 32 като групи на Галоа

В компютърната алгебна GAP 3+ се съдържа подробна информация за групите от ред $2^n, n \leq 8$. В таблицата, намираща се в приложението, сме дали следната информация за групите от ред 32: система пораждащи с техните съотношения, ранга (т.е. минималният брой на пораждащи на фактор-групата по подгрупата на Фратини), централните елементи и експонентата на групата. Имаме общо 51 групи, които са означени с G_i $(i = 1, \ldots, 51)$. Те се пораждат от 5 елемента $a_1, \ldots, a_5$ (разбира се, не винаги това е минимално пораждащо множество). Означаваме $[a_i, a_j] = a_i^{-1}a_j^{-1}a_ia_j$ – комутаторът на двата елемента a_i и a_j. Появата на някакъв израз в колоната за съотношенията в таблицата означава, че той е равен на 1. За краткост, ще пропуснем комутаторите, за които един от елементите лежи в центъра. Например, елементът a_5 е в центъра на всяка група, така че няма да пишем комутаторите от вида $[a_i, a_5]$.

За 24 групи не е нужно да пресмятаме препятствията. Това са абеловите групи – $G_1, G_3, G_{16}, G_{21}, G_{36}, G_{45}, G_{51}$; неабеловите групи с експонента 16 – G_{17}, G_{18}, G_{19} и G_{20}; неабеловите групи от вида $H \times C_2$ – $G_{22}, G_{23}, G_{37}, G_{39}, G_{40}, G_{41}, G_{46}, G_{47}$ и G_{48}; неабеловите групи от вида $H \times C_4$ – G_{24} and G_{25}; и екстра-специалните групи G_{49} и G_{50} (виж [Sm]).

Ще използваме съществено следните критерии, които се получават като следствия от теорема 2.2.1.

Теорема 3.2.1. *Нека $K/k = k(\sqrt{a_1}, \ldots, \sqrt{a_n})/k$ е C_2^n разширение, и нека $\sigma_1, \ldots, \sigma_n \in C_2^n$ се задават чрез $\sigma_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}\sqrt{a_j}$. Нека*

$$1 \longrightarrow \mu_2 \longrightarrow G \longrightarrow C_2^n \longrightarrow 1 \tag{3.11}$$

е неразцепимо разширение, и да изберем про-образи $s_1, \ldots, s_n \in G$ на $\sigma_1, \ldots, \sigma_n$. Дефинираме $d_{ij}, i \leq j$, чрез $s_i^2 = (-1)^{d_{ii}}$ и $s_is_j = (-1)^{d_{ij}}s_js_i, i < j$. Тогава препятствието на задачата за вложимост зададена чрез K/k и (3.11) е

$$\prod_{i \leq j}(a_i, a_j)^{d_{ij}} \in \mathrm{Br}(k).$$

Теорема 3.2.2. *Нека K/k е $C_4^r \times C_2^s$ разширение. Можем да запишем:*

$$K = k(\sqrt{q_1(a_1 + \sqrt{a_1})}, \ldots, \sqrt{q_r(a_r + \sqrt{a_r})}, \sqrt{a_{r+1}}, \ldots, \sqrt{a_{r+s}}),$$

където $a_1, \ldots, a_{r+s} \in k^*$ *са квадратично независими,* $a_i = 1 + c_i^2$ *за* $i \leq r$, *и* $q_i \in k^*$. *Нека* $\rho_1, \ldots, \rho_{r+s} \in \mathrm{Gal}(K/k)$ *са такива, че* $\rho_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}\sqrt{a_j}$. *Нека*

$$1 \longrightarrow \mu_2 \longrightarrow G \longrightarrow C_4^r \times C_2^s \longrightarrow 1 \tag{3.12}$$

е неразцепимо разширение, и да изберем про-образи $t_1, \ldots, t_{r+s} \in G$ *на* $\rho_1, \ldots, \rho_{r+s}$. *Тогава препятствието на задачата за вложимост зададена чрез* K/k *и* (3.12) *е:*

$$\prod_{i=r+1}^{r+s}(a_i, a_i)^{d_i} \cdot \prod_{i=1}^{r}[(a_i, 2)(-1, q_i)]^{d_i} \cdot \prod_{i<j}(a_i, a_j)^{d_{ij}},$$

където $t_i^2 = (-1)^{d_i}$ *за* $i > r$, $t_i^4 = (-1)^{d_i}$ *за* $i \leq r$, *и* $t_i t_j = (-1)^{d_{ij}} t_j t_i$.

Теорема 3.2.3. *Нека* K/k *е* D_8 *разширение както в началото на главата, нека*

$$1 \longrightarrow \mu_2 \longrightarrow G \longrightarrow D_8 \longrightarrow 1 \tag{3.13}$$

е неразцепимо разширение, и да изберем про-образи s *и* t *в* G *на* σ *и* τ, *съответно. Тогава препятствието на задачата за вложимост зададена чрез* K/k *и* (3.13) *е:*

$$[(a, -2)(-b, 2\alpha_1 r)]^i (b, -1)^j (a, -1)^k \in \mathrm{Br}(k),$$

където $s^4 = (-1)^i, t^2 = (-1)^j$ *и* $ts = (-1)^k s^3 t$.

Сега ще приложим горния критерий за групата $D_8 \times C_2$, породена от σ, τ и ρ със съотношения $\sigma^4 = \tau^2 = \rho^2 = 1, \tau\sigma = \sigma^3\tau$ и ρ е централен.

Теорема 3.2.4. *Нека* $K/k = k(\sqrt{r\alpha}, \sqrt{b}, \sqrt{c})/k$ *е* $D_8 \times C_2$ *разширение, нека*

$$1 \longrightarrow \mu_2 \longrightarrow G \longrightarrow D_8 \times C_2 \longrightarrow 1 \tag{3.14}$$

е неразцепимо разширение, и да изберем про-образи s, t *и* p *на* σ, τ *и* ρ *съответно. Тогава препятствието на задачата за вложимост зададена чрез* K/k *и* (3.14) *е:*

$$[(a, -2)(-b, 2\alpha_1 r)]^i (b, -1)^j (a, -1)^k (c^l a^{d_1} b^{d_2}, c),$$

където $s^4 = (-1)^i, t^2 = (-1)^j, ts = (-1)^k s^3 t, p^2 = (-1)^l, ps = (-1)^{d_1} sp, pt = (-1)^{d_2} tp$.

3.2.1 Директно произведение с обединена фактор-група

Нека $\varphi' : G' \to F$ и $\varphi'' : G'' \to F$ са хомоморфизми с ядра N' и N'', съответно. *Пулбек* на двойка хомоморфизми φ' и φ'' наричаме подгрупата в $G' \times G''$ на всички наредени двойки (σ', σ''), за които $\varphi'(\sigma') = \varphi''(\sigma'')$. Пулбекът се означава с $G' \curlywedge G''$. Той се нарича още директно произведение на групите G' и G'' с обединена фактор-група F и се означава с $G' *_F G''$.

Нека сега $N_1 = N' \times \{1\}$ и $N_2 = \{1\} \times N''$. Тогава N_1 и N_2 са нормални подгрупи на $G' \curlywedge G''$, за които $N_1 \cap N_2 = \{1\}$. Обратното също е вярно (виж [ИЛФ, §1.12]):

Лема 3.2.5. *Нека N_1 и N_2 са две нормални подгрупи на групата G такива, че $N_1 \cap N_2 = \{1\}$. Тогава G е изоморфна на пулбека $(G/N_1) \curlywedge (G/N_2)$. Също така, имаме комутативната диаграма:*

$$\begin{array}{ccccccccc}
 & & & & 1 & & 1 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & N_2 & = & N_2 & & \\
 & & & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & N_1 & \longrightarrow & G & \xrightarrow{\varphi_1} & G/N_1 & \longrightarrow & 1 \\
 & & \| & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_2^*} & & \\
1 & \longrightarrow & N_1 & \longrightarrow & G/N_2 & \xrightarrow{\varphi_1^*} & G/N_1N_2 & \longrightarrow & 1 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 1 & & 1 & &
\end{array}$$

където хомоморфизмите на групите в техните фактор-групи са естествени.

Приложението за задачите за вложимост се дава от следната:

Теорема 3.2.6. *Нека K/k е разширение на Галоа с група на Галоа F. В означенията на лема 3.2.5, нека $F \cong G/N_1N_2$ и $G \cong (G/N_1) \curlywedge (G/N_2)$. Тогава задачата за вложимост $(K/k, G, N_1 \times N_2)$ е разрешима тогава и само тогава, когато задачите за вложимост $(K/k, G/N_1, N_2)$ и $(K/k, G/N_2, N_1)$ са разрешими.*

Тъй като ще разглеждаме групи от ред 32, ще търсим нормални подгрупи N_1 и N_2 от ред 2. В този случай, групата G е пулбек тогава и само тогава, когато центърът $Z(G)$ има поне два елемента от ред 2 (с други думи, $Z(G)$ не е циклична група). Пулбеците, които ще дискутираме са 18: $G_2, G_4, G_5, G_9, G_{10}, G_{12}, G_{13}, G_{14}, G_{26} - G_{35}$.

Да започнем с групата G_2. Ще дадем всички детайли, които да послужат като образец за останалите групи.

Групата G_2.

Центърът $Z(G_2) = \langle a_3, a_4, a_5\rangle$ е изоморфен на C_2^3. Нека $N_1 = \langle a_4\rangle, N_2 = \langle a_5\rangle$ и $N = N_1N_2 = N_1 \times N_2$. Тогава фактор-групата G_2/N е изоморфна на D_8. Да разгледаме задачата за вложимост зададена чрез D_8 разширение K/k, според описанието в началото на тази глава, и груповото разширение

$$1 \longrightarrow N \longrightarrow G_2 \underset{\substack{a_1\mapsto\sigma_1\\ a_2\mapsto\tau_1}}{\longrightarrow} D_8 \longrightarrow 1,$$

където $\sigma_1^2 = \tau_1^2 = [\sigma_1, \tau_1]^2 = 1$. Нека $\sigma = \sigma_1\tau_1$ и $\tau = \tau_1$. Тогава $|\sigma| = 4, |\tau| = 2$ и $\tau\sigma = \sigma^3\tau$.

Да разгледаме сега задачата за вложимост зададена чрез K/k и груповото разширение

$$1 \longrightarrow N_2 \longrightarrow G_2/N_1 \underset{\substack{b_1b_2\mapsto\sigma\\ b_2\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1.$$

Групата G_2/N_1 се поражда от елементи $b_i = a_i\langle a_4\rangle \in G_2/N_1, i \neq 4$ такива, че $b_1^2 = b_3^2 = b_5^2 = 1, b_2^2 = b_5, [b_2, b_1] = b_3, b_3$ е централен. Тогава G_2/N_1 е изоморфна на $D \curlywedge C$. Също така, имаме съотношенията $(b_1b_2)^2 = b_5b_3, (b_1b_2)^4 = 1$ и $b_2(b_1b_2) = (b_1b_2)^3b_2b_5 = -(b_1b_2)^3b_2$. Според теорема 3.2.3 препятствието на тази задача е $(ab, -1) \in \mathrm{Br}(k)$.

Да разгледаме сега G_2/N_2, която се поражда от елементи $b_i = a_i\langle a_5\rangle \in G_2/N_2, i = 1, \ldots, 4$, със съотношения $b_1^4 = b_2^2 = b_3^2 = b_4^2 = 1, b_4 = b_1^2, [b_1, b_2] = b_3, b_3$ е централен. Следователно G_2/N_2 е изоморфна на $D \curlywedge C$. Имаме равентството $b_2(b_1b_2) = -(b_1b_2)^3b_2$. Тогава препятствието на задачата зададена чрез K/k и груповото разширение

$$1 \longrightarrow N_1 \longrightarrow G_2/N_2 \underset{\substack{b_1b_2\mapsto\sigma\\ b_2\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1.$$

е $(a, -1) \in \mathrm{Br}(k)$.

По този начин получихме, че задачата $(K/k, G_2, N)$ е разрешима тогава и само тогава, когато $(ab, -1) = (a, -1) = 1 \in \mathrm{Br}(k)$, където $a, b \in k^*$ са квадратично независими такива, че $(a, ab) = 1 \in \mathrm{Br}(k)$ (това е необходимо условие).

Останалите групи могат да се изследват по същия начин. Ние ще запишем само основните моменти в нашите пресмятания.

Групата G_4:

$Z(G_4) = \langle a_3, a_4, a_5\rangle = \langle a_3, a_4\rangle \cong C_4 \times C_2$, $N_1 = \langle a_4\rangle, N_2 = \langle a_5\rangle, N = N_1 \times N_2, G_4/N_1 \cong M_{16}, G_4/N_2 \cong C_4 \times C_4$. Задачата за вложимост $(K/k, G_4, N)$ зададена чрез $C_4 \times C_2$ разширение K/k и груповото разширение

$$1 \longrightarrow N \longrightarrow G_4 \underset{\substack{a_1\mapsto\rho_1\\ a_2\mapsto\rho_2}}{\longrightarrow} C_4 \times C_2 \longrightarrow 1$$

е разрешима тогава и само тогава, когато $(a, 2b)(-1, r) = (b, b) = 1 \in \mathrm{Br}(k)$, където $(a, a) = 1$ е необходимо условие за съществуването на C_4 разширение.

Групата G_5:

$Z(G_5) = \langle a_3, a_4, a_5\rangle = \langle a_3, a_4\rangle \cong C_2 \times C_4$, $N_1 = \langle a_3\rangle, N_2 = \langle a_5\rangle, N = N_1 \times N_2, G_5/N_1 \cong C_8 \times C_2, G_5/N_2 \cong D \curlywedge C$. Задачата за вложимост $(K/k, G_5, N)$ зададена чрез $C_4 \times C_2$ разширение K/k и груповото разширение

$$1 \longrightarrow N \longrightarrow G_5 \underset{\substack{a_1\mapsto\rho_1\\ a_2\mapsto\rho_2}}{\longrightarrow} C_4 \times C_2 \longrightarrow 1$$

е разрешима тогава и само тогава, когато $(a, 2)(-1, r) = (a, b) = 1 \in \mathrm{Br}(k)$, където $(a, a) = 1$ е необходимо условие.

Групата G_9:

$Z(G_9) = \langle a_4, a_5\rangle \cong C_2^2, N_1 = \langle a_4\rangle, N_2 = \langle a_5\rangle, N = N_1 \times N_2, G_9/N_1 \cong D_{16}, G_9/N_2 \cong D \curlywedge C$. Задачата за вложимост $(K/k, G_9, N)$ зададена чрез D_8 разширение K/k и груповото разширение

$$1 \longrightarrow N \longrightarrow G_9 \underset{\substack{a_1a_2\mapsto\sigma\\ a_2\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1$$

е разрешима тогава и само тогава, когато $(ab, 2)(-b, \alpha_1 r) = (a, a) = 1 \in \mathrm{Br}(k)$, където $(a, ab) = 1$ е необходимо условие.

Групата G_{10}:

$Z(G_{10}) = \langle a_4, a_5\rangle \cong C_2^2$, $N_1 = \langle a_4\rangle, N_2 = \langle a_5\rangle, N = N_1 \times N_2, G_{10}/N_1 \cong SD_{16}, G_{10}/N_2 \cong D \curlywedge C$. Задачата за вложимост $(K/k, G_{10}, N)$ зададена чрез D_8 разширение K/k и груповото разширение

$$1 \longrightarrow N \longrightarrow G_{10} \underset{\substack{a_1a_2\mapsto\sigma\\ a_2\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1$$

е разрешима тогава и само тогава, когато $(a,-2)(-b,2\alpha_1 r) = (a,a) = 1 \in \mathrm{Br}(k)$, където $(a,ab) = 1$ е необходимо условие.

Групата G_{12}:

$Z(G_{12}) = \langle a_3, a_4, a_5\rangle = \langle a_3, a_4\rangle \cong C_2 \times C_4$, $N_1 = \langle a_3\rangle, N_2 = \langle a_5\rangle, N = N_1 \times N_2, G_{12}/N_1 \cong C_8 \times C_2, G_{12}/N_2 \cong Q \leftthreetimes C$. Задачата за вложимост $(K/k, G_{12}, N)$ зададена чрез $C_4 \times C_2$ разширение K/k и груповото разширение

$$1 \longrightarrow N \longrightarrow G_{12} \underset{\substack{a_1\mapsto\rho_1\\ a_2\mapsto\rho_2}}{\longrightarrow} C_4 \times C_2 \longrightarrow 1$$

е разрешима тогава и само тогава, когато $(a,2)(-1,r) = (ab,b) = 1 \in \mathrm{Br}(k)$, където $(a,a) = 1$ е необходимо условие.

Групата G_{13}:

$Z(G_{13}) = \langle a_4, a_5\rangle \cong C_2^2, N_1 = \langle a_4\rangle, N_2 = \langle a_5\rangle, N = N_1 \times N_2, G_{13}/N_1 \cong SD_{16}, G_{13}/N_2 \cong Q \leftthreetimes C$. Задачата за вложимост $(K/k, G_{13}, N)$ зададена чрез D_8 разширение K/k и груповото разширение

$$1 \longrightarrow N \longrightarrow G_{13} \underset{\substack{a_1\mapsto\tau\\ a_2\mapsto\sigma}}{\longrightarrow} D_8 \longrightarrow 1$$

е разрешима тогава и само тогава, когато $(a,-2)(-b,2\alpha_1 r) = (b,b) = 1 \in \mathrm{Br}(k)$, където $(a,ab) = 1$ е необходимо условие.

Групата G_{14}:

$Z(G_{14}) = \langle a_4, a_5\rangle \cong C_2^2, N_1 = \langle a_4\rangle, N_2 = \langle a_5\rangle, N = N_1 \times N_2, G_{14}/N_1 \cong D_{16}, G_{14}/N_2 \cong Q \leftthreetimes C$. Задачата за вложимост $(K/k, G_{14}, N)$ зададена чрез D_8 разширение K/k и груповото разширение

$$1 \longrightarrow N \longrightarrow G_{14} \underset{\substack{a_1\mapsto\tau\\ a_2\mapsto\sigma}}{\longrightarrow} D_8 \longrightarrow 1$$

е разрешима тогава и само тогава, когато $(ab,2)(-b,\alpha_1 r) = (b,b) = 1 \in \mathrm{Br}(k)$, където $(a,ab) = 1$ е необходимо условие.

За всяка от останалите групи $G_{26} - G_{35}$ полагаме $N_1 = \langle a_4\rangle, N_2 = \langle a_5\rangle$ и $N = N_1 \times N_2$. Фактор-групата G_i/N е изоморфна на C_2^3. Затова ние ще разгледаме задачите

за вложимост зададени чрез C_2^3 разширение $K/k = k(\sqrt{a}, \sqrt{b}, \sqrt{c})/k$ и груповото разширение

$$1 \longrightarrow N \longrightarrow G_i \underset{\substack{a_1 \mapsto \sigma_1 \\ a_2 \mapsto \sigma_2 \\ a_3 \mapsto \sigma_3}}{\longrightarrow} C_2^3 \longrightarrow 1,$$

за $i = 26, \ldots 35$. Прилагаме теорема 3.2.1. Препятствията за разрешимост на задачите за вложимост $(K/k, G_i, N)$ са дадени в таблица 1:

Таблица 1

i	препятствия
26	$(ac, ac), (ab, b)(c, c)$
27	$(a, c), (a, b)$
28	$(a, c), (b, ab)$
29	$(a, c), (a, ab)(b, b)$
30	$(a, c), (c, c)(a, b)$
31	$(b, b)(a, c), (c, c)(a, b)$
32	$(b, b)(a, c), (a, a)(c, c)(a, b)$
33	$(b, b)(a, c), (b, b)(c, c)(a, b)$
34	$(ac, c), (ab, b)$
35	$(ac, c), (a, ab)(b, b)$

3.2.2 Групи, притежаващи фактор-група от вида $H \times C_2$

Групите, които при факторизиране с централен елемент от ред 2 имат фактор-група от вида $H \times C_2$ са четири: G_{38}, G_{42}, G_{43} и G_{44}.

Групата G_{38}.

Центърът $Z(G_{38}) = \langle a_1, a_4, a_5 \rangle = \langle a_1 \rangle$ е изоморфен на цикличната група C_8, а фактор-групата $G_{38}/\langle a_5 \rangle$ е изоморфна на $C_4 \times C_2^2$. Нека a, b и c са квадратично независими и $(a, a) = 1 \in \mathrm{Br}(k)$. Тогава $K/k = k(\sqrt{r(a + \sqrt{a})}, \sqrt{b}, \sqrt{c})/k$ е $C_4 \times C_2^2$ разширение за всяко $r \in k^*$. От теорема 3.2.2 следва, че задачата за вложимост зададена чрез K/k и груповото разширение

$$1 \longrightarrow \mu_2 \cong \langle a_5 \rangle \longrightarrow G_{38} \underset{\substack{a_1 \mapsto \rho_1 \\ a_2 \mapsto \rho_2 \\ a_3 \mapsto \rho_3}}{\longrightarrow} C_4 \times C_2^2 \longrightarrow 1$$

е разрешима тогава и само тогава, когато

$$(a,2)(-1,r)(b,c)=1\in \mathrm{Br}(k).$$

За останалите три групи имаме, че фактор-групата по цикличната подгрупа $\mu_2\cong\langle a_5\rangle$ е изоморфна на групата $D_8\times C_2\cong\langle\sigma,\tau\rangle\times\langle\rho\rangle$, значи можем да приложим теорема 3.2.4. Сега ще разгледаме следните три задачи за вложимост зададени чрез $D_8\times C_2$ разширение K/k и груповите разширения

$$1\longrightarrow \mu_2\cong\langle a_5\rangle\longrightarrow G_i \underset{\substack{a_2a_1\mapsto\sigma\\ a_2\mapsto\tau\\ a_3\mapsto\rho}}{\longrightarrow} D_8\times C_2\longrightarrow 1,$$

за $i=42,43,44$. Във всичките три случая имаме, че $(a,ab)=1$ е необходимо условие за образуването на задачите за вложимост. Препятствията за разрешимост на задачите за вложимост $(K/k,G_i,\langle a_5\rangle)$ са дадени в таблица 2:

Таблица 2

i	препятствия
42	$(a,2)(-b,2\alpha_1 r)(c,c)$
43	$(a,2c)(-b,2\alpha_1 r)$
44	$(a,-2c)(-b,2\alpha_1 r)(b,b)$

Да забележим, че препятствието за $i=43$ е произведение на две кватернионни алгебри. По тази причина ние можем да опишем в явен вид всички разширения на Галоа реализиращи групата G_{43}. Първо, ще направим параметризация на всички G_{43} разширения в общия случай, когато $b\neq_2 -1$, т.е. b и -1 са независими mod k^{*2} (за краткост ще използваме символа $=_2$ за да означим, че два елемента са квадратично зависими, и ще пишем $\neq_2$ ако те са независими).

Преди да продължим с описанието на G_{43} разширенията, ще дадем някои означения, следвайки [Le3]. За $a,b\in k^*$, *кватернионната алгебра* $(a,b/k)$ е k-алгебрата, породена от елементи α и β със съотношения $\alpha^2=a,\beta^2=b$ и $\beta\alpha=-\alpha\beta$. Класът на еквивалентност като елемент в групата на Брауер $\mathrm{Br}(k)$ бележим с (a,b). С тази кватернионна алгебра асоцииране квадратичната форма в каноничен вид $\langle a,b,-ab\rangle = ax^2+by^2-abz^2$. Тогава $(a,b/k)$ се разпада тогава и само тогава, когато $\langle a,b,-ab\rangle$

е изотропна (т.е. представя 0). Две кватернионни алгебри $(a, b/k)$ и $(c, d/k)$ са изоморфни тогава и само тогава, когато квадратичните форми $\langle a, b, -ab\rangle$ и $\langle c, d, -cd\rangle$ са еквивалентни. За удобство, ще означаваме с $\langle a, b, -ab\rangle$ също така диагоналната матрица $diag(a, b, -ab)$. Тогава еквивалентността на квадратичните форми $\langle a, b, -ab\rangle$ и $\langle c, d, -cd\rangle$ се изразява чрез матричното уравнение $\mathbf{P}^t\langle a, b, -ab\rangle\mathbf{P} = \langle c, d, -cd\rangle$, за някоя неособена 3×3 матрица $\mathbf{P}$ над k.

Теорема 3.2.7. ([Mi7, Theorem 5.1]) *Нека K/k е $D_8 \times C_2$ разширение както по-горе, и нека $\alpha_1 \neq 0$. Тогава задачата за вложимост $(K/k, G_{43}, \langle a_5\rangle)$ е разрешима тогава и само тогава, когато квадратичните форми $\langle b, r\alpha_1 c, br\alpha_1 c\rangle$ и $\langle ab, 2ca, 2bc\rangle$ са еквивалентни над k. Ако тази еквивалентност се изразява чрез матрицата $\mathbf{Q}$, т.е. ако*

$$\mathbf{Q}^t\langle b, r\alpha_1 c, br\alpha_1 c\rangle\mathbf{Q} = \langle ab, 2ca, 2bc\rangle,$$

можем да считаме, че $det\ \mathbf{Q} = 2a/\alpha_1 r$ и да получим решенията

$$K(\sqrt{s\omega})/k = k(\sqrt{s\omega}, \sqrt{b}, \sqrt{c})/k,\ \ s \in k^*,$$

където

$$\omega = 1 - q_{11}/\sqrt{a} + \frac{1}{2}(q_{32} + q_{23}/\sqrt{a})\sqrt{r\alpha} + \frac{1}{2}(q_{22}/b - q_{33}/\sqrt{a})\sqrt{r\alpha'}/\sqrt{a}.$$

Доказателство: Препятствието на задачата за вложимост е $(a, 2c)(-b, 2r\alpha_1)$, което е еквивалентно на $(-ab, -2ca)(-b, -r\alpha_1 c) \in \mathrm{Br}(k)$. Това доказва първата част на условието.

Да разгледаме сега задачата за вложимост зададена чрез $K/k(\sqrt{c})$ и груповото разширение

$$1 \longrightarrow \mu_2 \cong \langle a_5\rangle \longrightarrow D_{16} \cong \langle a_2a_1, a_2\rangle \underset{\substack{a_2a_1\mapsto\sigma\\ a_2\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1.$$

Дефинираме матрицата $\mathbf{P}$ с елементи от $k(\sqrt{c})$ по следния начин:

$$\mathbf{P} = \langle 1, \sqrt{c}, \sqrt{c}\rangle\mathbf{Q}\langle 1, 1/\sqrt{c}, 1/\sqrt{c}\rangle,$$

така че получаваме

$$\mathbf{P}^t\langle b, r\alpha_1, br\alpha_1\rangle\mathbf{P} = \langle ab, 2a, 2b\rangle.$$

Тъй като подгрупата породена от a_2a_1 и a_2 е изоморфна на D_{16}, получаваме критерият даден в [Le3]. Тогава $K(\sqrt{s\omega})/k(\sqrt{c})$, за $s \in k^*$ са всички решения на задачата

за вложимост $(K/k(\sqrt{c}), D_{16}, \mu_2)$, където

$$\omega = 1 - p_{11}/\sqrt{a} + \frac{1}{2}(p_{32} + p_{23}/\sqrt{a})\sqrt{r\alpha} + \frac{1}{2}(p_{22}/b - p_{33}/\sqrt{a})\sqrt{r\alpha'}/\sqrt{a}.$$

(Елементите на $\mathbf{P}$ и $\mathbf{Q}$ са p_{ij} и q_{ij}, $i, j = 1, 2, 3$.) Лесно се показва, че $p_{11} = q_{11}, p_{23} = q_{23}, p_{32} = q_{32}, p_{22} = q_{22}$ и $p_{33} = q_{33}$. Нататък, $K(\sqrt{s\omega})/k$ е разширение на Галоа, понеже $\rho\omega = \omega$. Остава само да се покаже, че това е точно G_{43} разширение, като се проверят съотношенията в групата. □

Сега ще дадем описание на G_{43} разширенията в частия случай, когато b и -1 са квадратично зависими.

Теорема 3.2.8. ([Mi7, Theorem 5.2]) *Нека $K/k = k(\sqrt[4]{a}, i, \sqrt{c})/k$ е $D_8 \times C_2$ разширение. Тогава задачата за вложимост $(K/k, G_{43}, \langle a_5 \rangle)$ е разрешима тогава и само тогава, когато*

$$\exists p, q \in k \ : \ p^2 - aq^2 = 2c.$$

В този случай, всички решения са

$$K(\sqrt{s\omega})/k, \ s \in k^*,$$

където $\omega = (p + q\sqrt{a})\sqrt[4]{a}$.

Доказателство: Препятствието на задачата за вложимост е $(a, 2c) \in \mathrm{Br}(k)$, значи съществуват $p, q \in k$ такива, че $p^2 - aq^2 = 2c$. Полагаме $\omega = (p + q\sqrt{a})\sqrt[4]{a}$. Тогава имаме $\sigma\omega/\omega = a_\sigma^2$, където

$$a_\sigma = \frac{\sqrt{c}(1+i)}{p + q\sqrt{a}} \in K;$$

$\tau\omega/\omega = 1$ и $\rho\omega/\omega = 1$. Следователно $K(\sqrt{s\omega})/k$ е разширение на Галоа. Тук е лесно да се покаже, че това е точно G_{43} разширеине. Очевидно, $a_2^2 = 1$ и $a_3^2 = 1$. Нататък, $a_\sigma \sigma a_\sigma \sigma^2 a_\sigma \sigma^3 a_\sigma = -1$, откъдето $a_2 a_1$ има ред 8. Също така, $a_2 a_1 \sqrt{s\omega} = a_\sigma \sqrt{s\omega}, a_2\sqrt{s\omega} = \pm\sqrt{s\omega}$ и $a_3\sqrt{s\omega} = \pm\sqrt{s\omega}$. Тогава $[a_2, a_3]\sqrt{s\omega} = \sqrt{s\omega}$, откъдето $[a_2, a_3] = 1$; и $[a_1, a_3]\sqrt{s\omega} = -\sqrt{s\omega}$, откъдето $[a_1, a_3] \neq 1$, но $[a_1, a_3]^2 = 1$. □

За нашите разглеждания по-нататък се нуждаем от така нареченото свойство на *общия слот* (виж [La, Ch. III, Exercise 12]).

Лема 3.2.9. *Нека $a, b, c, d \in k^*$. Тогава $(a, b)(c, d) = 1 \in \mathrm{Br}(k) \iff \exists x \in k^*$, така че $(a, bx) = (c, dx) = (ac, x) = 1$.*

Теорема 3.2.10. ([Mi7, Theorem 5.4]) *От реализирането на G_{44} като група на Галоа над k следва реализирането на G_{43} (т.е. имаме автоматичната реализация $G_{44} \Rightarrow G_{43}$).*

Доказателство: В зависимост от поведението на елементите -1 и 2 имаме следните случаи.

1. -1 и 2 са квадратично независими над k. Ако ни е дадено, че G_{44} се реализира като група на Галоа, ще имаме, че $|k/k^{*2}| \geq 8$. Полагаме $b = -1$ и $c = 2$: $(a, 1) = (a, 4)(1, 2\alpha_1 r) = 1$ за всяко a – квадратично независимо с -1 и 2. По този начин, получаваме нещо повече в този случай: ако $|k/k^{*2}| \geq 8$, групата G_{43} се реализира.

2. $-1 \in k^{*2}$. Тогава препятствията за реализирането на групите G_{43} и G_{44} са идентични: $(a, 2c)(b, 2\alpha_1 r) \in \mathrm{Br}(k)$.

3. $-1 \notin k^{*2}, 2 \in k^{*2}$ и $-2 \notin k^{*2}$. Тогава G_{43} се реализира тогава и само тогава, когато
$$(a, -b) = (a, c)(-b, \alpha_1 r) = 1;$$
и G_{44} се реализира тогава и само тогава, когато
$$(a, -b) = (a, -c)(-b, \alpha_1 r)(b, -1) = 1.$$
Нека сега G_{44} се реализира за някои a, b и c. Разглеждаме следните под-случаи.

Ако $a =_2 -b$, то $(a, c)(-b, \alpha_1 r) = (-b, \alpha_1 rc) = 1$ за $r = \alpha_1 c$, значи G_{43} се реализира.

Ако $a =_2 -1$, то $(-1, -b) = 1$ и $(b, -1) = (-1, -1)$. Оттук
$$(a, -c)(-b, \alpha_1 r)(b, -1) = (-1, c)(-1, -1)(-b, \alpha_1 r)(b, -1) =$$
$$= (-1, c)(-b, \alpha_1 r) = 1.$$

Ако $b =_2 -1$, то $(a, -c)(-1, -1) = 1$. Използваме свойството на общия слот: $(a, -c)(-1, -1) = 1 \iff \exists y \in k^*$, така че $(a, -cy) = (-1, -y) = (-a, y) = 1$. Ако $(a, a) = 1$, то можем да положим $b' = -a$ (квадратично независимо с a): $(a, -b') = (a, a) = 1$ и $(a, c)(-b', \alpha_1 r) = (a, \alpha_1 rc) = 1$ за $r = \alpha_1 c$. Сега имаме няколко възможности:

Ако $-cy =_2 a$, то $(a, a) = 1$ и G_{43} се реализира, както току що показахме.

Ако $-cy =_2 -1$, то отново $(a, a) = 1$.

Ако $-cy \in k^{*2}$, то $y =_2 -c, (-1, -y) = (-1, c) = 1$ и $(-a, y) = (-a, -c) = 1$. В този случай можем да положим $a' = -a$ и $c' = -c$. Тогава $a', -1$ и c' са отново квадратично независими. По този начин, $(a', 1) = (a', c')(1, \alpha_1 r) = 1$.

Ако $-cy =_2 -a$, то $y =_2 ca, (-1, -y) = (-1, -ca) = 1$ и $(-a, ca) = (-a, c) = 1$. Можем да положим $a' = -a$ и да получим $(a', 1) = (a', c)(1, \alpha_1 r) = 1$.

Ако $-1, a$ и $-cy$ са квадратично независими, то можем да положим $c' = -cy : (a, c') = 1$, откъдето G_{43} отново се реализира.

Ако a, b и -1 са квадратично независими, можем да положим $c = -b : (a, -b) = (a, -b)(-b, \alpha_1 r) = 1$ за $r = \alpha_1$.

Последният случай е:

4. $-1 \notin k^{*2}, 2 \notin k^{*2}$ и $-2 \in k^{*2}$. Тогава G_{43} се реализира тогава и само тогава, когато

$$(a, -b) = (a, -c)(-b, -\alpha_1 r) = 1;$$

и G_{44} се реализира тогава и само тогава, когато

$$(a, -b) = (a, c)(-b, -\alpha_1 r)(b, -1) = 1.$$

Нека сега G_{44} се реализира за някои a, b и c. Да разгледаме следните под-случаи.

Ако $a =_2 -b$, то $(a, -c)(-b, -\alpha_1 r) = (-b, \alpha_1 rc) = 1$ за $r = \alpha_1 c$, значи G_{43} се реализира.

Ако $a =_2 -1$, то $(-1, -b) = 1$ и $(b, -1) = (-1, -1)$. Оттук

$$(a, c)(-b, -\alpha_1 r)(b, -1) = (-1, -c)(-1, -1)(-b, -\alpha_1 r)(b, -1) =$$
$$= (-1, -c)(-b, -\alpha_1 r) = 1.$$

Ако $b =_2 -1$, то $(a, c)(-1, -1) = 1$. Аналогично на съответния подслучай на случай 3, получаваме, че G_{43} се реализира.

Накрая:

Ако a, b и -1 са квадратично независими, полагаме $c =_2 -1 : (a, -c)(-b, -\alpha_1 r) = 1$ за $r = -\alpha_1$. □

Теорема 3.2.11. ([Mi7, Theorem 5.5]) *Нека K/k е $D_8 \times C_2$ разширение както в теорема 3.2.7 или 3.2.8, и нека $(ab, ab) = 1 \in \mathrm{Br}(k)$. В този случай съществуват $\gamma_1, \gamma_2 \in k$ такива, че $\gamma_1^2 - ab\gamma_2^2 = ab$. Тогава препятствията за разрешимост на задачите за вложимост $(K/k, G_{44}, \langle a_5 \rangle)$ и $(K/k, G_{43}, \langle a_5 \rangle)$ са идентични и решенията на задачата за вложимост $(K/k, G_{44}, \langle a_5 \rangle)$ са*

$$K(\sqrt{s(\gamma_1 + \sqrt{ab}\gamma_2)\omega})/k, \ s \in k^*,$$

където ω е както в теорема 3.2.7 или 3.2.8.

Доказателство: Полагаме $\gamma = \gamma_1 + \sqrt{ab}\gamma_2$. Тогава $\sigma(\gamma\omega)/(\gamma\omega) = a_\sigma^2, \tau(\gamma\omega)/(\gamma\omega) = a_\tau^2, \rho(\gamma\omega)/(\gamma\omega) = 1$, където $a_\sigma \sigma a_\sigma \sigma^2 a_\sigma \sigma^3 a_\sigma = -1, a_\tau \tau a_\tau = -1$. Оттук $|a_2 a_1| = 8, |a_2| = 4$ и $|a_3| = 2$. Следователно $K(\sqrt{s\gamma\omega})/k$ е разширение на Галоа. □

3.2.3 Групите G_6, G_7 и G_8

Групата G_6

Първо, да вземем групата от ред 64 с номер 32 в библиотеката на 2-групите в GAP [GAP] и да я означим с $G_{(64,32)}$. Тя има ранг 2 и се поражда от елементи $b_1, \ldots, b_6$ такива, че $b_1^2 = b_4, b_2^2 = 1, [b_2, b_1] = b_3, b_3^2 = 1, [b_3, b_1] = b_5, [b_3, b_2] = 1, b_4^2 = 1, [b_4, b_2] = b_5, [b_4, b_3] = b_6, b_5^2 = 1, [b_5, b_1] = b_6, b_6^2 = 1, [b_5, b_2] = [b_5, b_3] = [b_5, b_4] = 1$ и $\langle b_6 \rangle$ е центърът на $G_{(64,32)}$. Пулбекът $G = D \curlywedge C$ се поражда от елементи x и y такива, че $x^4 = y^2 = 1, [y, x] = z, z^2 = 1$ и z е централен. Полагаме $E_4 = \langle b_5, b_6 \rangle \cong C_2^2$. Да забележим, че $b_1 b_5 b_1^{-1} = b_5 b_6$ и $b_i b_5 b_i^{-1} = b_5$ за $i = 2, \ldots, 6$. Да разгледаме груповото разширение

$$1 \longrightarrow E_4 \longrightarrow G_{(64,32)} \underset{\substack{b_1 \mapsto x \\ b_2 \mapsto y}}{\longrightarrow} G \cong D \curlywedge C \longrightarrow 1. \tag{3.15}$$

Нататък, полагаме $H = \langle x^2, y, z \rangle \cong C_2^3$ и $\mathcal{H} = \langle b_2, \ldots, b_6 | b_2^2 = \cdots = b_6^2 = 1, [b_4, b_2] = b_5, [b_4, b_3] = b_6 \rangle$ – про-образът на H в $G_{(64,32)}$. Очевидно, $\mathcal{H}$ лежи в централизатора на E_4 в $G_{(64,32)}$. Имаме груповото разширение $1 \longrightarrow E_4 \longrightarrow \mathcal{H} \longrightarrow H \longrightarrow 1$. Означаваме с c_1 2-кокласа в $H^2(G, \mu_2)$, представен от груповото разширение

$$1 \longrightarrow E_4/\langle b_6 \rangle \cong \mu_2 \longrightarrow G_{(64,32)}/\langle b_6 \rangle \underset{\substack{a_1 \mapsto x \\ a_2 \mapsto y}}{\longrightarrow} G \cong D \curlywedge C \longrightarrow 1,$$

където $G_{(64,32)}/\langle b_6 \rangle$ е изоморфна на групата $G_{(32,6)}$, означена в таблица 1 като G_6. Означаваме с c_2 2-кокласа в $H^2(H, \mu_2)$, представен от груповото разширение

$$1 \longrightarrow E_4/\langle b_5\rangle \cong \mu_2 \longrightarrow \mathcal{H}/\langle b_5\rangle \underset{\substack{a_4\mapsto\sigma\\ a_2\mapsto\tau}}{\longrightarrow} H \longrightarrow 1,$$

където $\mathcal{H}/\langle b_5\rangle$ е изоморфна на директното произведение $D_8 \times C_2$. Според точка 3.1.1, всички $D \curlywedge C$-разширения L/F могат да се опишат по следния начин:

$$L/F = F\left(\sqrt{s(\beta_1+\beta_2\sqrt{b})}, \sqrt{r(\alpha_1+\alpha_2\sqrt{a})}\right)/F,$$

където $\alpha_1^2 - a\alpha_2^2 = a$ и $a = \beta_1^2 - b\beta_2^2$ за някои $\alpha_1, \alpha_2, \beta_1, \beta_2, r, s \in F$. Имаме, че

$$\begin{aligned}\sqrt{s(\beta_1+\beta_2\sqrt{b})} &= \frac{1}{2}\left(\sqrt{2s(\beta_1+\sqrt{a})} \pm \sqrt{2s(\beta_1-\sqrt{a})}\right)\\ \sqrt{r(\alpha_1+\alpha_2\sqrt{a})} &= \frac{1}{2}\left(\sqrt{2r(\alpha_1+\sqrt{a})} \pm \sqrt{2r(\alpha_1-\sqrt{a})}\right).\end{aligned}$$

Оттук L може да се запише във вида

$$L = K\left(\sqrt{b}, \sqrt{2r(\alpha_1-\sqrt{a})}, \sqrt{2s(\beta_1+\sqrt{a})}\right),$$

където $K = F(\sqrt{a})$ е неподвижното подполе на $H \cong C_2^3$.

Както знаем, препятствието на задачата за вложимост $(L/K, \mathcal{H}/\langle b_5\rangle, \mu_2)$ зададена чрез c_2 е $(2r(\alpha_1-\sqrt{a}), 2s(\beta_1+\sqrt{a}))_K \in \mathrm{Br}_2(K)$. Нататък, от теореми 2.3.3 и 2.3.7 следва, че задачата за вложимост $(L/F, G_{(64,32)}, E_4)$ зададена чрез (3.15) е подходящо разрешима тогава и само тогава, когато $(2r(\alpha_1-\sqrt{a}), 2s(\beta_1+\sqrt{a}))_K = 1 \in \mathrm{Br}_2(K)$.

Да положим $E = F(\sqrt{a}, \sqrt{b})$ и $\gamma = \alpha_1 + \beta_1 + \alpha_2\sqrt{a} + \beta_2\sqrt{b}$. Тогава за норменото изображение N са в сила равенствата $N_{E/F(\sqrt{a})}(\gamma) = d\alpha$ и $N_{E/F(\sqrt{b})}(\gamma) = d\beta$, където $d = 2(\alpha_1+\beta_1), \alpha = \alpha_1 + \alpha_2\sqrt{a}, \beta = \beta_1 + \beta_2\sqrt{b}$. От теорема 2.3.8 следва, че $c_1 = \mathrm{cor}_{G/H}(c_2)$, така че можем да пресметнем препятствието на задачата $(L/F, G_{(32,6)}, \mu_2)$ съответстваща на c_1, като приложим лема 2.3.10:

$$\begin{aligned}&\mathrm{cor}_{K/F}((2r(\alpha_1-\sqrt{a}), 2s(\beta_1+\sqrt{a}))_K)\\ =\ &(4r^2(\alpha_1^2-a), -2r(-2s\beta_1 2r - 2r\alpha_1 2s))_F(4s^2(\beta_1^2-a), 2s(4sr\beta_1 + 4rs\alpha_1))_F\\ =\ &(4r^2a\alpha_2^2, 2r4rs(\alpha_1+\beta_1))_F(4s^2b\beta_2^2, 2s4rs(\alpha_1+\beta_1))_F\\ =\ &(a, sd)_F(b, rd)_F.\end{aligned}$$

Тъй като препятствието е произведение на две кватернионни алгеби, можем да опишем всички $G_{(32,6)}$ разширения.

Теорема 3.2.12. ([Mi7, Theorem 6.1],[Mi5, Theorem 5.1]) *Препятствието за разрешимост на задачата за вложимост* $(L/F, G_{(32,6)}, \mu_2)$ *е* $(b, dr)(a, ds) \in \mathrm{Br}_2(F)$. *Ако* $(b, dr)(a, ds) = 1 \in \mathrm{Br}_2(F)$, *то съществуват елементи* $\delta_1, \delta_2, \delta_3 \in E$ *и* $v \in F^*$ *такива, че* $drv = N_{E/F(\sqrt{a})}(\delta_1), dsv = N_{E/F(\sqrt{b})}(\delta_2), v = N_{E/F(\sqrt{a})}(\delta_3) = N_{E/F(\sqrt{b})}(\delta_3)$, *и*

$$M/F = E(\sqrt{r\alpha}, \sqrt{s\beta}, \sqrt{t\delta_1\delta_2\delta_3})/F,\ t \in F^*$$

са всички разширения на Галоа, решаващи задачата за вложимост $(L/F, G_{(32,6)}, \mu_2)$.

Доказателство: Препятствието вече го пресметнахме. Нека $(b, dr)(a, ds) = 1 \in \mathrm{Br}(k)$. От свойството на общия слот (лема 3.2.9) следва, че съществува $v \in k^*$ такова, че $(b, drv) = (a, dsv) = (ab, v) = 1$. Тогава трябва да съществуват елементи $\delta_1, \delta_2, \delta_3 \in E$ и $v \in k^*$, както в условието на теоремата. Да припомним, че $N_{E/k(\sqrt{a})}(\gamma) = d\alpha$ и $N_{E/k(\sqrt{b})}(\gamma) = d\beta$. Полагаме $\delta = \gamma\delta_1\delta_2\delta_3$. Тогава

$$N_{E/k(\sqrt{a})}(\delta) = d^2v^2\delta_2^2 r\alpha \in K^{*2}$$

и

$$N_{E/k(\sqrt{b})}(\delta) = d^2v^2\delta_1^2 s\beta \in K^{*2}.$$

Следователно $M/k = E(\sqrt{r\alpha}, \sqrt{s\beta}, \sqrt{t\delta})/k, t \in k^*$ е разширение на Галоа.

Сега ще покажем, че M/k е G_6 Разширение. За удобство, ще считаме, че $t = 1$. Пресмятанията показват, че $y\delta/\delta = a_y^2$, за $a_y = dv\sqrt{r\alpha}/(\gamma\delta_1\delta_3)$ и $x\delta/\delta = a_x^2$, за $a_x = dv\sqrt{s\beta}/(\gamma\delta_2\delta_3)$. Следователно, $a_y y a_y = 1$, значи про-образът на y в $\mathrm{Gal}(M/k)$ има ред 2, и $a_x x a_x x^2 a_x x^3 a_x = 1$, значи про-образът на x има ред 4. Означаваме про-образите на x, y и z с a_1, a_2 и a_3, съответно. Тъй като $z\delta/\delta = [z, x]\delta/\delta = 1$, получаваме, че a_3 и $[a_3, a_1]$ имат ред 2. Допълнителната проверка установява, че останалите съотношения в групата G_6 също се удовлетворяват. □

Групите G_7 и G_8

Тук ще разгледаме групите от ред 32 с номера 7 и 8 – $G_{(32,7)}$ и $G_{(32,8)}$. (В таблица 1 те са означени с G_7 и G_8.) Нека L/F е $D \curlywedge C$ разширение, според описанието от точка 3.1.1. Да означим с $O_{G_{(32,7)}}$ и $O_{G_{(32,8)}}$ препятствията на задачите за вложимост зададени съответно чрез груповите разширения

$$1 \longrightarrow \langle a_5 \rangle \cong \mu_2 \longrightarrow G_{(32,7)} \underset{\substack{a_1 \mapsto x \\ a_2 \mapsto y}}{\longrightarrow} G \cong D \curlywedge C \longrightarrow 1$$

и

$$1 \longrightarrow \langle a_5 \rangle \cong \mu_2 \longrightarrow G_{(32,8)} \underset{\substack{a_1 \mapsto x \\ a_2 \mapsto y}}{\longrightarrow} G \cong D \leftthreetimes C \longrightarrow 1.$$

Сега можем да пресметнем тези препятствия.

Теорема 3.2.13. ([Mi5, Proposition 5.2]) $O_{G_{(32,7)}} = (b, dr)(a, 2ds)(-1, r) \in \mathrm{Br}_2(F)$.

Доказателство: Да забележим, че $\{a_1, a_2\}$ е минимално пораждащо множество за двете групи $G_{(32,7)}$ и $G_{(32,6)}$, и още, че $G_{(32,7)} = G_{(32,6)}^{(8,x)}$. Тъй като препятствието на задачата за вложимост зададена с груповото разширение $1 \longrightarrow \mu_2 \longrightarrow C_8 \longrightarrow C_4 \longrightarrow 1$ в нашата ситуация е $(a, 2)(-1, r) \in \mathrm{Br}_2(F)$, получаваме разлагането, дадено в условието. □

Теорема 3.2.14. ([Mi5, Proposition 5.3]) $O_{G_{(32,8)}} = (b, -dr)(a, 2ds)(-1, r) \in \mathrm{Br}_2(F)$.

Доказателство: Тук отново $\{a_1, a_2\}$ е минимално пораждащо множество за групата $G_{(32,8)}$. Имаме, че $G_{(32,8)} = G_{(32,7)}^{(4,y)}$. Следователно, $O_{G_{(32,8)}} = O_{G_{(32,7)}}(b, -1)$. □

От последните две теореми може лесно да се докаже, че е в сила автоматичната реализация $G_{(32,8)} \implies G_{(32,7)}$.

Глава 4
Препятствия за реализиране на p-групи като групи на Галоа

В тази глава пресмятаме препятствията за реализирането на редица p-групи. Даваме също така описание на разширенията на Галоа, които реализират тези групи. В параграф 4.1 разглеждаме неабеловите групи от ред p^3, в параграф 4.2 се спираме на четири неабелови групи от ред p^4. Най-важните резултати са изложени в параграф 4.3, където задълбочено изследваме модулярната p-група, както и някои нейни производни групи. Тези резултати са публикувани в работите [Mi3, Mi4].

4.1 Двете неабелови групи от ред p^3 като групи на Галоа

В този параграф ще изследваме реализирането на двете неабелови групи от ред p^3 за p-нечетно просто число. Първата е групата на Хайзенберг с експонента p. Означаваме я с G_1, а нейните пораждащи с g_1, g_2 и g_3, за които имаме съотношенията $g_1^p = g_2^p = g_3^p = 1, g_1g_2 = g_2g_1g_3$ и g_3 е централен. Групата на Хайзенберг е дискутирана например в [JLY, Ma, MS2] и [Br]. Нека $K = k(\sqrt[p]{a}_1, \sqrt[p]{a}_2)$ е $C_p \times C_p$ разширение на k и нека $K_i = k(\sqrt[p]{a}_i), i = 1, 2$. Означаваме с H групата на Галоа на K/k и пораждащите на H с σ_1 и σ_2 такива, че $\sigma_i(\sqrt[p]{a_j})/\sqrt[p]{a_j} = \zeta^{\delta_{ij}}, i = 1, 2$.

Теорема 4.1.1. ([Mi3, Theorem 3.1]) *Задачата за вложимост зададена чрез K/k и груповото разширение*

$$1 \longrightarrow \langle g_3 \rangle \cong C_p \longrightarrow G_1 \underset{\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}}{\longrightarrow} H \longrightarrow 1$$

е разрешима тогава и само тогава, когато $a_2 \in N_{K_1/k}(K_1^*)$. В този случай, за $\omega \in K_1^*$ такова, че $N(\omega) = a_2$ полагаме $\alpha = \omega^{p-1}\sigma_1(\omega)^{p-2} \cdots \sigma_1^{p-2}(\omega)$. Тогава множеството $\{K(\sqrt[p]{f\alpha}) \mid f \in k^*\}$ дава всички решения.

Доказателство: От следствие 2.2.2 можем лесно да пресметнем препятствието: $(a_1, a_2; \zeta) \in \mathrm{Br}(k)$. Следователно, задачата за вложимост е разрешима тогава и само тогава, когато $a_2 \in N_{K_1/k}(K_1^*)$.

Нека сега $\omega \in K_1^*$ е такова, че $N_{K_1/k}(\omega) = a_2$ и нека α е както в условието на теоремата. Пресмятанията показват, че $\sigma_2(\alpha) = \alpha$ и $\sigma_1(\alpha) = \alpha x^p$, където $x = \sqrt[p]{a_2}/\omega \in K^*$. Следователно, $L = K(\sqrt[p]{f\alpha})$ е разширение на Галоа над k. Нататък, $x\sigma_1(x)\cdots\sigma_1^{p-1}(x) = 1$, значи про-образът на σ_1 в $\mathrm{Gal}(L/k)$ има ред p. Същото важи за σ_2, откъдето $\mathrm{Gal}(L/k) \cong G_1$. □

Да разгледаме сега другата неабелова група от ред p^3. Означаваме я с G_2, нейните пораждащи с g_1 и g_2, имащи съотношенията $g_1^{p^2} = g_2^p = 1$ и $g_1 g_2 = g_2 g_1^{p+1}$.

Теорема 4.1.2. ([Mi3, Theorem 3.2]) *Задачата за вложимост зададена чрез K/k и груповото разширение*

$$1 \longrightarrow \langle g_1^p \rangle \cong C_p \longrightarrow G_2 \underset{\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}}{\longrightarrow} H \longrightarrow 1$$

е разрешима тогава и само тогава, когато $a_2\zeta \in N_{K_1/k}(K_1^*)$. В този случай, за $\omega \in K_1^*$ такова, че $N(\omega) = a_2\zeta$ полагаме $\alpha = \omega^{p-1}\sigma_1(\omega)^{p-2}\cdots\sigma_1^{p-2}(\omega)$. Тогава множеството $\{K(\sqrt[p]{f\sqrt[p]{a_1}^{-1}\alpha}) \mid f \in k^*\}$ дава всички решения.

Доказателство: От следствие 2.2.2 получаваме, че препятствието е $(a_1, a_2\zeta; \zeta) \in \mathrm{Br}(k)$. Следователно, задачата за вложимост е разрешима тогава и само тогава, когато $a_2\zeta \in N_{K_1/k}(K_1^*)$.

Нека сега $\omega \in K_1^*$ е такова, че $N_{K_1/k}(\omega) = a_2\zeta$, нека α е както в условието на теоремата, и да означим $\alpha_1 = \sqrt[p]{a_1}^{-1}\alpha$. Пресмятанията показват, че $\sigma_2(\alpha_1) = \alpha_1$ и $\sigma_1(\alpha_1) = \alpha_1\beta^p$, където $\beta = \sqrt[p]{a_2}/\omega \in K^*$. Следователно, $L = K(\sqrt[p]{f\alpha_1})$ е разширение на Галоа над k за всяко $f \in k^*$. Нататък, $\beta\sigma_1(\beta)\cdots\sigma_1^{p-1}(\beta) = \zeta^{-1}$, значи про-образът на σ_1 в $\mathrm{Gal}(L/k)$ има ред p^2, откъдето $\mathrm{Gal}(L/k) \cong G_2$. □

4.2 Четири неабелови групи от ред p^4 като групи на Галоа

В този параграф ще анализираме задачи за вложимост, касаещи неабеловите групи от ред p^4, които притежават фактор-група от вида $H \times C_p$ за някоя група H от ред p^2. По принцип има 15 групи от ред p^4 за всяко нечетно просто p. Описанието на тези групи чрез пораждащи и съотношения може да бъде намерено като се използва базата данни, която се намира в компютърната алгебра GAP 4 [GAP]. В някои случаи, обаче описанието зависи от вида на простото число p, така че като цяло не можем да разглеждаме въпроси за реализирането на тези групи за произволни стойности на p. За щастие, споменатите четири неабелови групи притежават описание, което не зависи от избора на p. Разбира се, няма да се спираме на групите $G_1 \times C_p$ и $G_2 \times C_p$, понеже тяхното реализиране като групи на Галоа зависи единствено от реализирането на групите G_1 и G_2. Три от тези четири групи имат за фактор-група $C_{p^2} \times C_p$, а четвъртата има $(C_p)^3$ за фактор-група.

В началото, ще дадем описание на неабеловите групи, притежаващи фактор-групата $C_{p^2} \times C_p$, която се поражда от елементи σ_1 и σ_2 такива, че $\sigma_1^{p^2} = \sigma_2^p = 1$ и $\sigma_1\sigma_2 = \sigma_2\sigma_1$. Представянията на тези групи могат да се дадат чрез съотношенията между техните пораждащи g_1, g_2, g_3 и g_4. Представянията не са минимални, но са удобни за нашите цели. Със символа $[a, b]$ по-надолу означаваме комутатора $a^{-1}b^{-1}ab$.

$$G_3 : g_1^p = g_4, g_2^p = g_3^p = g_4^p = 1, [g_2, g_1] = g_3,\ g_3 \text{ и } g_4 \text{ са централни},$$
$$G_4 : g_1^p = g_4, g_2^p = g_3, g_3^p = g_4^p = 1, [g_2, g_1] = g_3,\ g_3 \text{ и } g_4 \text{ са централни},$$
$$G_5 : g_1^p = g_3, g_3^p = g_4, g_2^p = g_4^p = 1, [g_2, g_1] = g_4,\ g_3 \text{ и } g_4 \text{ са централни}.$$

В сила са следните централни групови разширения:

$$1 \longrightarrow \langle g_3 \rangle \cong \mu_p \longrightarrow G_3 \underset{\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}}{\longrightarrow} C_{p^2} \times C_p \longrightarrow 1, \tag{4.1}$$

$$1 \longrightarrow \langle g_3 \rangle \cong \mu_p \longrightarrow G_4 \underset{\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}}{\longrightarrow} C_{p^2} \times C_p \longrightarrow 1, \tag{4.2}$$

$$1 \longrightarrow \langle g_4 \rangle \cong \mu_p \longrightarrow G_5 \underset{\substack{g_1 \mapsto \sigma_1 \\ g_2 \mapsto \sigma_2}}{\longrightarrow} C_{p^2} \times C_p \longrightarrow 1. \tag{4.3}$$

Последната група, която ще разгледаме се задава с представянето

$$G_6 : g_1^p = g_2^p = 1, g_3^p = g_4, g_4^p = 1, [g_2, g_1] = g_4,\ g_3 \text{ и } g_4 \text{ са централни}.$$

Ако групата $(C_p)^3$ се поражда от елементите ρ_1, ρ_2 и ρ_3, получаваме централното групово разширение:

$$1 \longrightarrow \langle g_4 \rangle \cong \mu_p \longrightarrow G_6 \underset{g_i \mapsto \rho_i}{\longrightarrow} (C_p)^3 \longrightarrow 1. \tag{4.4}$$

4.2.1 Препятствия и разширения на Галоа

Нашата първа цел е да намерим препятствията за реализирането на тези четири групи като групи на Галоа с помощта на задачи за вложимост, асоциирани със съответните централни групови разширения.

Нека k е поле с характеристика $\neq p$, нека ζ е примитивен p-ти корен на единицата в k за нечетно просто число p, и нека a_1, a_2 са елементи от k^*, линейно независими по модул k^{*p}. Означаваме $K = k(\sqrt[p]{a_1}, \sqrt[p]{a_2})$ и $K_i = k(\sqrt[p]{a_i}), i = 1, 2$. Нека да приемем, че задачата за вложимост $(K_1/k, C_{p^2}, \mu_p)$ е разрешима. Тогава $(a_1, \zeta; \zeta) = 1$, значи съществува $\alpha \in K_1$, за което $\zeta = N_{K_1/k}(\alpha)$. Да изберем някое C_{p^2} разширение над k: $L_1 = K_1(\sqrt[p]{f_1\beta})$, където $f_1 \in k^*$ и $\beta = \sqrt[p]{a_1}(\alpha^{p-1}\sigma_1(\alpha)^{p-2} \cdots \sigma_1^{p-2}(\alpha))^{-1}$. Тогава имаме $C_{p^2} \times C_p$ разширение $L = L_1(\sqrt[p]{a_2})$. Ще намерим препятствията и ще опишем разширенията в следващите три теореми.

Теорема 4.2.1. ([Mi3, Theorem 4.1]) *Препятствието на задачата за вложимост зададена чрез L/k и груповото разширение* (4.1) *е $(a_2, a_1; \zeta)$. Ако задачата е разрешима, т.е. $a_2 = N_{K_1/k}(\omega)$ за $\omega \in K_1^*$, можем да положим*

$$\gamma = \omega^{p-1}\sigma_1(\omega)^{p-2} \cdots \sigma_1^{p-2}(\omega).$$

Тогава всички разширения на Галоа, реализиращи G_3 са $\{L(\sqrt[p]{f_2\gamma})/k \mid f_2 \in k^*\}$.

Доказателство: Тъй като про-образът на групата C_{p^2} в G_3 е изоморфен на $C_{p^2} \times C_p$, алгебрата на кръстосаното произведение $[L_1, C_{p^2}, \zeta]$ е тривиална в $\mathrm{Br}(k)$. От теорема 2.2.1 тогава следва, че препятствието за разрешимостта на нашата задача е $(a_1, a_2; \zeta^{-1}) = (a_2, a_1; \zeta)$.

Нека сега $(a_2, a_1; \zeta) = 1 \in \mathrm{Br}(k)$ и нека γ е както в условието на теоремата. Тогава $\sigma_2(\gamma)/\gamma = 1$ и $\sigma_1(\gamma)/\gamma = N_{K_1/k}(\omega)/\omega^p = a_2/\omega^p$. Оттук $\sigma_1(\gamma) = \gamma x^p$ за $x = \sqrt[p]{a_2}/\omega \in K^*$. Следователно $M = L(\sqrt[p]{\gamma})$ е разширение на Галоа над k.

Можем да положим за про-образите g_1 и g_2 на σ_1 и σ_2 в $\mathrm{Gal}(M/k)$, съответно, $g_1(\sqrt[p]{\gamma}) = \sqrt[p]{\gamma}x$ и $g_2(\sqrt[p]{\gamma}) = \sqrt[p]{\gamma}$. Очевидно, $\mathrm{ord}g_2 = p$. От равенствата $g_1^p(\sqrt[p]{\gamma}) = \sqrt[p]{\gamma}a_2/N_{K_1/k}(\omega) = \sqrt[p]{\gamma}$ следва, че $\mathrm{ord}g_1 = \mathrm{ord}\sigma_1 = p^2$. Нататък, лесно може да се

проверят равенствата $g_3(\sqrt[p]{\gamma}) = \sqrt[p]{\gamma}\zeta$ и $[g_3, g_1](\sqrt[p]{\gamma}) = [g_3, g_2](\sqrt[p]{\gamma}) = \sqrt[p]{\gamma}$, откъдето получаваме съотношенията $\mathrm{ord} g_3 = p$ и $[g_3, g_1] = [g_3, g_2] = 1$. Така показахме, че M/k е точно G_3 разширение. □

Теорема 4.2.2. ([Mi3, Theorem 4.2]) *Препятствието на задачата за вложимост зададена чрез разширението на Галоа L/k и груповото разширение* (4.2) *е* $(a_2, a_1\zeta; \zeta)$. *Ако задачата е разрешима, т.е.* $a_1\zeta = N_{K_2/k}(x)$ *за* $x \in K_2^*$, *можем да положим*

$$\omega = \sqrt[p]{a_2}(x^{p-1}\sigma_2(x^{p-2})\sigma_2^2(x^{p-3})\cdots\sigma_2^{p-2}(x))^{-1}.$$

Тогава всички разширения на Галоа, реализиращи G_4 *са* $\{L(\sqrt[p]{f_2\omega})/k \mid f_2 \in k^*\}$.

Доказателство: От теорема 2.2.1 намираме, че препятствието е $(a_2, a_1\zeta; \zeta)$. Нека сега $(a_2, a_1\zeta; \zeta) = 1$ и ω е както в условието. В този случай $\sigma_1(\omega)/\omega = 1$ и $\sigma_2(\omega)/\omega = x^p/a_1 \in K^{*p}$, значи $M/k = L(\sqrt[p]{\omega})/k$ е разширение на Галоа. Можем да положим за про-образите g_1 и g_2 на σ_1 и σ_2 в $\mathrm{Gal}(M/k)$: $g_1(\sqrt[p]{\omega}) = \sqrt[p]{\omega}$ и $g_2(\sqrt[p]{\omega}) = \sqrt[p]{\omega}x/\sqrt[p]{a_1}$. Не е трудно да се провери, че $g_3 = g_2^p$ има ред p и $g_3 = [g_2, g_1]$, което означава, че $\mathrm{Gal}(M/k) \cong G_4$. □

Теорема 4.2.3. ([Mi3, Theorem 4.3]) *Препятствието на задачата за вложимост зададена чрез разширението на Галоа L/k и груповото разширение* (4.3) *е* $[L_1, C_{p^2}, \zeta]$ $(a_2, a_1; \zeta)$. *Ако k съдържа примитивен корен на единицата $\zeta_{p^2} = \sqrt[p]{\zeta}$ от степен p^2, то препятствието е* $(\zeta_{p^2}^{-1}a_2, a_1; \zeta)$. *Ако ни е дадено, че задачата за вложимост е разрешима, т.е.* $\zeta_{p^2}^{-1}a_2 = N_{K_1/k}(y)$, *за някои* $y \in K_1$, *можем да положим*

$$\omega = \sqrt[p^2]{a_1}y^{p-1}\sigma_1(y)^{p-2}\cdots\sigma_1^{p-2}(y).$$

Тогава всички разширения на Галоа, които реализират G_5 *са* $\{L(\sqrt[p]{f\omega})/k \mid f \in k^*\}$.

Доказателство: Тук про-образът на C_{p^2} в G_5 е изоморфен на цикличната група C_{p^3}, а за тази група не е ясно как да изразим алгебрата на кръстосаното произведение $[L_1, C_{p^2}, \zeta]$ като произведение на кватернионни алгебри. Затова ще оставим препятствието в този му вид: $[L_1, C_{p^2}, \zeta](a_2, a_1; \zeta)$. Когато, обаче ζ е в k^{*p}, от [Pi, Ch. 15, §15.1, Cor. b] следва, че $[L_1, C_{p^2}, \zeta] = [K_1, C_p, \zeta_{p^2}] = (a_1, \zeta_{p^2}; \zeta)$. В този случай препятствието приема вида $(a_1, \zeta_{p^2}; \zeta)(a_2, a_1; \zeta) = (\zeta_{p^2}^{-1}a_2, a_1; \zeta)$.

Нека сега да приемем, че $(\zeta_{p^2}^{-1}a_2, a_1; \zeta) = 1$, $L_1 = k(\sqrt[p^2]{a_1})$ и ω е както в условието. В този случай $\sigma_1(\omega)/\omega = a_2/y^p \in L^{*p}$ и $\sigma_2(\omega)/\omega = 1$, значи $M/k = L(\sqrt[p]{\omega})/k$ е разширение на Галоа. Можем да положим за про-образите g_1 и g_2 на σ_1 и σ_2 в $\mathrm{Gal}(M/k)$

: $g_1(\sqrt[p]{\omega}) = \sqrt[p]{\omega}\sqrt[p]{a_2}/y$ и $g_2(\sqrt[p]{\omega}) = \sqrt[p]{\omega}$. Тогава $g_1^{p^2}(\sqrt[p]{\omega}) = \sqrt[p]{\omega}\zeta$ и $[g_2, g_1](\sqrt[p]{\omega}) = \sqrt[p]{\omega}\zeta$, откъдето $g_1^{p^2} = [g_2, g_1]$ има ред p, значи имаме G_5 разширение. □

Сега ще спрем нашето внимание на групата G_6. Да въведем следните означения: Нека $a_1, a_2, a_3 \in k^*, K_i = k(\sqrt[p]{a_i})$ $(i = 1, 2, 3)$, и нека $K/k = k(\sqrt[p]{a_1}, \sqrt[p]{a_2}, \sqrt[p]{a_3})/k$ е C_p^3 разширение с пораждащи ρ_1, ρ_2 и ρ_3, за които $\rho_j(\sqrt[p]{a_i})/\sqrt[p]{a_i} = \zeta^{\delta_{ij}}$ $(i, j = 1, 2, 3$ и δ_{ij} както обикновено е делтата на Кронекер).

Теорема 4.2.4. ([Mi3, Theorem 4.4]) *Препятствието на задачата за вложимост зададена чрез разширението на Галоа K/k и груповото разширение* (4.4) *е* $(a_3, \zeta; \zeta)$ $(a_2, a_1; \zeta)$. *Ако ни е дадено, че* $(a_3, \zeta; \zeta) = (a_2, a_1; \zeta) = 1$, *т.е. съществува* $x \in K_3$ *такова, че* $\zeta = N_{K_3/k}(x)$ *и съществува* $y \in K_2$ *такова, че* $a_1 = N_{K_2/k}(y)$, *можем да положим*

$$\omega = \sqrt[p]{a_3}(y^{p-1}\rho_2(y)^{p-2}\cdots\rho_2^{p-2}(y))^{-1}(x^{p-1}\rho_3(x)^{p-2}\cdots\rho_3^{p-2}(x))^{-1}.$$

Тогава всички разширения на Галоа, реализиращи G_6 *са* $\{K(\sqrt[p]{f\omega})/k \mid f \in k^*\}$.

Доказателство: Препятствието се получава веднага от следствие 2.2.2. Нека сега ω е дефинирано както в условието. Тогава имаме $\rho_1(\omega)/\omega = 1, \rho_2(\omega)/\omega = y^p/a_1 \in K^p$ и $\rho_3(\omega)/\omega = x^p \in K^p$. Следователно $K(\sqrt[p]{\omega})/k$ е разширение на Галоа. Сега можем да положим за про-образите g_1, g_2 и g_3 на ρ_1, ρ_2 и ρ_3 в $\mathrm{Gal}(K(\sqrt[p]{\omega})/k)$: $g_1(\sqrt[p]{\omega}) = \sqrt[p]{\omega}, g_2(\sqrt[p]{\omega}) = \sqrt[p]{\omega}y/\sqrt[p]{a_1}$ и $g_3(\sqrt[p]{\omega}) = \sqrt[p]{\omega}x$. Лесно се проверява, че $g_1^p(\sqrt[p]{\omega}) = \sqrt[p]{\omega}, g_2^p(\sqrt[p]{\omega}) = \sqrt[p]{\omega}, g_3^p(\sqrt[p]{\omega}) = \sqrt[p]{\omega}\zeta$ и $[g_2, g_1](\sqrt[p]{\omega}) = \sqrt[p]{\omega}\zeta$, откъдето получаваме точно G_6 разширение. □

4.2.2 Автоматични реализации

В тази точка ще премахнем изискването примитивен p-ти корен на единицата да се съдържа в основното поле k. Нашето намерение е да опишем както разширенията на Галоа, така и да открием автоматични реализации, както е направено в [Br]. Например, в споменатата статия е доказана автоматичната реализация $G_1 \implies G_2$, т.е. ако групата G_1 се реализира над произволно поле k, то G_2 също се реализира над това поле. Ще покажем, че е в сила автоматичната реализация $G_3 \implies G_4$. Обратната реализация $G_4 \implies G_3$ не е в сила, както ще видим в следващата точка.

Нека сега k е произволно поле с характеристика различна от p, и нека k не съдържа примитивен p-ти корен на единицата. Да изберем и фиксираме един примитивен p-ти корен на единицата ζ. Тогава разширението $k(\zeta)/k$ е циклично от

степен d, където d трябва да дели $p-1$. Нека κ е пораждащият елемент на групата $\mathrm{Gal}(k(\zeta)/k)$, която е изоморфна на цикличната група C_d. Тогава съществува $e \in \mathbb{Z} \setminus p\mathbb{Z}$, така че $\kappa(\zeta) = \zeta^e$. Нека K/k е p-разширение с група на Галоа $H = \mathrm{Gal}(K/k)$. Тогава $K(\zeta)/k(\zeta)$ също е H-разширение и можем да отъждествим групите $\mathrm{Gal}(K/k)$ и $\mathrm{Gal}(K(\zeta)/k(\zeta))$. Можем също така да отъждествим групите $\mathrm{Gal}(K(\zeta)/K)$ и $\mathrm{Gal}(k(\zeta)/k)$. Доказателството на следващата теорема може да се разглежда като компилация на конструкциите, използвани в [Gi, Théorème 5], [Br, Theorem 4] и [JLY, Theorem 6.6.4].

Теорема 4.2.5. ([Mi3, Theorem 5.1]) *Нека*

$$1 \longrightarrow C_p \longrightarrow G \underset{\pi}{\longrightarrow} H \longrightarrow 1 \tag{4.5}$$

е неразцепимо групово разширение. Тогава задачата за вложимсост, зададена чрез (4.5) *и* K/k *е разрешима тогава и само тогава, когато задачата за вложимост зададена чрез* (4.5) *и* $K(\zeta)/k(\zeta)$ *е разрешима.*

Доказателство: Ако задачата $(K/k, G, C_p)$ е разрешима и L е едно нейно решение, то очевидно $L(\zeta)$ е решение на задачата $(K(\zeta)/k(\zeta), G, C_p)$.

Обратно, нека задачата $(K(\zeta)/k(\zeta), G, C_p)$ е разрешима и нека $K(\zeta, \sqrt[p]{\beta})/k(\zeta)$ е едно решение на тази задача за някое $\beta \in K(\zeta)^*$. Тогава за всяко $\sigma \in H$ съществува $x_\sigma \in K(\zeta)^*$ такова, че $\sigma(\beta)/\beta = x_\sigma^p$. Можем да продължим σ върху $K(\zeta, \sqrt[p]{\beta})$: $\overline{\sigma}(\sqrt[p]{\beta}) = x_\sigma \sqrt[p]{\beta}$. Тогава за всяко σ и τ в H ще имаме $\overline{\sigma\tau\sigma\tau}^{-1}(\sqrt[p]{\beta})/\sqrt[p]{\beta} = x_\sigma \sigma(x_\tau) x_{\sigma\tau}^{-1} = \zeta^{X(\sigma,\tau)}$, където $X(\sigma,\tau)$ е 2-коцикъл от H в $\mathbb{F}_p$. (Да отбележим, че можем да отъждествим групите $C_p = \mathrm{Gal}(K(\zeta, \sqrt[p]{\beta})/K(\zeta))$ и $\mathbb{F}_p$, според теоремата на Кумер.) По този начин, на епиморфизма π (т.е. на груповото разширение (4.5)) съответства 2-кокласът $[X] \in H^2(H, \mathbb{F}_p)$. Нека естественото число m е такова, че $mde^{d-1} \equiv 1 \pmod{p}$. Дефинираме изображение $\Phi : K(\zeta) \to K(\zeta)$ чрез

$$\Phi(x) = (x^{e^{d-1}} \kappa(x^{e^{d-2}}) \cdots \kappa^{d-1}(x))^m,$$

за $x \in K(\zeta)$. Да отбележим, че $\Phi(\zeta) = (\zeta^{de^{d-1}})^m = \zeta$. Ако положим $\omega = \Phi(\beta)$ и $y_\sigma = \Phi(x_\sigma)$, то $\sigma(\omega)/\omega = y_\sigma^p$. Нататък, $\kappa(\omega)/\omega^e = (\beta^{-m(e^d-1)/p})^p$, значи $K(\zeta, \sqrt[p]{\omega})/k$ е разширение на Галоа. Тогава

$$y_\sigma \sigma(y_\tau) y_{\sigma\tau}^{-1} = \Phi(x_\sigma \sigma(x_\tau) x_{\sigma\tau}^{-1}) = \Phi(\zeta^{X(\sigma,\tau)}) = \zeta^{X(\sigma,\tau)}.$$

Следователно, получаваме същият 2-коцикъл и в частност изоморфизмът

$$\mathrm{Gal}(K(\zeta, \sqrt[p]{\omega})/k(\zeta)) \cong \mathrm{Gal}(K(\zeta, \sqrt[p]{\beta})/k(\zeta)).$$

Нека да продължим σ и κ върху $K(\zeta, \sqrt[p]{\omega})$ като положим $\widehat{\sigma}(\sqrt[p]{\omega}) = y_\sigma \sqrt[p]{\omega}$ и $\overline{\kappa}(\sqrt[p]{\omega}) = \beta^{-m(e^d-1)/p} \sqrt[p]{\omega}^e$, където $\overline{\kappa}$ е единственият про-образ от ред d. Тогава

$$\overline{\kappa}\widehat{\sigma}(\sqrt[p]{\omega}) = \kappa(y_\sigma)\beta^{-m(e^d-1)/p} \sqrt[p]{\omega}^e$$

и

$$\widehat{\sigma}\overline{\kappa}(\sqrt[p]{\omega}) = \beta^{-m(e^d-1)/p} x_\sigma^{-m(e^d-1)} y_\sigma^e \sqrt[p]{\omega}^e,$$

но $\kappa(y_\sigma) = x_\sigma^{-m(e^d-1)} y_\sigma^e$, значи $\overline{\kappa}\widehat{\sigma} = \widehat{\sigma}\overline{\kappa}$. По този начин получаваме изоморфизмът $\mathrm{Gal}(K(\zeta, \sqrt[p]{\omega})/k) \cong G \times C_d$, където $G \cong \mathrm{Gal}(K(\zeta, \sqrt[p]{\omega})/k(\zeta))$, и C_d се поражда от $\overline{\kappa}$. Неподвижното подполе $L = K(\zeta, \sqrt[p]{\omega})^{C_d}$ на C_d тогава ни дава решение на задачата за вложимост $(K/k, G, C_p)$. □

Сега ще докажем автоматичната реализация $G_3 \implies G_4$.

Теорема 4.2.6. ([Mi3, Theorem 5.2]) *Нека k е произволно поле. Ако G_3 се реализира над k, то G_4 също се реализира. Ако k има характеристика p или ако $x^{p^2} - 1$ се разлага в $k(\zeta)$, то обратната реализация също е в сила.*

Доказателство: Ако k има характеристика p, реализирането на произволна p-група над k зависи само от нейния ранг (виж [Wi, Satz p. 237]), и понеже G_3 и G_4 имат ранг две, теоремата е в сила.

Ще предполагаме от сега нататък, че k има характеристика различна от p. Ако $x^{p^2} - 1$ се разлага в k, то препятствията, които са пресметнати в теореми 4.2.1 и 4.2.2 са еквивалентни, така че реализирането на едната група влече реализирането на другата група. Да отбележим, че междинното поле L, описано в споменатите теореми е еднакво и за двете групи.

Да предположим сега, че $x^p - 1$ се разлага на линейни множители в k, но $x^{p^2} - 1$ не се разлага. Нека M е разширение на Галоа на k с $\mathrm{Gal}(M/k)$ изоморфна на G_3, и нека L е междинното (p^2, p) разширение, както е описано преди теорема 4.2.1. Образите на a_1 и a_2 в k^*/k^{*p} са линейно независими и затова не могат едновременно да се съдържат в редицата, породена от образа на ζ. Ако ζ и a_2 са линейно независими, можем да положим $a_1 = \zeta^{-1}$, откъдето $(a_1, \zeta; \zeta) = (a_2, \zeta a_1; \zeta) = 1$. В другия случай, когато a_1 и ζ са линейно независими, можем да положим $a_2 = \zeta$, така че отново

$(a_1, \zeta; \zeta) = (a_2, \zeta a_1; \zeta) = 1$. По този начин се убеждаваме, че групата G_4 се реализира над k.

Нататък, ще се освободим от предположението, че $x^p - 1$ се разлага в k. Нека N/k е разширение на Галоа такова, че $\mathrm{Gal}(N/k)$ е изоморфна на G_3. Тогава групата $\mathrm{Gal}(N(\zeta)/k(\zeta))$ също е изоморфна на G_3. От доказаното по-горе следва, че съществува G_4 разширение $M/k(\zeta)$. Нещо повече, ако $x^{p^2} - 1$ се разлага на линейни множители в $k(\zeta)$, то можем да изберем M такова, че неговото междинно (p^2, p) разширение е същото като това на $N(\zeta)$; както преди, означаваме това поле с L. Знаем, че $L = L'(\zeta)$, където L' е междинното (p^2, p) разширение на N/k. От теорема 4.2.5 следва, че L' се съдържа в G_4 разширение на k. Обратното следва аналогично. Ако $x^{p^2} - 1$ не се разлага в $k(\zeta)$, нека L_1 и L_2 са междинните (p^2, p) разширения на $N(\zeta)/k(\zeta)$ и $M/k(\zeta)$, съответно. Нека $K = k(\zeta)(\sqrt[p]{a_1}, \sqrt[p]{a_2})$ е междинното (p, p) разширение на $L_1/k(\zeta)$ за някои a_1 и a_2 в $k(\zeta)$. Имаме два случая.

Първо, ако a_2 и ζ са линейно независими, можем да вземем $k(\zeta)(\sqrt[p]{\zeta^{-1}}, \sqrt[p]{a_2})$ в ролята на междинно (p, p) разширение; полагаме $L_2 = k(\zeta)(\sqrt[p^2]{\zeta^{-1}}, \sqrt[p]{a_2})$ в ролята на междинно (p^2, p) разширение. Да отбележим, че L_1 (което е композитът на $k(\zeta)$ и на (p^2, p) разширение на k) е абелово над k. В частност, $k(\zeta)(\sqrt[p]{a_2})$ е абелово над k. Такова е и $k(\zeta)(\sqrt[p^2]{\zeta^{-1}}) = k(\zeta_{p^3})$. Следователно L_2 също е абелово разширение на k, и понеже p не дели $[k(\zeta) : k]$, трябва да съществува (p^2, p) разширение L_2' на k такова, че $L_2 = L_2'(\zeta)$. Тук отново можем да използваме теорема 4.2.5.

Второ, ако a_1 и ζ са линейно независими, можем да вземем $k(\zeta)(\sqrt[p]{a_1}, \sqrt[p]{\zeta})$ в ролята на междинно (p, p) разширение на $L_2/k(\zeta)$. Имаме (p^2, p) разширението $L_1 = k(\zeta)(\sqrt[p]{f_1\beta}, \sqrt[p]{a_2})$ дадено над теорема 4.2.1. (Можем да забележим, че има леко несъответствие между описанието на L и L_1, дадено преди теорема 4.2.1 и това дадено тук, което е трудно да се избегне.) Тогава L_1, бивайки композитът на $k(\zeta)$ и на (p^2, p) разширение на k, е абелово над k. В частност, $k(\zeta)(\sqrt[p]{f_1\beta})$ е абелово над k и същото важи за $k(\zeta)(\sqrt[p]{\zeta}) = k(\zeta_{p^2})$. Следователно, L_2 също е абелово разширение над k. Тъй като p не дели $[k(\zeta) : k]$, съществува (p^2, p) разширение L_2' на k такова, че $L_2 = L_2'(\zeta)$. Така отново можем да използваме теорема 4.2.5. $\square$

В следващата точка ще покажем, че обратната реализация не е в сила, когато $x^{p^2} - 1$ не се разлага в $k(\zeta)$.

4.2.3 Локални полета

Нека k е локално поле, т.е. локално компактно по отношение на някое нетривиално нормиране. Така то е едно от следните видове

(a) крайно разширение на $\mathbb{Q}_p$, за някое просто число p;

(b) крайно разширение на $\mathbb{F}_p((T))$, където $\mathbb{F}_p$ е поле с p елемента;

(c) $\mathbb{R}$ или $\mathbb{C}$.

Означаваме с v регулярното нормиране на k, с π конформният елемент на v (също наричан униформиращ или прост елемент на k), и с U групата на единиците на k. Тогава всеки елемент на k^* може да бъде еднозначно записан във вида $a = \pi^m u$ с $u \in U$ и $m = \mathrm{ord}_k(a)$. Полето от класове $\overline{k}$ на k има q елемента, и неговата характеристика е p. За всяко естествено число n съществува единствено неразклонено разширение k_n от степен n над k. Полето k_n е полето на разлагане на полинома $x^{q^n-1}-1$. Означаваме с H_n групата на Галоа на разширението k_n/k, която е циклична от ред n, породена от някакъв елемент φ_n. Тогава имаме изоморфизмът

$$\mathrm{INV} \ : \ H^2(H_n, k_n^*) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}. \tag{4.6}$$

Ако ни е дадено произволно $x \in k_n^*$, можем да дефинираме кръстосаният хоморфизъм $f \in Z^2(H_n, k_n)$ чрез

$$f(\varphi_n^i, \varphi_n^j) = \begin{cases} 1, & 0 \le i, j, i+j < n \\ x, & 0 \le i, j < n \le i+j \end{cases} \tag{4.7}$$

Означаваме с $[f]$ 2-кокласът породен от f в $H^2(H_n, k_n^*)$. Тогава изоморфизмът (4.6) се задава чрез

$$\mathrm{INV} \ : \ [f] \mapsto \frac{v(x)}{n} + \mathbb{Z}.$$

Означаваме с $\mathcal{G}(k)$ множеството на всички крайно мерни централни прости алгебри над k. Нека алгебрата $A \in \mathcal{G}(k)$ има степен n над k. Тогава $[A] = [(k_n, H_n, f)]$, където k_n, H_n и f са както преди. Следователно, $\mathrm{INV}([A]) = \frac{v(x)}{n} + \mathbb{Z} \in \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Нека $A, B \in \mathcal{G}(k)$. Ще запишем някои известни свойства на изоморфизма INV:

- $A \sim B$ (т.е. $[A] = [B]$) $\iff$ $\mathrm{INV}(A) = \mathrm{INV}(B)$;

- $A \sim k$ (т.е. $[A] = 1$) $\iff$ $\mathrm{INV}(A) = 0$;

- $\mathrm{INV}(A \otimes B) = \mathrm{INV}(A) + \mathrm{INV}(B)$.

Нататък, да разгледаме цикличната алгебра $B = (k_n, H_n, f)$. Тя се описва напълно чрез следните свойства:

- $B = \bigoplus_{0 \leq j < n} u^j k_n$;

- $u^{-1} du = \varphi_n(d), \forall d \in k_n$, където φ_n а автоморфизмът на Фробениус на разширението k_n/k;

- $u^n = x \in k^*$.

Системата фактори f се дефинира чрез

$$u_{\varphi_n^i} u_{\varphi_n^j} = f(\varphi_n^i, \varphi_n^j) u_{\varphi_n^{i+j}}.$$

Може да се покаже, че f удовлетворява формулата (4.6). Полагаме $u_{\varphi_n} = u, u_{\varphi_n^i} = u^i, u_1 = u^n = x$.

Отсега нататък ще считаме, че k съдържа примитивен n-ти корен на единицата ζ. Означаваме с $\mathfrak{p}$ простият идеал породен от конформния елемент $\pi \in k$. Нека $q = \mathbb{N}\mathfrak{p}$ е броят на елементите в полето от класове $\overline{k}$. Тогава $\mathbb{F}_q^*$ е циклична група от ред $q-1$, значи $n | q-1$ и $u^{\frac{q-1}{n}} \in \langle \zeta \rangle = \mu_n \in \mathbb{F}_q^*$. За $a \in k^*$ означаваме с $(a|\mathfrak{p})$ единственият n-ти корен на единицата такъв, че $(a|\mathfrak{p}) \equiv a^{\frac{q-1}{n}} \pmod{\mathfrak{p}}$.

Теорема 4.2.7. *За $a \in k^*$ такова, че $\mathrm{ord}_k a = 0$, следните условия са еквивалентни:*

(a) $(a|\mathfrak{p}) = 1$*;*

(b) *a е n-та степен в $\overline{k}$;*

(c) *a е n-та степен в k.*

Да дефинираме сега символът на Хилберт $(a, b)_v$ за локалното поле k:

$$(a, b)_v = \zeta^{n \mathrm{INV}_v(a, b; \zeta)}.$$

Инвариантата на обобщената кватернионна алгебра $(a, b; \zeta)$ е елемент на $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$, и оттук $n\mathrm{INV}_v(a, b; \zeta)$ е елемент на $\mathbb{Z}/n\mathbb{Z}$. Така ние получаваме билинейно изображение $k^*/k^{*n} \times k^*/k^{*n} \longrightarrow \mu_n = \langle\zeta\rangle$. Може лесно да се покаже, че произведението на кватернионни класове в групата на Брауер се разпада тогава и само тогава, когато произведението на символите на Хилберт е 1.

Да предположим сега, че $(a, b; \zeta)$ е алгебра с деление, породена от елементи α и β такива, че $\alpha^n = a, \beta^n = b$ и $\beta\alpha = \zeta\alpha\beta$. Да припомним, че за да пресметнем инвариантата на централна алгебра с деление D над локално поле k, ние трябва да извършим следното:

(a) избираме максимално неразклонено поле $L = k(i)$ в D, където $i^n = c \in k$;

(b) намираме елемент $j \in D$, за който $x \mapsto jxj^{-1}$ е автоморфизмът на Фробениус на L чрез теоремата на Ньотер-Сколем;

(c) прилагаме формулата $\mathrm{INV}_v([D]) = v(j) + \mathbb{Z}$.

Да изберем неразклоненото разширение $L = k(\alpha) = k(\sqrt[n]{a})$. Нека $(a|\mathfrak{p}) = \zeta^r$, така че $(\mathfrak{p}, L/k)(\alpha) = \zeta^r\alpha$, където $(\mathfrak{p}, L/k)$ е елементът на Фробениус за $\mathfrak{p}$, съответстващ на автоморфизма на Фробениус в $\mathrm{Gal}(\overline{k(\alpha)}/\overline{k})$. Тъй като $\beta\alpha\beta^{-1} = \zeta\alpha$, виждаме, че можем да вземем $j = \beta^r$. Тогава $j^n = b^r$, значи $v(j) = \frac{r}{n}v(b)$. Следователно,

$$(a, b)_v = \zeta^{n\mathrm{INV}_v(a,b;\zeta)} = \zeta^{rv(b)} = (a|\mathfrak{p})^{v(b)}.$$

Нека сега $k = \mathbb{Q}_l$, където l е нечетно просто число такова, че $l \equiv 1 \pmod p$, но $l \not\equiv 1 \pmod{p^2}$. Тогава $\zeta \in k$, но $\sqrt[p]{\zeta} = \zeta_{p^2} \notin k$. Неразклоненото разширение на k е полето на разлагане на полинома $g(x) = x^{l^p-1} - 1$ над k. Тъй като p^2 дели $l^p - 1 = (l-1)(l^{p-1} + l^{p-2} + \cdots + l + 1)$, ζ_{p^2} е корен на $g(x)$, следователно $k(\zeta_{p^2})$ е неразклонено разширение. Получаваме, че $\dim_{\mathbb{F}_p} \mathbb{Q}_l^*/\mathbb{Q}_l^{*p} = 2$, т.е. $\mathbb{Q}_l^*/\mathbb{Q}_l^{*p}$ има p^2 елемента. Следователно l и ζ пораждат $\mathbb{Q}_l^*/\mathbb{Q}_l^{*p}$ над $\mathbb{F}_p$. Сега можем да опишем напълно символът на Хилберт: $(\zeta, b)_l = (\zeta|l)^{v(b)} = \zeta^{\frac{l-1}{p}v(b)}$. В частност, $(\zeta, b)_l = 1 \iff v(b) = 0$, т.е. $b \in U$. Оттук получаваме, че има само две задачи за вложимост зададени с груповото разширение $1 \longrightarrow \langle\varepsilon\rangle \cong \mu_p \longrightarrow C_{p^2} \longrightarrow C_p \longrightarrow 1$. Едната от тези задачи е разрешима, именно, когато a се съдържа в редицата, породена от ζ.

Нека сега да разгледаме групите G_1 и G_2. За да имаме $(a_1, a_2)_l = 1$, елементите a_1 и a_2 трябва да се съдържат в редицата, породена от ζ, което е противоречие с

предположението, че те са линейно независими по модул $(\mathbb{Q}_l)^p$. Следователно, G_1 не се реализира над $\mathbb{Q}_l$. За $a_2 = \zeta^{-1}$, получаваме $(a_1, a_2\zeta)_l = 1$, значи G_2 се реализира над $\mathbb{Q}_l$.

За да можем да конструираме задачи за вложимост зададени чрез груповите разширения (4.1) и (4.2), трябва да имаме $(a_1, \zeta)_l = 1$, т.е. a_1 и ζ трябва да се съдържат в една и съща редица. Тогава $(a_2, a_1) \neq 1$, понеже a_1 и a_2 не могат едновременно да се съдържат в редицата, породена от ζ. Следователно, G_3 не се реализира над $\mathbb{Q}_l$. За $a_1 = \zeta^{-1}$, получаваме $(a_2, a_1\zeta)_l = 1$, значи задачата за вложимост, зададена чрез (4.2) е разрешима, и групата G_4 се реализира над $\mathbb{Q}_l$. Това показва, че автоматичната реализация $G_4 \implies G_3$ не е в сила.

За да построим задача за вложимост, зададена чрез груповото разширение (4.4), трябва да имаме $\dim_{\mathbb{F}_p} \mathbb{Q}_l^*/\mathbb{Q}_l^{*p} \geq 3$, което е невъзможно, значи групата G_6 не се реализира над $\mathbb{Q}_l$.

Накрая, нека да разгледаме p-адичното циклотомно поле $k = \mathbb{Q}_p(\zeta)$ за примитивен p-ти корен на единицата ζ. Символът на Хилберт може да бъде напълно описан, както е направено например в [Ив] и [CF]. Ние ще дадем някои от свойствата му. Елементът $\pi = 1 - \zeta$ е конформен за полето k, което е напълно разклонено разширение над $\mathbb{Q}_p$ от степен $p - 1$. Означаваме с U_i подгрупата на единиците $\equiv 1 \pmod{\pi^i}$ в k^* за $i = 1, 2, \ldots$. Тогава образът на елемента $\eta_i = 1 - \pi^i$ поражда групата U_i/U_{i+1}, която е циклична от ред p. Елементите $\pi, \eta_1 = \zeta, \eta_2 = 1 - \pi^2, \ldots, \eta_p = 1 - \pi^p$ пораждат групата k^*/k^{*p}, която има ред p^{p+1} и има размерност $p + 1$ над $\mathbb{F}_p$, така че тези пораждащи елементи могат да бъдат избрани за базис. Тогава са в сила следните леми.

Лема 4.2.8. *За всеки i, j такива, че $1 \leq i, j \leq p - 1$ имаме $(\eta_j, \eta_i)_\pi = \prod_{r,s} \zeta^{i/s}$, където произведението е по всички $r, s \in \mathbb{N}$ такива, че $ri + sj = p$.*

Лема 4.2.9. *Изображението на Хилберт*

$$a, b \mapsto (a, b)_\pi \ : \ k^* \times k^* \longrightarrow \mu_p$$

е единственото анти-симетрично изображение, удовлетворяващо

(a) $(\eta_i, \eta_j)_\pi = (\eta_i, \eta_{i+j})_\pi (\eta_{i+j}, \eta_j)_\pi (\pi, \eta_{i+j})_\pi^j$, *за всички $i, j \geq 1$;*

(b)

$$(\pi, \eta_i)_\pi = \begin{cases} 1, & 1 \leq i \leq p-1 \\ \zeta, & i = p \end{cases}$$

(c) $(*,*)_\pi = 1$ *върху* $U_i \times U_j$, *ако* $i + j \geq p + 1$.

Да разгледаме отново задачата за вложимост зададена чрез груповото разширение $1 \longrightarrow \langle\varepsilon\rangle \cong \mu_p \longrightarrow C_{p^2} \longrightarrow C_p \longrightarrow 1$. От лема 4.2.9 следва, че $(a, \zeta)_\pi = 1$ за $a = \pi, \zeta$ и η_p, значи задачата е разрешима в тези случаи. Тъй като $\dim_{\mathbb{F}_p} k^*/k^{*p} = p+1$, имаме $p + 1$ съществено различни задачи за вложимост, зададени чрез груповото разширение $1 \longrightarrow \langle\varepsilon\rangle \cong \mu_p \longrightarrow C_{p^2} \longrightarrow C_p \longrightarrow 1$. Тук възниква въпросът – кои са стойностите на a такива, че задачата за вложимост е разрешима? С помощта на лема 4.2.9 може да се покаже, че ако $\frac{p-1}{2} \leq j \leq p-1$, то задачата за вложимост за $a = \eta_j$ не е разрешима. Прилагайки лема 4.2.8 получаваме, че ако $p = 11$ задачата за вложимост е разрешима за $a = \eta_3$. Не е трудно да се покаже, че за всяко a_1 такова, че можем да построим задачи за вложимост зададени чрез (4.1) и (4.2), съществува a_2 такова, че тези задачи са разрешими. Накрая за $a_1 = \zeta, a_2 = \pi$ и $a_3 = \eta_p$ имаме $(a_3, \zeta)_\pi = (a_2, a_1)_\pi = 1$, откъдето задачата за вложимост зададена чрез (4.4) е разрешима.

4.3 Модулярната p-група като група на Галоа

Означаваме модулярната p-група от ред p^n с $M(p^n)$, за $n \geq 3$. Тя се поражда от два елемента α и β със съотношения $\alpha^{p^{n-1}} = \beta^p = 1$ и $\beta\alpha = \alpha^{1+p^{n-2}}\beta$, виж например [Ha, Th. 12.5.1]. Поради честата употреба на простата степен p^{n-2} в този параграф, ще положим $q = p^{n-2}$. Модулярната група $M(2^n)$ е една от четирите неабелови групи от ред 2^n, които имат циклична подгрупа с индекс 2, за $n \geq 4$. За нечетно p, модулярната група $M(p^n)$ е единствената неабелова група от ред p^n, която има циклична подгрупа с индекс p, за $n \geq 3$. Да забележим, че подгрупата $C_q \times C_p = \langle \alpha^p, \beta \rangle$ има индекс p в модулярната група $M(p^n)$.

4.3.1 $M(p^n)$-разширения на Галоа

Описанието на разширенията на Галоа е съществена част от теорията на препятствията. От една страна, прецизното пресмятане на едно препятствие често води до описание на решенията на съответната задача за вложимост. От друга страна, познаването на всички разширения на Галоа, които реализират дадена група може да ни позволи да навлезем по-надълбоко в кохомологични разсъждения, които да доведат до получаването на нови препятствия.

В тази точка ще опишем в явен вид модулярните p-разширения. Резултатите, които ще получим могат да бъдат получени по два начина: чрез 'елементарна' Кумеровата теория, следвайки [Wa], или чрез 'висша' Кумерова теория, развита в работите [MS1, MS2, MSS1, MSS2].

Нека първо да въведем някои означения. Нека $K_1 = k(\sqrt[p]{a_1})$ за $a_1 \in k^* \setminus k^{*p}$, и нека K/k е циклично $C_q = \langle \sigma \rangle$ разширение такова, че $K_1 \subset K$.

За груповия пръстен $\mathbb{F}_p[C_q]$ съществуват точно q ненулеви фактор-пръстени, именно $M_j = \mathbb{F}_p[C_q]/\langle (\sigma - 1)^j \rangle$ за $j = 1, 2, \ldots, q$. Всеки пръстен M_j е C_q модул, понеже произведението в $\mathbb{F}_p[C_q]$ индуцира $\mathbb{F}_p[C_q]$-действие върху M_j. Нататък, нека $J = K^*/K^{*p}$ е $\mathbb{F}_p[C_q]$ модул на p-ти степенни класове. Ще записваме елементите на J като $[\gamma], \gamma \in K^*$. Цокъл сериите на J се задават чрез $J_1 = J^{C_q}$ - неподвижния подмодул на J и $J_i/J_{i-1} = (J/J_{i-1})^{C_q}$ за $i > 1$. Имаме, че $J_i = \ker(\sigma - 1)^i$, където $(\sigma - 1)^i$ го разглеждаме като ендоморфизъм на J. От [Wa] имаме съответствието на Кумер над K на крайните подпространства на J и крайните абелови разширения на K с експонента p.

Тъй като α^q е централен и $\alpha^{-1}\beta\alpha = \alpha^q\beta$, подгрупата породена от α^q и β е нормална в $M(p^n)$. Така получаваме груповото разширение:

$$1 \longrightarrow C_p \times C_p \cong \langle \alpha^q, \beta \rangle \longrightarrow M(p^n) \underset{\alpha \mapsto \sigma}{\longrightarrow} C_q \longrightarrow 1. \tag{4.8}$$

Нашата първа цел е да опишем решенията на задачата за вложимост зададена чрез by K/k и (4.8).

Теорема 4.3.1. ([Mi4, Proposition 3.1]) *Нека L/K е разширение на Галоа с група на Галоа изоморфна на $C_p \times C_p$. Тогава L/k е неабелово разширение на Галоа тогава и само тогава, когато $L = K(b_0^{1/p}, b_1^{1/p})$, където $b_0 \in K^* \setminus K^{*p}, b_1 = \sigma(b_0)/b_0 \in K^* \setminus K^{*p}$ и $b_2 = \sigma(b_1)/b_1 \in K^{*p}$. В този случай, $G = \mathrm{Gal}(L/k)$ е изоморфна или на $M(p^n)$, или на полудиректното произведение $C_q \rtimes (C_p)^2$.*

Доказателство: Според [MSS2], неабеловите разширения L/k са във взаимно еднозначно съответствие с неразложимите подмодули на J имащи размерност 2. Освен това, групата на Галоа $G = \mathrm{Gal}(L/k)$ е изоморфна или на модулярната група, или на полудиректното произведение $C_q \rtimes (C_p)^2$. □

Сега вече можем да направим описание на всички $M(p^n)$ разширения, което е целта на следната

Теорема 4.3.2. ([Mi4, Theorem 3.2]) *L/k е $M(p^n)$ разширение, което е решение на задачата за вложимост зададена чрез* (4.8)*, тогава и само тогава, когато съществуват $b_0 \in K^* \setminus K^{*p}, f \in k^* \setminus k^* \cap K^{*p}$ и $x \in K^*$ такива, че $\sigma(b_0)/b_0 = fx^p, L/k = K(\sqrt[p]{b_0}, \sqrt[p]{f})/k$ и $c = f^{q/p}N_{K/k}(x)$ е p-ти корен на единицата, но $c \neq 1$.*

Доказателство: '$\Rightarrow$': Нека $L/k = K(b_0^{1/p}, b_1^{1/p})/k$ е $M(p^n)$ разширение, за което $b_0 \in K^* \setminus K^{*p}, b_1 = \sigma(b_0)/b_0 \in K^* \setminus K^{*p}$ и $\sigma(b_1)/b_1 = d^p$, където $d \in K^*$. Нека $\alpha \in \mathrm{Gal}(L/k)$ е про-образ на σ. Да положим $\omega_0 = b_0^{1/p}, \omega_1 = \alpha(\omega_0)/\omega_0 = b_1^{1/p}, \omega_2 = \alpha(\omega_1)/\omega_1 = d, \ldots, \omega_q = \alpha(\omega_{q-1})/\omega_{q-1}$. Имаме следното (в експоненциални означения): $\omega_1 = \omega_0^{\alpha-1}, \omega_2 = \omega_0^{(\alpha-1)^2}, \ldots, \omega_q = \omega_0^{(\alpha-1)^q}$. Биномното развитие на $X^q = [(X-1)+1]^q$ ни показва, че

$$\omega_0^{\alpha^q} = \omega_0^{\sum_{k=0}^{q}(\alpha-1)^k\binom{q}{k}} = \prod_{k=0}^{q}\omega_0^{(\alpha-1)^k\binom{q}{k}} = \prod_{k=0}^{q}\omega_k^{\binom{q}{k}}.$$

Полагаме $c = \omega_0^{\alpha^q-1} = \prod_{k=1}^{q}\omega_k^{\binom{q}{k}}$. От $\omega_0^p = b_0$ и $\alpha^q(b_0) = \sigma^q(b_0) = b_0$ следва, че $c^p = 1$. Тогава имаме $c = b_1^{q/p}d^\gamma$, където $\gamma = \binom{q}{2} + \binom{q}{3}(\sigma-1) + \cdots + \binom{q}{q}(\sigma-1)^{q-2}$. Нека $\tau_0, \tau_1 \in$

$\mathrm{Gal}(L/K)$ са такива, че $\tau_0(\omega_0) = \omega_0\zeta, \tau_0(\omega_1) = \omega_1, \tau_1(\omega_0) = \omega_0$ и $\tau_1(\omega_1) = \omega_1\zeta$. Да отбележим, че $\alpha\tau_0\alpha^{-1} = \tau_0$ и $\alpha\tau_1\alpha^{-1} = \tau_1\tau_0^{-1}$, което се вижда като сравним действията върху ω_0 и ω_1. Елементът α^q лежи в $\mathrm{Gal}(L/K)$ и е неподвижен под действието на σ. Тогава α^q трябва да бъде някаква степен на τ_0, значи е тривиален само ако неговото действие върху ω_0 е тривиално.

Отчитайки, че L/k е модулярно разширение, получаваме, че α^q не е тривиален, откъдето $c \neq 1$. Да означим както е обичайно с $N_{K/k} : K \to k$ норменото изображение. От $b_1 = \sigma(b_0)/b_0$ следва, че $N_{K/k}(b_1) = 1$, значи

$$N_{K/k}(b_1) = b_1\sigma(b_1)\cdots\sigma^{q-1}(b_1) = b_1^q(d^p)^{q-1}\sigma(d^p)^{q-2}\cdots\sigma^{q-2}(d^p) = 1.$$

Оттук получаваме, че елементът $h = b_1^{q/p}d^{q-1}\sigma(d)^{q-2}\cdots\sigma^{q-2}(d)$ се намира в циклична група, породена от ζ. В частност, $\sigma(h)/h = N_{K/k}(d) = 1$. Сега от теорема 90 на Хилберт следва, че съществува $x \in K^*$ такова, че $d = \sigma(x)/x$. Следователно, $\sigma(b_1)/b_1 = \sigma(x^p)/x^p$ и за някое $f \in k^* \setminus k^* \cap K^{*p}$ получаваме $b_1 = fx^p$. Нататък, $c = (fx^p)^{q/p}(\sigma(x)/x)^\gamma = f^{q/p}x^\delta$, където $\delta = q + \binom{q}{2}(\sigma-1) + \cdots + \binom{q}{q}(\sigma-1)^{q-1} = \sum_{k=0}^{q-1}\sigma^k$, значи $c = f^{q/p}N_{K/k}(x)$.

'$\Leftarrow$': Нека b_0, f и c са както в условието. Полагаме $b_1 = fx^p$ и $d = \sigma(x)/x$. От теорема 4.3.1 следва, че $L/k = K(b_0^{1/p}, b_1^{1/p})/k$ е или полудиректно, или $M(p^n)$ разширение. С помощта на същите дефиниции на $\omega_0, \ldots, \omega_q$ както в доказателството на другата посока '$\Rightarrow$', получаваме, че $c = (fx^p)^{q/p}(\sigma(x)/x)^\gamma = \omega_0^{\alpha^q-1} \neq 1$, т.е. $\alpha^q \neq 1$, значи L/k е точно $M(p^n)$ разширение. □

Забележка 4.3.3. В теорема 4.3.2 получихме, че $b_1 = b_0^{\sigma-1} \notin K^{*p}$, значи $[b_0] \notin J_1$, и $b_2 = b_0^{(\sigma-1)^2} \in K^{*p}$, значи $[b_0] \in J_2$, т.е. $[b_0] \in J_2 \setminus J_1$. По този начин явният вид на елемента b_0 се определя от структурата на модула J_2, която не е съвсем ясна. Явният вид на елемента b_0, обаче няма особено значение за нашите цели.

Нататък, ще обобщим теорема 4.3.1 за неабелови разширения на C_q с ядро $(C_p)^3$.

Теорема 4.3.4. ([Mi4, Proposition 3.3]) *Нека L/k е неабелово разширение на Галоа, съдържащо K/k и нека $\mathrm{Gal}(L/K)$ е изоморфна на $(C_p)^3$. Тогава $L = K(b_0^{1/p}, b_1^{1/p}, b_2^{1/p})$, където $b_0 \in K^* \setminus K^{*p}, b_1 = \sigma(b_0)/b_0 \in K^* \setminus K^{*p}, b_2 = \sigma(b_1)/b_1$ и съществуват само две възможности:*

(i) *$b_2 \in K^* \setminus K^{*p}$ и $\sigma(b_2)/b_2 \in K^{*p}$;*

(ii) $b_2 \in K^{*p}$ *и* $\sigma(b_2)/b_2 \in K^{*p}$.

Доказателство: Неабеловите разширения на Галоа L/k такива, че $\mathrm{Gal}(L/K)$ е изоморфна на $(C_p)^3$ са в биективно съответствие с подмодулите на J с размерност 3, които не са изоморфни на $\mathbb{F}_p^3$. От теорията на модулите над области на цялост следва, че съществуват само два класа такива модули с точност до изоморфизъм: $\mathbb{F}_p[C_q]/\langle(\sigma-1)^3\rangle$ и $\mathbb{F}_p \oplus \mathbb{F}_p[C_q]/\langle(\sigma-1)^2\rangle$, даващи случаите **(i)** и **(ii)**, съответно. $\square$

Нека да разгледаме сега двата случая по отделно. Първият ни дава подмодул $W \cong \mathbb{F}_p[C_q]/\langle(\sigma-1)^3\rangle$, значи за $n>3$ има само два класа на изоморфност, които са възможни за $\mathrm{Gal}(L/K)$, в зависимост от това дали индексът на W е тривиален или не.

Теорема 4.3.5. ([Mi4, Proposition 3.4]) *Нека* $L = K(b_0^{1/p}, b_1^{1/p}, b_2^{1/p})$, *където* $b_0 \in K^* \setminus K^{*p}, b_1 = \sigma(b_0)/b_0 \in K^* \setminus K^{*p}, b_2 = \sigma(b_1)/b_1 \in K^* \setminus K^{*p}$ *и* $\sigma(b_2)/b_2 \in K^{*p}$. *Тогава* L/k *е разширение на Галоа и групата на Галоа на* L/k *е изоморфна или на полудиректното произведение* $C_q \rtimes (C_p)^3$, *или на група, породена от* σ_1, τ_0, τ_1 *и* τ_2 *такива, че* $\sigma_1^q = \tau_0, \sigma_1\tau_1\sigma_1^{-1} = \tau_1\tau_0^{-1}, \sigma_1\tau_2\sigma_1^{-1} = \tau_2\tau_0\tau_1^{-1}$, *където* τ_0, τ_1 *и* τ_2 *са пораждащи на* $\mathrm{Gal}(L/K)$, *зададени чрез* $\tau_i(\sqrt[p]{b_j}) = \sqrt[p]{b_j}\zeta^{\delta_{ij}}$.

Вторият случай ни дава подмодул $W \cong \mathbb{F}_p \oplus \mathbb{F}_p[C_q]/\langle(\sigma-1)^2\rangle$, значи имаме три класа на изоморфност, които са възможни за $\mathrm{Gal}(L/K)$, в зависимост от индексите на двете директни събираеми.

Да означим с $\widetilde{M}(p^{n+1})$ групата породена от елементите σ_1, τ_1 и ρ_1 такива, че $|\sigma_1| = pq, \tau_1^p = \rho_1^p = 1, \tau_1\sigma_1 = \sigma_1^{q+1}\tau_1\rho_1$ и ρ_1 е централен. Полагаме $N_1 = \langle\sigma_1^p\rangle, N_2 = \langle\rho_1\rangle$. Тогава N_1 и N_2 са нормални в $\widetilde{M}(p^{n+1})$ и $N_1 \cap N_2 = \{1\}$. Фактор-групата $\widetilde{M}(p^{n+1})/N_1$ е изоморфна на групата на Хайзенберг H_{p^3}, за $p \neq 2$, и на диедралната група D_8 от ред 8, за $p=2$. Фактор-групата $\widetilde{M}(p^{n+1})/N_2$ е изоморфна на модулярната група $M(p^n)$. Групата $\widetilde{M}(p^{n+1})$ тогава е изоморфна на директното произведение на групите $\widetilde{M}(p^{n+1})/N_1$ и $\widetilde{M}(p^{n+1})/N_2$ с обединена фактор-група $\widetilde{M}(p^{n+1})/N_1N_2 \cong (C_p)^2$.

Теорема 4.3.6. ([Mi4, Proposition 3.5]) *Нека* $L = K(b_0^{1/p}, b_1^{1/p}, b_2^{1/p})$, *където* $b_0 \in K^* \setminus K^{*p}, b_1 = \sigma(b_0)/b_0 \in K^* \setminus K^{*p}, \sigma(b_1)/b_1 \in K^{*p}, b_2 \in K^* \setminus K^{*p}$ *и* $\sigma(b_2)/b_2 \in K^{*p}$. *Тогава* L/k *е неабелово разширение на Галоа и групата на Галоа на* L/k *е изоморфна или на* $(C_q \rtimes (C_p)^2) \times C_p$, *или на* $M(p^n) \times C_p$, *или на* $\widetilde{M}(p^{n+1})$.

Като илюстрация на теореми 4.3.2 и 4.3.6, ще конструираме $\widetilde{M}(2^{n+1})$ разширение над полето на рационалните числа в следния

Пример 4.3.7. Нека $p = 2, k = \mathbb{Q}$ и нека ξ е примитивен корен на единицата от степен 2^{n+1} за $n \geq 4$. Добре известно е, че групата на Галоа на $\mathbb{Q}(\xi)/\mathbb{Q}$ е изоморфна на мултипликативната група $\mathbb{Z}^*_{2^{n+1}}$, която на свой ред е изоморфна на $C_{2^{n-1}} \times C_2 = \langle\overline{5}\rangle \times \langle -\overline{1}\rangle$ (виж [ПСЧ]). Полагаме $\theta_k = \xi^k + \xi^{-k}$ за $k \geq 1$ и $\theta = \theta_1$. Тогава за нечетно k ще имаме, че θ_k са спрегнатите на θ, и $\mathbb{Q}(\xi) = \mathbb{Q}(\theta, i)$, където $i = \sqrt{-1} = \xi^{2^{n-1}}$. Действията на $\overline{5}$ и $-\overline{1}$ са:

$$\overline{5} : \theta \mapsto \theta_5, i \mapsto i; \ -\overline{1} : \theta \mapsto \theta, i \mapsto -i.$$

Следователно, групата на Галоа на $K/k = \mathbb{Q}(\theta_2)/\mathbb{Q}$ е $\langle\overline{5}\rangle/\langle\overline{5}^{2^{n-2}}\rangle$, която е изоморфна на цикличната група $C_{2^{n-2}}$.

Сега можем да конструираме $M(2^n)$ разширение, прилагайки теорема 4.3.2. Имаме, че $\theta^2 = \theta_2 + 2$ и $\sqrt{2}$ са в K, значи можем да положим $b_0 = \sqrt{2}\theta^2$. Означаваме с σ пораждащият на $C_{2^{n-2}}$. Тогава $\sigma(b_0)/b_0 = -x^2$, където $x = \overline{5}(\theta)/\theta = \theta_5/\theta = \theta_2^2 - \theta_2 - 1 \in K^*$. Нататък, трябва да пресметнем нормата на x:

$$N_{K/k}(x) = \overline{5}^{2^{n-2}}(\theta)/\theta = (\xi^{1+2^n} + \xi^{-1-2^n})/\theta = -1,$$

понеже $5^{2^{n-2}} \equiv 1+2^n \pmod{2^{n+1}}$. По този начин, за $f = -1$ получаваме $\sigma(b_0)/b_0 = fx^2$ и $c = f^{q/2}N_{K/k}(x) = -1$, откъдето $K(\sqrt[4]{2}\theta, i)/k = \mathbb{Q}(\theta_2, \sqrt[4]{2}\theta, i)/\mathbb{Q}$ е $M(2^n)$ разширение.

Да положим $b_1 = -x^2$ и $b_2 = \theta^2$ (тук очевидно b_1 и b_2 са в $K^* \setminus K^{*2}$). Тъй като $\sigma(\sqrt{2})/\sqrt{2} = -1$, получаваме $\sigma(b_2)/b_2 = x^2$, значи $K(\sqrt[4]{2}\theta, i, \theta)/k = \mathbb{Q}(\sqrt[4]{2}, \xi)/\mathbb{Q}$ е $\widetilde{M}(2^{n+1})$ разширение. □

Описанието на модулярните p-разширения може да бъде направено в още по-явен вид в някои частни случаи, които сега ще разгледаме.

Нека $a_1, a_2 \in k^*$ са независими $\bmod k^{*p}$ и да означим $K_i = k(\sqrt[p]{a_i}), i = 1, 2$. Както преди, нека K/k е $C_q = \langle\sigma\rangle$ разширение такова, че $K_1 \subset K$. Тогава $L/k = K(\sqrt[p]{a_2})/k$ е $C_q \times C_p$ разширение, с пораждащи елементи σ и τ такива, че $\sigma^q = \tau^p = 1$. Имаме груповото разширение:

$$1 \longrightarrow \mu_p \cong \langle\alpha^q\rangle \longrightarrow M(p^n) \underset{\substack{\alpha\mapsto\sigma \\ \beta\mapsto\tau}}{\longrightarrow} C_q \times C_p \longrightarrow 1. \tag{4.9}$$

Според теорема 2.2.1 препятствието на задачата за вложимост зададена чрез L/k и (4.9) е

$$[K, C_q, \zeta](a_2, a_1; \zeta) \in \mathrm{Br}(k), \tag{4.10}$$

където $[K, C_q, \zeta]$ е класът на еквивалентност на цикличната алгебра на кръстосаното произведение (K, σ, ζ), зададено чрез ограниченото групово разширение

$$1 \longrightarrow \mu_p \cong \langle \alpha^q \rangle \longrightarrow C_{pq} \underset{\alpha \mapsto \sigma}{\longrightarrow} C_q \longrightarrow 1.$$

Сега ще дадем няколко примера на модулярни разширения, получени чрез анализ на препятствието (4.10).

Пример 4.3.8. Да предположим, че примитивен q-ти корен на единицата ζ_q се съдържа в k. Според [Pi, Corollary 15.1b], имаме

$$(K, \sigma, \zeta) = (K, \sigma, \zeta_q^{q/p}) = (K_1, \sigma|_{K_1}, \zeta_q) = (a_1, \zeta_q; \zeta) \in \mathrm{Br}(k).$$

Препятствието тогава придобива вида:

$$[K, C_q, \zeta](a_2, a_1; \zeta) = (a_1, \zeta_q; \zeta)(a_2, a_1; \zeta) = (\zeta_q^{-1} a_2, a_1; \zeta) \in \mathrm{Br}(k).$$

Нека сега $(\zeta_q^{-1} a_2, a_1; \zeta) = 1$, значи съществува $y \in K_1$ такова, че $N_{K_1/k}(y) = \zeta_q^{-1} a_2$. Можем за простота още да считаме, че $K = k(\sqrt[q]{a_1})$. Полагаме

$$\omega = \sqrt[q]{a_1} y^{p-1} \sigma(y)^{p-2} \cdots \sigma^{p-2}(y).$$

Тогава имаме $\sigma(\omega)/\omega = \zeta_q N_{K_1/k}(y)/y^p = a_2/y^p \in L^{*p}$ и $\tau(\omega)/\omega = 1$. Следователно, $L(\sqrt[p]{\omega})/k$ е разширение на Галоа. Нека g_1 и g_2 са автоморфизмите от $\mathrm{Gal}(L(\sqrt[p]{\omega})/k)$, които се изобразяват, съответно в σ и τ. Можем да дефинираме тяхното действие така: $g_1(\sqrt[p]{\omega}) = \sqrt[p]{\omega}\sqrt[p]{a_2}/y$ и $g_2(\sqrt[p]{\omega}) = \sqrt[p]{\omega}$. Релациите $g_1^{pq} = g_2^p = 1$ и $g_1^q = [g_2, g_1] = g_2^{-1} g_1^{-1} g_2 g_1$ сега лесно се проверяват, откъдето $L(\sqrt[p]{\omega})/k$ е точно $M(p^n)$ разширение. □

Пример 4.3.9. Да предположим, че примитивен q-ти корен на единицата ζ_q е в k^*, но не е в k^{*p}. Нека отново да приемем,че $K/k = k(\sqrt[q]{a_1})/k$ е C_q разширение. Полагаме $b_0 = \sqrt[q]{a_1}$ и $b_1 = \zeta_q$. Тогава имаме $b_1 = \sigma(b_0)/b_0 \in K^* \setminus K^{*p}, \sigma(b_1)/b_1 = 1$ и $c = b_1^{q/p} = \zeta_q^{q/p} = \zeta \neq 1$. От теорема 4.3.2 тогава следва, че $K(\sqrt[pq]{a_1}, \sqrt[p]{\zeta_q})/k$ е $M(p^n)$ разширение. Същият резултат може да получим, ако положим $a_2 = \zeta_q$ и $\omega = \sqrt[q]{a_1}$, понеже $(\zeta_q^{-1} a_2, a_1; \zeta) = (1, a_1; \zeta) = 1$. □

Пример 4.3.10. Нека $n > 3$. Да предположим, че $\zeta \in N_{K/k}(K^*)$, т.е. съществува $\omega \in K^*$ такова, че $\zeta = N_{K/k}(\omega)$. Да вземем произволен елемент $\omega_1 \in K_1^* \setminus k^*$. Тогава ще имаме $N_{K/k}(\omega_1) = [N_{K_1/k}(\omega_1)]^{q/p} = f^{q/p}$ за $f = N_{K_1/k}(\omega_1)$, и единственото ограничение

върху избора на ω_1, от което се нуждаем е $f \in k^* \setminus K_1^{*p} \cap k^*$. Ако положим $x = \omega_1^{-1}\omega$ и $b_1 = fx^p$, имаме $c = f^{q/p}N_{K/k}(x) = \zeta$. Тогава за всяко b_0 такова, че $\sigma(b_0)/b_0 = b_1$, ние ще получим $M(p^n)$ разширение $L/k = K(b_0^{1/p}, (N_{K_1/k}(\omega_1))^{1/p})/k$.

Да отбележим, че предположението $\zeta \in N_{K/k}(K^*)$ означава, че цикличната алгебра $[K, C_q, \zeta]$ се разпада в $\mathrm{Br}(k)$, което води до препятствието $(a_2, a_1; \zeta) \in \mathrm{Br}(k)$. В този случай разпадането на препятствието е еквивалентно на $a_2 = f = N_{K_1/k}(\omega_1) \in k^* \setminus K_1^{*p} \cap k^*$. □

4.3.2 Рестрикции, корестрикции и препятствия

Ще започнем с описанието на рестрикции на групови разширения, получени с помощта на транзитивни влагания на някои 2-групи в симетричната група S_{2^l}.

Лема 4.3.11. ([Mi4, Lemma 4.1]) *Да разгледаме изображението на рестрикция*

$$\mathrm{res} : H^2(S_d, \mu_2) \longrightarrow H^2(G, \mu_2),$$

където G се влага транзитивно в симетричната група S_d от степен $d = 2^l \geq 4$, според метода описан в параграф 2.5 (с използването на примитивен елемент).

1. ([DEK, Lemma 2]) *Нека $G = C_2 \times C_2$. Тогава* $\mathrm{res}(s_4)$ *съответства на груповото разширение*
$$1 \longrightarrow \mu_2 \longrightarrow Q_8 \longrightarrow C_2 \times C_2 \longrightarrow 1.$$

2. *Нека $G = C_{2^{n-2}} \times C_2$ за $n \geq 4$. Тогава* $\mathrm{res}(s_{2^{n-1}})$ *съответства на груповото разширение*
$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{C_{2^{n-2}} \times C_2} \longrightarrow C_{2^{n-2}} \times C_2 \longrightarrow 1,$$
където $\widetilde{C_{2^{n-2}} \times C_2}$ има представяне: $x^{2^{n-2}} = y^2 = 1, yx = -xy$.

3. *Нека $G = M(2^n)$. Тогава* $\mathrm{res}(s_{2^n})$ *съответства на груповото разширение*
$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{M(2^n)} \longrightarrow M(2^n) \longrightarrow 1,$$
където $\widetilde{M(2^n)} \cong \widetilde{M}(2^{n+1})$ е групата описана преди теорема 4.3.6 за $p = 2$.

Доказателство: (1) Нека $L/k = k(\sqrt{a}, \sqrt{b})/k$ е $C_2 \times C_2$ разширение. Тогава $\theta = \sqrt{a}+\sqrt{b}$ е примитивен елемент на L/k. Спрегнатите на θ са: $\theta = \theta_1 = \sqrt{a}+\sqrt{b}, \theta_2 = -\sqrt{a}+\sqrt{b}, \theta_3 = \sqrt{a}-\sqrt{b}$ и $\theta_4 = -\sqrt{a}-\sqrt{b}$. Тогава $\sigma = (1,2)(3,4)$ и $\tau = (1,3)(2,4)$ са

пораждащите на $C_2 \times C_2 = \mathrm{Gal}(L/k)$. Тъй като произведението на две независими транспозиции се повдига до елемент от ред 4 в $\widetilde{S}_4$, получаваме $\widetilde{C_2 \times C_2} \cong Q_8$.

(2) Нека $L/k = k(\alpha, \sqrt{b})/k$ е $C_{2^{n-2}} \times C_2$ разширение, и нека σ и τ са пораждащите на последната група: $\sigma^{2^{n-2}} = \tau^2 = 1, \sigma\tau = \tau\sigma$. Полагаме $\alpha_1 = \alpha, \alpha_2 = \sigma(\alpha_1), \ldots, \alpha_{2^{n-2}} = \sigma^{2^{n-2}-1}(\alpha_1)$. Тогава $\theta = \alpha + \sqrt{b}$ е примитивен елемент на L/k и спрегнатите на θ са

$$\theta_1 = \theta, \theta_2 = \alpha_2 + \sqrt{b}, \ldots, \theta_{2^{n-2}} = \alpha_{2^{n-2}} + \sqrt{b},$$
$$\theta_{2^{n-2}+1} = \alpha_1 - \sqrt{b}, \theta_{2^{n-2}+2} = \alpha_2 - \sqrt{b}, \ldots, \theta_{2^{n-1}} = \alpha_{2^{n-2}} - \sqrt{b}.$$

Следователно,

$$\sigma = (1, 2, \ldots, 2^{n-2})(2^{n-2}+1, 2^{n-2}+2, \ldots, 2^{n-1}),$$
$$\tau = (1, 2^{n-2}+1)(2, 2^{n-2}+2)\cdots(2^{n-2}, 2^{n-1}).$$

Тъй като $n \geq 4$ и про-образите $\widetilde{(i,j)}$ и $\widetilde{(k,l)}$ на две независими транспозиции антикомутират, получаваме $\widetilde{\sigma}^{2^{n-2}} = \widetilde{\tau}^2 = 1$.

Да положим сега $\sigma_1 = (1, 2, \ldots, 2^{n-2})$ и $\sigma_2 = (2^{n-2}+1, 2^{n-2}+2, \ldots, 2^{n-1})$. Пресмятанията показват, че $\tau\sigma_1\tau = \sigma_2$. Можем да запишем σ_1 и σ_2 като произведение на транспозиции:

$$\sigma_1 = (1,2)(2,3)\cdots(2^{n-2}-1, 2^{n-2}),$$
$$\sigma_2 = (2^{n-2}+1, 2^{n-2}+2)(2^{n-2}+2, 2^{n-2}+3)\cdots(2^{n-1}-1, 2^{n-1}).$$

Очевидно, всички транспозиции от разлагането на σ_1 са независими с онези от разлагането на σ_2, значи

$$\widetilde{\sigma}_1\widetilde{\sigma}_2 = (-1)^{(2^{n-2}-1)^2}\widetilde{\sigma}_2\widetilde{\sigma}_1 = -\widetilde{\sigma}_2\widetilde{\sigma}_1.$$

(3) Нека $L/k = K(\sqrt{b_0}, \sqrt{f})/k$ е $M(2^n)$ разширение според описанието в теорема 4.3.2. Тогава $\theta = \sqrt{b_0} + \sqrt{f}$ е примитивен елемент на L/K. Да означим с σ и τ пораждащите на $M(2^n)$: $\sigma^{2^{n-1}} = \tau^2 = 1, \tau\sigma = \sigma^{2^{n-2}+1}\tau$. С подобни разсъждения както в (2), получаваме разлагането на σ и τ в S_{2^n}:

$$\begin{aligned}\sigma &= (1, 2, \ldots, 2^{n-1})(2^{n-1}+1, 2^{n-1}+2, \ldots, 2^n),\\ \tau &= (1, 2^{n-1}+1)(2, 2^{n-1}+2^{n-2}+2)(3, 2^{n-1}+3)(4, 2^{n-1}+2^{n-2}+4)\cdots\\ &\quad \cdots(2^{n-1}, 2^{n-1}+2^{n-2}).\end{aligned}$$

Следователно, $\widetilde{\sigma}^{2^{n-1}} = \widetilde{\tau}^2 = 1$. Полагаме $\sigma_1 = (1, 2, \ldots, 2^{n-1})$ и $\sigma_2 = (2^{n-1}+1, 2^{n-1}+2, \ldots, 2^n)$. Пресмятанията показват, че $\tau\sigma_1\tau = \sigma_2^{2^{n-2}+1}$ и $\tau\sigma_2\tau = \sigma_1^{2^{n-2}+1}$. Тук отново $\widetilde{\sigma}_1\widetilde{\sigma}_2 = -\widetilde{\sigma}_2\widetilde{\sigma}_1$, значи

$$\widetilde{\tau}\widetilde{\sigma}\widetilde{\tau} = \widetilde{\sigma}_2^{2^{n-2}+1}\widetilde{\sigma}_1^{2^{n-2}+1} = -\widetilde{\sigma}^{2^{n-2}+1}.$$

□

Сега ще опишем хомоморфизмът на корестрикция, запазвайки означенията на предишната лема.

Теорема 4.3.12. ([Mi4, Theorem 4.2]) *Нека G е крайна 2-група породена от два елемента g и h_2 такива, че $g^2 = h_1, h_2^2 = 1$ и $h_1h_2 = h_2h_1$. Нека H е подгрупата на G породена от h_1 и h_2.*

1. *Нека $G \cong C_4 \times C_2, H \cong C_2 \times C_2$ и нека $\overline{f} \in Z^2(H, \mu_2)$ представят груповото разширение*

$$1 \longrightarrow \mu_2 \longrightarrow Q_8 \longrightarrow H \longrightarrow 1.$$

Тогава $f = \mathrm{cor}_{G/H}(\overline{f}) \in Z^2(G, \mu_2)$ представя груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{C_4 \times C_2} \cong D \curlywedge C \longrightarrow G \longrightarrow 1.$$

2. *Нека $G \cong C_{2^{n-2}} \times C_2, H \cong C_{2^{n-3}} \times C_2$ за $n \geq 5$ и нека $\overline{f} \in Z^2(H, \mu_2)$ представя груповото разширение*

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{C_{2^{n-3}} \times C_2} \longrightarrow H \longrightarrow 1.$$

Тогава $f = \mathrm{cor}_{G/H}(\overline{f}) \in Z^2(G, \mu_2)$ представя груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{C_{2^{n-2}} \times C_2} \longrightarrow G \longrightarrow 1.$$

3. *Нека $G \cong M(2^n), H \cong C_{2^{n-2}} \times C_2$ за $n \geq 4$ и нека $\overline{f} \in Z^2(H, \mu_2)$ представя груповото разширение*

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{C_{2^{n-2}} \times C_2} \longrightarrow H \longrightarrow 1.$$

Тогава $f = \mathrm{cor}_{G/H}(\overline{f}) \in Z^2(G, \mu_2)$ представя груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{M(2^n)} \longrightarrow G \longrightarrow 1.$$

Доказателство: (1) Нека $L/k = k(\alpha, \sqrt{b})/k$ е $C_4 \times C_2$ разширение, където $\alpha = \sqrt{r(a+\sqrt{a})}$ за $a = 1 + c^2, c, r \in k^*$. Тогава $\theta = \alpha + \sqrt{b}$ е примитивен елемент за L/k. Означаваме с $K = k(\sqrt{a})$ неподвижното подполе L^H на H, и с

$$\theta_1 = \alpha + \sqrt{b}, \theta_2 = -\alpha + \sqrt{b}, \theta_3 = \alpha - \sqrt{b}, \theta_4 = -\alpha - \sqrt{b}$$

спрегнатите на θ над K. Тогава H се влага транзитивно в $A_4 \hookrightarrow SO_4(k)$:

$$h_1 = (1,2)(3,4), h_2 = (1,3)(2,4).$$

Нататък, полагаме $\alpha' = g(\alpha)$ и

$$\theta_5 = \alpha' + \sqrt{b}, \theta_6 = -\alpha' + \sqrt{b}, \theta_7 = \alpha' - \sqrt{b}, \theta_8 = -\alpha' - \sqrt{b}$$

– останалите спрегнати на θ над k. Индуцираното ортогонално представяне тогава ни дава транзитивно влагане на G в S_8:

$$g = (1,5,2,6)(3,7,4,8),$$
$$h_2 = (1,3)(2,4)(5,7)(6,8).$$

Прилагайки лема 4.3.11(1), (2) и теорема 2.5.2, получаваме групата $D \leftthreetimes C$.

Ще пропуснем доказателството на останалите случаи, понеже то е аналогично. □

Забележка 4.3.13. Последната теорема може да бъде доказана също с прилагане на явната формула от теорема 2.3.9. За групи с повече пораждащи и съотношения, обаче става все по-трудно да се пресмятат корестрикциите на групови разширения.

Сега ще покажем, че двата вида транзитивни влагания в симетричната група, описани в края на параграф 2.5, могат да доведат до нееквивалентни групови разширения.

Пример 4.3.14. Нека k съдържа примитивен корен на единицата ξ от степен 2^{n-2}, но $\xi \notin k^2$. Нека $a \in k^* \setminus k^{*2}$ и нека $M = k(\sqrt[2^{n-1}]{a}, \sqrt{\xi})$, т.е. M е полето на разлагане на полинома $f(x) = x^{2^{n-1}} - a$. От пример 4.3.9 знаем, че M/k е $M(2^n)$ разширение (виж също [MR, KR]).

Ще покажем сега, че $\theta = \sqrt[2^{n-1}]{a} + \sqrt{\xi}$ е примитивен елемент на M/k. Да предположим, че $\sigma \in \mathrm{Gal}(M/k)$ оставя θ неподвижно. Тъй като $\sigma(\sqrt[2^{n-1}]{a}) = \sqrt[2^{n-1}]{a}(\sqrt{\xi})^k$

и $\sigma(\sqrt{\xi}) = (-1)^l\sqrt{\xi}$ за някои $k, l \geq 0$, получаваме, че $\sqrt[2^{n-1}]{a} + \sqrt{\xi} = \sqrt[2^{n-1}]{a}(\sqrt{\xi})^k + (-1)^l\sqrt{\xi}$. Следователно, $\sqrt[2^{n-1}]{a}(1 - (\sqrt{\xi})^k) = \sqrt{\xi}((-1)^l - 1)$, значи $a(1 - (\sqrt{\xi})^k)^{2^{n-1}} = ((-1)^l - 1)^{2^{n-1}}$, което е възможно само ако $k = l = 0$, т.е. $\sigma = 1$.

Нататък, ще вложим транзитивно $M(2^n)$ в симетричната група S_{2^n} както е описано в лема 4.3.11 (3). От [MR] знаем, че формата следа $\mathrm{tr}_{M/k} < 1 >$ на $M/k = k(\theta)/k$ е Вит-еквивалентна на формата на Пфистер $\ll \xi, a \gg$. Прилагайки теорема 2.4.6 можем да пресметнем, че препятствието (вторият клас на Стийфил-Уитни) на груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{M(2^n)} \longrightarrow M(2^n) \longrightarrow 1.$$

е (a, ξ).

Нека сега $L = k(\sqrt[2^{n-1}]{a})$. Пресмятанията показват, че формата следа $\mathrm{tr}_{L/k} < 1 >$ е Вит-еквивалентна на квадратичната форма $< 2, 2a >$. Тогава $M(2^n)$ се влага транзитивно в $S_{2^{n-1}}$ и рестрикцията $\mathrm{res}(s_{2^{n-1}})$ съответства на груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{M(2^n)}' \longrightarrow M(2^n) \longrightarrow 1,$$

чието препятствие се разпада. Наистина, $2 \notin k^2$ за $n = 4$, значи препятствието е $(2, 2a)(2, a) = 1$. Ако $n > 4$ то $2 \in k^2$ и препятствието е $(1, a) = 1$. Всичко това показва, че двете групови разширения са нееквивалентни. $\square$

Нататък, ще покажем, че групата $H^2(C_q \times C_2, \mu_2)$ е изоморфна на μ_2^3 за $n \geq 4$, групата $H^2(M(2^n), \mu_2)$ е изоморфна на μ_2^2, и хомоморфизмът на корестрикция $\mathrm{cor} : H^2(C_q \times C_2, \mu_2) \to H^2(M(2^n), \mu_2)$ е сюрективен. Наистина, елементите $c_{\varepsilon_1,\varepsilon_2,\varepsilon_3} \in H^2(C_q \times C_2, \mu_2)$ за $\varepsilon_i = \pm 1$ се определят от нееквивалентните групови разширения

$$1 \longrightarrow \mu_2 \longrightarrow G_{\varepsilon_1,\varepsilon_2,\varepsilon_3} \underset{\widetilde{\tau}\mapsto\tau}{\overset{\widetilde{\sigma}\mapsto\sigma}{\longrightarrow}} C_q \times C_2 \longrightarrow 1,$$

където $\widetilde{\sigma}^q = \varepsilon_1, \widetilde{\tau}^2 = \varepsilon_2, [\widetilde{\tau}, \widetilde{\sigma}] = \varepsilon_3$.

Аналогично, елементите $c_{\varepsilon_2,\varepsilon_3} \in H^2(M(2^n), \mu_2)$ за $\varepsilon_i = \pm 1$ се определят от груповите разширения

$$1 \longrightarrow \mu_2 \longrightarrow G_{\varepsilon_2,\varepsilon_3} \underset{\widetilde{\beta}\mapsto\beta}{\overset{\widetilde{\alpha}\mapsto\alpha}{\longrightarrow}} M(2^n) \longrightarrow 1,$$

където $\widetilde{\beta}^2 = \varepsilon_2, \widetilde{\alpha}^q[\widetilde{\beta}, \widetilde{\alpha}] = \varepsilon_3$ и $\widetilde{\alpha}^{2q} = 1$, понеже не съществува група с експонента 2^n, която има фактор-група изоморфна на модулярната група от ред 2^n.

Да припомним, че от теорема 4.3.12 (3) имаме, че корестрикцията на 2-кокласа $c_{1,1,-1}$ съответстващ на груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{C_{2^{n-2}} \times C_2} \longrightarrow C_{2^{n-2}} \times C_2 \longrightarrow 1.$$

е 2-кокласът $c_{1,-1}$, който представя груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{M(2^n)} \longrightarrow M(2^n) \longrightarrow 1.$$

Подобни разсъждения показват също, че $\mathrm{cor}(c_{-1,1,1}) = c_{-1,-1}$ и $\mathrm{cor}(c_{-1,1,-1}) = c_{-1,1}$.

С помощта на някои кохомологични престмятания може да се покаже, че всяка от горните групи има своите 'двойници' за нечетно p, значи групата $H^2(C_q \times C_p, \mu_p)$ е изоморфна на μ_p^3 за $n \geq 4$ и групата $H^2(M(p^n), \mu_p)$ е изоморфна на μ_p^2. Изненадващо, обаче корестрикцията $\mathrm{cor} : H^2(C_q \times C_p, \mu_p) \to H^2(M(p^n), \mu_p)$ не е сюрективна, както ще видим.

Нека първо да опишем кохомологичните групи. Да вземем групата $M(p^n)$ с пораждащи α и β както в началото на параграф 4.3. Подгрупата породена от $\sigma = \alpha^p$ и $\tau = \beta$ е изоморфна на $C_q \times C_p$. Елементите $c_{\varepsilon_1,\varepsilon_2,\varepsilon_3} \in H^2(C_q \times C_p, \mu_p)$ за $\varepsilon_i = \zeta^k$ се определят от груповите разширения

$$1 \longrightarrow \mu_p \longrightarrow G_{\varepsilon_1,\varepsilon_2,\varepsilon_3} \underset{\substack{\widetilde{\sigma}\mapsto\sigma \\ \widetilde{\tau}\mapsto\tau}}{\longrightarrow} C_q \times C_p \longrightarrow 1,$$

където $\widetilde{\sigma}^q = \varepsilon_1, \widetilde{\tau}^p = \varepsilon_2, [\widetilde{\tau}, \widetilde{\sigma}] = \varepsilon_3$.

Аналогично, елементите $c_{\varepsilon_2,\varepsilon_3} \in H^2(M(p^n), \mu_p)$ за $\varepsilon_i = \zeta^k$ се определят от груповите разширения

$$1 \longrightarrow \mu_p \longrightarrow G_{\varepsilon_2,\varepsilon_3} \underset{\substack{\widetilde{\alpha}\mapsto\alpha \\ \widetilde{\beta}\mapsto\beta}}{\longrightarrow} M(p^n) \longrightarrow 1,$$

където $\widetilde{\beta}^p = \varepsilon_2, \widetilde{\alpha}^q[\widetilde{\beta}, \widetilde{\alpha}] = \varepsilon_3$ и $\widetilde{\alpha}^{pq} = 1$.

Да изберем $\overline{f} = c_{\varepsilon_1,\varepsilon_2,\varepsilon_3}$ и нека $f = \mathrm{cor}_{M(p^n)/C_q \times C_p}(\overline{f})$. Ще пресметнем редът на $\widetilde{\beta}$. Да припомним, че $\alpha\beta\alpha^{-1} = \alpha^{-q}\beta = \sigma^{-q/p}\tau$. Тогава, според теорема 2.3.9 получаваме

$$f(\beta, \beta^{p-1}) = \prod_{k=0}^{p-1} \overline{f}(\alpha^k\beta\alpha^{-k}, \alpha^k\beta^{p-1}\alpha^{-k}) = \prod_{k=0}^{p-1} \overline{f}(\sigma^{-kq/p}\tau, (\sigma^{-kq/p}\tau)^{p-1}).$$

Тъй като всеки множител в горното произведение е равен на 1 за $\varepsilon_1 = \varepsilon_2 = 1$ и $\varepsilon_3 = \zeta$, получаваме $\widetilde{\beta}^p = 1$. От друга страна, за $\varepsilon_1 = \zeta, \varepsilon_2 = 1$ и $\varepsilon_3 = 1$ имаме $(\widetilde{\sigma}^{-kq/p}\tau)^p = \zeta^{-k}$,

значи $f(\beta,\beta^{p-1})=\zeta^{-1-2-\cdots-(p-1)}=\zeta^{-p(p-1)/2}=1$, за разлика от случая $p=2$, когато стойността на $\zeta^{-p(p-1)/2}$ е -1. Това означава, че за нечетно p редът на $\widetilde{\beta}$ е p, докато за $p=2$ редът му е 4.

Нататък, нека p е произволно просто число, да положим $\widetilde{C_q\times C_p}=G_{1,1,\zeta}$ и да означим с $\overline{f}\in Z^2(C_q\times C_p,\mu_p)$ 2-коцикълът съответстващ на груповото разширение

$$1\longrightarrow\mu_p\cong\langle\zeta\rangle\longrightarrow\widetilde{C_q\times C_p}\underset{\substack{\widetilde{\sigma}\mapsto\sigma\\ \widetilde{\tau}\mapsto\tau}}{\longrightarrow}C_q\times C_p\longrightarrow 1. \tag{4.11}$$

Прилагайки явната формула от теорема 2.3.9, може да се покаже, че 2-коцикълът $f=\mathrm{cor}_{M(p^n)/C_q\times C_p}(\overline{f})\in Z^2(M(p^n),\mu_p)$ съответства на груповото разширение:

$$1\longrightarrow\mu_p\cong\langle\zeta\rangle\longrightarrow\widetilde{M}(p^{n+1})\underset{\substack{\widetilde{\alpha}\mapsto\alpha\\ \widetilde{\beta}\mapsto\beta}}{\longrightarrow}M(p^n)\longrightarrow 1. \tag{4.12}$$

Да вземем сега произволно $M(p^n)$ разширение L/k, според описанието дадено в теорема 4.3.2: $L/k=K(\sqrt[p]{b_0},\sqrt[p]{a_2})/k$, където $b_0\in K^*\setminus K^{*p}$, $a_2\in k^*\setminus k^*\cap K^{*p}$ и $x\in K^*$ са такива, че $\sigma(b_0)/b_0=a_2x^p$, и $c=a_2^{q/p}N_{K/k}(x)$ е p-ти корен на единицата, но $c\neq 1$. Нещо повече, имаме включването $k(\sqrt[p]{a_1},\sqrt[p]{a_2})\subset L$, където $K_1=k(\sqrt[p]{a_1})=L^{C_q\times C_p}$. От теорема 2.2.1 следва, че препятствието на задачата за вложимост зададена чрез L/K и (4.11) е $(a_2,a_1';\zeta)\in\mathrm{Br}_p(K_1)$, където $a_1'\in K_1^*\setminus K_1^{*p}$ е такова, че $N_{K_1/k}(a_1')=a_1$.

Теорема 4.3.15. ([Mi4, Proposition 4.3]) *Препятствието на задачата за вложимост зададена чрез L/k и (4.12) е $(a_2,a_1;\zeta)\in\mathrm{Br}_p(k)$.*

Доказателство: За да получим препятствието, трябва само да приложим проекционната формула: $\mathrm{cor}_{K_1/k}(a_2,a_1';\zeta)=(a_2,N_{K_1/k}(a_1');\zeta)=(a_2,a_1;\zeta)$. □

Теорема 4.3.16. ([Mi4, Proposition 4.4]) *Препятствието на задачата за вложимост зададена чрез L/k и груповото разширение*

$$1\longrightarrow\mu_p\longrightarrow G_{\zeta,1}\underset{\substack{x\mapsto\alpha\\ y\mapsto\beta}}{\longrightarrow}M(p^n)\longrightarrow 1,$$

където $G_{\zeta,1}\cong\langle x,y\mid x^{p^{n-1}}=y^{p^2}=1, y^p-$ централен, $yx=x^{q+1}y\rangle$ е $(a_2,\zeta;\zeta)\in\mathrm{Br}_p(k)$.

Доказателство: Да разгледаме груповото разширение

$$1\longrightarrow\mu_p\longrightarrow M(p^n)\times C_p\underset{\substack{\alpha\mapsto\alpha\\ \beta\mapsto\beta}}{\longrightarrow}M(p^n)\longrightarrow 1. \tag{4.13}$$

Да забележим, че според дефиниция 2.2.3 имаме, че $G_{\zeta,1} = (M(p^n) \times C_p)^{(p^2,\beta)}$ и следователно можем да приложим теорема 2.2.4. Тъй като препятствието на задачата зададена чрез L/k и (4.13) е тривиално и препятствието на задачата зададена чрез K_2/k и груповото разширение $1 \longrightarrow \mu_p \longrightarrow C_{p^2} \longrightarrow C_p \longrightarrow 1$ е $(a_2, \zeta; \zeta) \in \mathrm{Br}_p(k)$, получаваме желаният резултат. □

Препятствието в следващата теорема сега се пресмята лесно, като се отчете структурата на кохомологичната група $H^2(M(p^n), \mu_p)$.

Теорема 4.3.17. ([Mi4, Proposition 4.5]) *Препятствието на задачата за вложимост зададена чрез L/k и груповото разширение*

$$1 \longrightarrow \mu_p \longrightarrow G_{\zeta,\zeta} \underset{\substack{x \mapsto \alpha \\ y \mapsto \beta}}{\longrightarrow} M(p^n) \longrightarrow 1,$$

където $G_{\zeta,\zeta} \cong \langle x, y \mid x^{p^{n-1}} = y^{p^2} = 1, y^p -$ централен, $yx = x^{q+1}y^{p+1} \rangle$ е $(\zeta a_1, a_2; \zeta) \in \mathrm{Br}_p(k)$.

Глава 5
Препятствия за реализиране на неабеловите 2-групи, имащи циклична подгрупа с индекс 2

Неабеловите групи от ред 2^{n+3} ($n \geq 1$), имащи циклична подгрупа с индекс 2 са едни от най-често срещаните групи в работи разглеждащи въпроси от теорията на Галоа. Намирането на необходими и достатъчни условия за реализирането на тези групи, като групи на Галоа над произволни полета с характеристика различна от 2 представлява сериозно предизвикателство, като един все още нерешен напълно проблем при $n \geq 3$. Ако основното поле съдържа примитивен корен на единицата от степен 2^{n+1}, Фрьолих пресмята в [Fr] препятствията за реализирането на диедралната и кватернионната групи от ред 2^{n+3} ($n \geq 1$).

В тази глава пресмятаме препятствията на задачите за вложимост с циклично ядро от ред 2^n за четирите такива групи, като отслабваме изискването за корените на едницата, предполагайки само, че за някой примитивен 2^n-ти корен на единицата ζ, елементите $\zeta + \zeta^{-1}$ и $i(\zeta - \zeta^{-1})$ едновременно се съдържат в основното поле k.

В параграф 5.4 даваме явно описание на разширенията на Галоа, които реализират модулярната група от ред от ред 2^{n+3} при предположението, че примитивен корен на единицата от степен 2^{n+2} се съдържа в квадратично разширение на основното поле.

Резултатите от тази глава са публикувани в работите [Mi1, Mi2].

5.1 Препятствие за реализирането на цикличната 2-група

Да означим както обикновено с C_{2^n} цикличната група от ред $2^n (n \geq 1)$ породена от елемента σ. Да разгледаме първо задачата за вложимост зададена с квадратичното разширение $k(\sqrt{a})/k$ за $a \in k^* \setminus k^{*2}$ и груповото разширение

$$1 \longrightarrow C_2 = \{\pm 1\} \hookrightarrow C_4 \longrightarrow C_2 \longrightarrow 1. \tag{5.1}$$

Препятствието е добре известно: $(a, a) \in \mathrm{Br}(k)$. Нека сега $(a, a) = 1 \in \mathrm{Br}(k)$. Можем да предполагаме,че $a = 1 + c^2, c \in k^*$. Множеството на всички решения на (5.1) тогава се задава така: $\{k(\sqrt{r(a + \sqrt{a})}) \mid r \in k^*\}$. Наистина, ако положим $\varphi = \sqrt{r(a + \sqrt{a})}, \psi = \sqrt{r(a - \sqrt{a})}$ и $K = k(\varphi)$, то $\mathrm{Gal}(K/k)$ се поражда от елемента $\sigma : \varphi \mapsto \psi, \psi \mapsto -\varphi$, където $\varphi\psi = rc\sqrt{a}$.

Също така е извесно, че препятствието на задачата за вложимост $(K/k, C_8, C_2)$ зададена с груповото разширение

$$1 \longrightarrow C_2 = \{\pm 1\} \hookrightarrow C_8 \longrightarrow C_4 \longrightarrow 1. \tag{5.2}$$

е $(a, 2)(-1, r) \in \mathrm{Br}(k)$. В термините на нормени изображения, задачата е разрешима тогава и само тогава, когато $-1 \in N_{K/k}(K^*)$. Ако $i \in k$, то задачата за вложимост зададена с $k(\sqrt{a})/k$ и (5.1) винаги е разрешима и всички решения могат да се опишат по този начин: $K/k = k(\sqrt[4]{a'})/k$, където $a' = [2r(1 - ic)]^2 a$. В този случай, препятствието на задачата за вложимост зададена с K/k и (5.2) е $(a, 2)(-1, r) = (a, 2) = (a, i) \in \mathrm{Br}(k)$.

Лема 5.1.1. ([Mi2, Lemma 2.1]) *Нека $\zeta \in k$ е примитивен 2^n-ти корен на единицата $(n \geq 1)$, нека $K/k = k(\sqrt[4]{a})/k$ е C_4 разширение, и нека $\sigma \in C_4$ се задава с $\sigma(\sqrt[4]{a}) = i\sqrt[4]{a}$. За да бъде задачата за вложимост $(K/k, C_{2^{n+2}}, \mu_{2^n})$ зададена с груповото разширение*

$$1 \longrightarrow \mu_{2^n} \hookrightarrow C_{2^{n+2}} \longrightarrow C_4 \longrightarrow 1 \tag{5.3}$$

разрешима, е необходимо да съществуват $\alpha, \beta \in k, \alpha \neq 0$ такива, че $\alpha^2 - a\beta^2 = \zeta$. В този случай препятствието е $(a, \alpha)(\zeta, \alpha\beta) \in \mathrm{Br}(k)$.

Доказателство: Ще приложим математическа индукция по n. При $n = 1$ имаме $i^2 = -1 = \zeta$, така че можем да положим $\alpha = i, \beta = 0$ за да получим препятствието $(a, i) \in \mathrm{Br}(k)$.

Нека сега да предположим, че задачата за вложимост зададена с K/k и

$$1 \longrightarrow \mu_{2^{n-1}} \hookrightarrow C_{2^{n+1}} \longrightarrow C_4 \longrightarrow 1$$

е разрешима. Тогава можем да положим $\alpha = \zeta, \beta = 0$, откъдето препятствието е $(a,\zeta)(\zeta^2,0) = (a,\zeta) \in \mathrm{Br}(k)$. Да отбележим, че появата в даден централизатор на елементи j и $k \neq 0$ със съотношения $j^2 = c^2, k^2 = 0$ и $jk = -kj$ означава, че той се разпада.

Разрешимостта на съпътстващата задача $(K/k, C_4, \mu_{2^{n-1}})$, обаче е необходима за разрешимостта на задачата $(K/k, C_{2^{n+2}}, \mu_{2^n})$. Тогава трябва да имаме $(a,\zeta) = 1 \in \mathrm{Br}(k)$, значи съществуват $\alpha, \beta \in k$ такива, че $\alpha^2 - a\beta^2 = \zeta$. Ние винаги можем да получим $\alpha \neq 0$ по следния начин: Тъй като $i \in k$, имаме $\zeta = x^2 + y^2$, за някои $x, y \in k, y \neq 0$. Ако $-a\beta^2 = \zeta$ полагаме $\alpha' = y(1 + x^2/y^2) \neq 0$ и $\beta' = i\beta x/y$. Следователно

$$\alpha'^2 - a\beta'^2 = y^2(1 + x^2/y^2)^2 + a\beta^2x^2/y^2 = \zeta(1 + x^2/y^2) - \zeta x^2/y^2 = \zeta.$$

Да разгледаме сега алгебрата $\Gamma = k[\sqrt[4]{a}, u], u^4 = \zeta, ux = \sigma(x)u, \forall x \in K$, представяща препятствието. Следните две кватернионни алгебри се съдържат в Γ:

$$\begin{aligned} Q_1 &: i_1 = \sqrt{a}, \quad j_1 = (\alpha + \beta\sqrt{a} + iu^2)u, \\ Q_2 &: i_2 = u^2, \quad\ \ j_2 = \sqrt[4]{a}(\alpha + i\beta\sqrt{a} + u^2). \end{aligned}$$

Имаме $i_1j_1 = -j_1i_1, i_2j_2 = -j_2i_2, i_1^2 = a, j_1^2 = ((\alpha + iu^2)^2 - a\beta^2)u^2 = (\alpha^2 + 2\alpha iu^2 - u^4 - a\beta^2)u^2 = 2\alpha i\zeta, i_2^2 = \zeta, j_2^2 = \sqrt{a}((\alpha + i\beta\sqrt{a})^2 - u^4) = \sqrt{a}(\alpha^2 + 2\alpha\beta i\sqrt{a} - \beta^2a - \zeta) = 2\alpha\beta ia$. Очевидно i_1 комутира с Q_2 и i_2 комутира с Q_1. Накрая, проверяваме равенството $j_2j_1 = j_1j_2$:

$$\begin{aligned} j_2j_1 &= \sqrt[4]{a}(\alpha^2 + \alpha\beta\sqrt{a} + \alpha iu^2 + \alpha\beta i\sqrt{a} + i\beta^2a - \beta\sqrt{a}u^2 + \alpha u^2 + \beta\sqrt{a}u^2 + i\zeta)u \\ &= \sqrt[4]{a}(\alpha^2 + \alpha\beta\sqrt{a}(1+i) + \alpha(1+i)u^2 + i(a\beta^2 + \zeta))u \\ &= \sqrt[4]{a}(\alpha^2 + \alpha\beta\sqrt{a} + \alpha u^2)(1+i)u \end{aligned}$$

и

$$\begin{aligned} j_1j_2 &= (\alpha + \beta\sqrt{a} + iu^2)\sqrt[4]{a}i(\alpha - i\beta\sqrt{a} + u^2)u = \sqrt[4]{a}(\alpha + \beta\sqrt{a} - iu^2)(\alpha - i\beta\sqrt{a} + \\ &u^2)iu = \sqrt[4]{a}(\alpha^2 - \alpha\beta i\sqrt{a} + \alpha u^2 + \alpha\beta\sqrt{a} - i\beta^2a + \beta\sqrt{a}u^2 - \alpha iu^2 - \beta\sqrt{a}u^2 - \\ &i\zeta)iu = \sqrt[4]{a}(\alpha^2 - i\beta^2a - i\zeta + \alpha\beta\sqrt{a}(1-i) + \alpha u^2(1-i))iu = \sqrt[4]{a}(\alpha^2 + \\ &\alpha\beta\sqrt{a} + \alpha u^2)(1-i)iu = \sqrt[4]{a}(\alpha^2 + \alpha\beta\sqrt{a} + \alpha u^2)(1+i)u. \end{aligned}$$

Следователно кватернионните алгеби комутират и получаваме разлагането

$$[\Gamma] = [Q_1][Q_2] = (a, 2\alpha i\zeta)(\zeta, 2\alpha\beta ia) = (a, \alpha)(\zeta, \alpha\beta) \in \mathrm{Br}(k).$$

□

Сега ще насочим нашето внимание към случая когато за един примитивен 2^n-ти корен на единицата ζ имаме, че $\zeta + \zeta^{-1}$ и $i(\zeta - \zeta^{-1})$ едновременно се съдържат в k. Оказва се, че препятствията за задачи с циклични групи играят важна роля при пресмятанията на препятствията за диедралната, полудиедралната, кватернионната и модулярната 2-групи, на които са посветени следващите два параграфа.

Ще разгледаме трите възможности за местоположението на i в $K(i)$:

1. $i \in k$. Можем да запишем $K/k = k(\sqrt[4]{a})/k, a \in k^*$. Както видяхме в теорема 5.1.1, препятствието на задачата за вложимост $(K/k, C_{2^{n+2}}, \mu_{2^n})$ е $(a, \alpha)(\zeta, \alpha\beta) \in \mathrm{Br}(k)$, където съществуването на $\alpha, \beta \in k, \alpha \neq 0$, за които $\alpha^2 - a\beta^2 = \zeta$ е необходимо условие за разрешимостта на тази задача. В частност, квадратичното разширение $k(\sqrt{a})/k$ може да се вложи в $C_{2^{n+2}}$ разширение, тогава и само тогава, когато $k(\sqrt[4]{r^2a})/k$ може да се вложи в $C_{2^{n+2}}$ разширение за някое $r \in k^*$. Следователно, задачата за вложимост зададена с $k(\sqrt{a})/k$ и груповото разширение

   $$1 \longrightarrow C_{2^{n+1}} \hookrightarrow C_{2^{n+2}} \longrightarrow C_2 \longrightarrow 1$$

   е разрешима тогава и само тогава, когато $(a, \zeta) = 1 \in \mathrm{Br}(k)$ и $(a, \alpha)(\zeta, r\alpha\beta) = 1 \in \mathrm{Br}(k)$.

2. $a = -1$. Трябва да имаме $-1 = u^2 + v^2$, за някои $u, v \in k$ и $K = k(\sqrt{r(1 - iu)})$ за някое $r \in k^*$. Според теорема 1.6.1 задачата за вложимост $(k(\sqrt{a'})/k, C_{2^{n+2}}, C_{2^n})$ за $a' = r(1 - iu)$ съответстваща на груповото разширение

   $$1 \longrightarrow C_{2^n} \hookrightarrow C_{2^{n+2}} \longrightarrow C_4 \longrightarrow 1 \tag{5.4}$$

   е разрешима тогава и само тогава, когато задачите за вложимост $(k(\sqrt{a'})/k(i), C_{2^{n+1}}, C_{2^n})$ и $(K/k, C_8, C_2)$ съответстващи на

   $$1 \longrightarrow C_{2^n} \hookrightarrow C_{2^{n+1}} \longrightarrow C_2 \longrightarrow 1 \tag{5.5}$$

   и

   $$1 \longrightarrow C_2 \hookrightarrow C_8 \longrightarrow C_4 \longrightarrow 1. \tag{5.6}$$

са разрешими. Но задачата за вложимост съответстваща на (5.5) е разрешима тогава и само тогава, когато задачата $(k(\sqrt[4]{r'^2a'})/k, C_{2^{n+1}}, C_{2^{n-1}})$ е разрешима за някое $r' \in k^*$. Тъй като $\alpha'^2 - a'r'^2\beta'^2 = \zeta^2$ се удовлетворява за $\alpha' = \zeta, \beta' = 0$, според теорема 5.1.1 препятствието е $(a', \alpha')(\zeta^2, \alpha'\beta') = (a', \alpha') = (a', \zeta) = (r(1 - iu), \zeta) \in \mathrm{Br}(k(i))$. Съответно, препятствието на задачата съответстваща на (5.2) е $(-1, r) \in \mathrm{Br}(k)$. Следователно, задачата $(k(\sqrt{a'})/k, C_{2^{n+2}}, C_{2^n})$ е разрешима тогава и само тогава, когато $(-1, r) = 1 \in \mathrm{Br}(k)$ и $(r(1 - iu), \zeta) = 1 \in \mathrm{Br}(k(i))$.

В частност, $k(i)/k$ може да се вложи в $C_{2^{n+2}}$ разширение тогава и само тогава, когато $(-1, -1) = 1 \in \mathrm{Br}(k)$, $(-1, r) = 1 \in \mathrm{Br}(k)$ и $(r(1 - iu), \zeta) = 1 \in \mathrm{Br}(k(i))$ за някое $r \in k^*$, където $u, v \in k^*$ са такива, че $-1 = u^2 + v^2$.

3. a и -1 са квадратично независими. Тук $K = k(\sqrt{r(a + \sqrt{a})})$ и $K(i) = k(i, \sqrt[4]{a'})$ за $a' = [2r(1-ic)]^2a$. Според следствие 1.6.3 задачата за вложимост $(K/k, C_{2^{n+2}}, C_{2^n})$ е разрешима тогава и само тогава, когато задачите $(K(i)/k(i), C_{2^{n+2}}, \mu_{2^n})$ и $(K/k, C_8, C_2)$ са разрешими. Следователно задачата $(K/k, C_{2^{n+2}}, C_{2^n})$ е разрешима тогава и само тогава, когато $(a, 2)(-1, r) = 1 \in \mathrm{Br}(k)$ и $(a, \alpha')(\zeta, \alpha'\beta') = 1 \in \mathrm{Br}(k(i))$, където $\alpha' \in k(i)^*, \beta' \in k$ са такива, че $\alpha'^2 - a'\beta'^2 = \zeta$.

   В частност, квадратичното разширение $k(\sqrt{a})/k$ може да се вложи в $C_{2^{n+2}}$ разширение тогава и само тогава, когато $(a, a) = 1$, $(a, 2)(-1, r) = 1 \in \mathrm{Br}(k)$ и $(a, \alpha')(\zeta, \alpha'\beta') = 1 \in \mathrm{Br}(k(i))$ за някое $r \in k^*$, където $x, y \in k^*$ са такива, че $a = x^2 + y^2$ и $\alpha' \in k(i)^*, \beta' \in k(i)$ са такива, че $\alpha'^2 - [2r(x - iy)]^2a\beta'^2 = \zeta$. Тук имаме $K(i) = k(i, \sqrt[4]{a''})$ за $a'' = [2r(x - iy)]^2a$.

По този начин доказахме следната

Теорема 5.1.2. ([Mi2, Theorem 2.2]) *Нека ζ е примитивен 2^n-ти корен на единицата такъв, че $\zeta + \zeta^{-1} \in k$ и $i(\zeta - \zeta^{-1}) \in k$. Нека $K/k = k(\sqrt{r(a + \sqrt{a})})/k$ е C_4 разширение за $a = 1 + c^2, r \in k^*$. Тогава задачата за вложимост зададена с K/k и груповото разширение*

$$1 \longrightarrow C_{2^n} \hookrightarrow C_{2^{n+2}} \longrightarrow C_4 \longrightarrow 1 \tag{5.7}$$

има следните препятствия за $n \geq 2$:

1. *$i \in k$ (т.е. $\zeta \in k$) : $(a, \alpha)(\zeta, r\alpha\beta) \in \mathrm{Br}(k)$, където трябва да имаме $\alpha \in k^*, \beta \in k$ такива, че $\alpha^2 - a\beta^2 = \zeta$.*

2. $a = -1$ *:* $(-1, r) \in \mathrm{Br}(k)$ *и* $(r(1 - iu), \zeta) \in \mathrm{Br}(k(i))$*, където трябва да имаме* $-1 = u^2 + v^2$ *за някои* $u, v \in k$ *и* $K = k(\sqrt{r(1 - iu)})$*.*

3. a *и* -1 *са квадратично независими:* $(a, 2)(-1, r) \in \mathrm{Br}(k)$ *и* $(a, \alpha)(\zeta, r(1-ic)\alpha\beta) \in \mathrm{Br}(k(i))$*, където трябва да имаме* $\alpha \in k(i)^*, \beta \in k(i)$ *такива, че* $\alpha^2 - a\beta^2 = \zeta$*.*

Аналогично на случая $n = 2$, разгледан в [Le2], може да се покаже, че задачата за вложимост, съответстваща на (5.4) е разрешима тогава и само тогава, когато $-1 \in N_{K/k}(K^*)$ и $\zeta \in N_{K(i)/k(i)}(K(i)^*)$ – частен случай на [AFSS, Theorem 3].

5.2 Препятствия за реализирането на диедралната, полудиедралната и кватернионната 2-групи

В този параграф ще изследваме задачи за вложимост, касаещи диедралната D_{2^n}, полудиедралната SD_{2^n} и кватернионната Q_{2^n} групи от ред $2^n, n \geq 4$. Да припомним техните представяния

$$\begin{aligned} D_{2^n} &\cong \langle \sigma, \tau | \sigma^{2^{n-1}} = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle \\ SD_{2^n} &\cong \langle \sigma, \tau | \sigma^{2^{n-1}} = \tau^2 = 1, \tau\sigma = \sigma^{2^{n-2}-1}\tau \rangle \\ Q_{2^n} &\cong \langle \sigma, \tau | \sigma^{2^{n-1}} = 1, \tau^2 = \sigma^{2^{n-2}}, \tau\sigma = \sigma^{-1}\tau \rangle \end{aligned}$$

Като начало, нека да разгледаме случая $n = 4$. Нека $K/k = k(\sqrt{r(\alpha + \beta\sqrt{a})}, \sqrt{b})/k$ е D_8 разширение, където a и b са квадратично независими, $r \in k^*$ и $\alpha, \beta \in k$ са такива, че $\alpha^2 - a\beta^2 = ab$. Означаваме $\varphi = \sqrt{r(\alpha + \beta\sqrt{a})}$ и $\psi = \sqrt{r(\alpha - \beta\sqrt{a})}$. Тогава $\varphi\psi = r\sqrt{ab}$, и D_8 се поражда от елементи σ и τ, за които

$$\begin{aligned} \sigma &: \varphi \mapsto \psi, \psi \mapsto -\varphi, \sqrt{b} \mapsto \sqrt{b}; \\ \tau &: \varphi \mapsto \varphi, \psi \mapsto -\psi, \sqrt{b} \mapsto -\sqrt{b}. \end{aligned}$$

Нека сега да разгледаме груповото разширение

$$1 \longrightarrow C_2 = \{\pm 1\} \longrightarrow G \underset{t \mapsto \tau}{\overset{s \mapsto \sigma}{\longrightarrow}} D_8 \longrightarrow 1,$$

където s и t са про-образи в G на σ и τ, съответно, такива, че $s^4 = -1, t^2 = \varepsilon_1$ и $ts = \varepsilon_2 s^3 t$ за $\varepsilon_1 = (-1)^{m_1}, \varepsilon_2 = (-1)^{m_2};\ m_1, m_2 \in \{0, 1\}$.

Алгебрата на кръстосаното произведение $\Gamma = (K, D_8, -1)$, съответстваща на груповото разширение, съдържа следните три кватернионни подалгебри:

$$\begin{aligned} &Q_1 : i_1 = t, && j_1 = \sqrt{b}, \\ &Q_2 : i_2 = (s + s^3)\sqrt{b}^{m_2}, && j_2 = \sqrt{a}, \\ &Q_3 : i_3 = s^2\sqrt{b}, && j_3 = (\varphi + \psi s)\sqrt{a}. \end{aligned}$$

Виждаме, че $i_1^2 = (-1)^{m_1}, j_1^2 = b, i_2^2 = -2b^{m_2}, j_2^2 = a, i_3^2 = -b$ и $j_3^2 = 2r\alpha a$. Тъй като Q_1, Q_2 и Q_3 комутират две по две, получаваме

$$[\Gamma] = [Q_1][Q_2][Q_3] = ((-1)^{m_1}, b)(-2b^{m_2}, a)(-b, 2r\alpha a) \in \mathrm{Br}(k).$$

Така доказахме следната

Теорема 5.2.1. *Препятствията на задачите за вложимост* $(K/k, G, C_2)$ *са следните:*

1. $m_1 = 0, m_2 = 1$ $(G = D_{16}) : (a, 2)(-b, 2r\alpha) \in \mathrm{Br}(k)$;
2. $m_1 = m_2 = 1$ $(G = Q_{16}) : (a, 2)(b, b)(-b, 2r\alpha) \in \mathrm{Br}(k)$;
3. $m_1 = m_2 = 0$ $(G = SD_{16}) : (a, -2)(-b, 2r\alpha) \in \mathrm{Br}(k)$;
4. $m_1 = 1, m_2 = 0$ $(G = SD_{16}) : (a, -2)(b, b)(-b, 2r\alpha) \in \mathrm{Br}(k)$.

Да отбележим, че имаме две различни препятствия за SD_{16}, понеже двете съответни групови разширения са нееквивалентни. Подробно изложение на теорията на препятствията за групите от ред 16 може да се намери в работите [GSS, Ki, Le1].

Нека сега K/k е D_8 разширение и нека $\zeta \in K$ е примитивен 2^n-ти корен на единицата такъв, че $\zeta \notin k, \zeta + \zeta^{-1} \in k$ и $i(\zeta - \zeta^{-1}) \in k$. Тогава $K/k = k(\sqrt[4]{a}, i)$ за някое $a \in k \setminus k^2$, и D_8 е породена от елементи σ и τ, зададени така:

$$\sigma : \sqrt[4]{a} \mapsto i\sqrt[4]{a}, i \mapsto i;\ \tau : \sqrt[4]{a} \mapsto \sqrt[4]{a}, i \mapsto -i$$

(в частност $\sigma(\zeta) = \zeta$ и $\tau(\zeta) = \zeta^{-1}$).

Ще спрем нашето внимание на случая, когато G е група породена от елементи s и t такива, че s има ред $2^{n+2}, t^2 = \varepsilon_1$ и $ts = \varepsilon_2 s^{-1}t$, където $\varepsilon_1^2 = \varepsilon_2^2 = 1$. Тъй като $ts^4 = s^{-4}t$, можем да положим $s^4 = \zeta$, и да получим груповото разширение

$$1 \longrightarrow \mu_{2^n} \underset{\zeta \mapsto s^4}{\longrightarrow} G \underset{\substack{s \mapsto \sigma \\ t \mapsto \tau}}{\longrightarrow} D_8 \longrightarrow 1, \tag{5.8}$$

където сме отъждествили цикличната група $\langle s^4 \rangle$ с групата μ_{2^n} на корените на единицата от степен 2^n. Следователно имаме $s^4 = \zeta, t^2 = \varepsilon_1$ и $ts = \varepsilon_2 \zeta^{-1} s^3 t$, където $\varepsilon_1, \varepsilon_2 \in \{+1, -1\}$. Групата G има елемент от ред 2^{n+2}, откъдето G е изоморфна или на диедралната или на полудиедралната или на кватернионната група от ред 2^{n+3}. Нашият основен резултат в този параграф е следващата теорема, където пресмятаме препятствието на задачата за вложимост $(K/k, G, \mu_{2^n})$.

Теорема 5.2.2. ([Mi1, Theorem 3.2]) *За разрешимостта на задачата за вложимост* $(K/k, G, \mu_{2^n})$ *при* $n \geq 1$, *е необходимо да съществуват* $\alpha_1 \in k^*$ *и* $\beta_1 \in k$ *такива, че* $\alpha_1^2 + a\beta_1^2 = 2 - \zeta - \zeta^{-1}$. *В този случай препятствието е*

$$(-1, \varepsilon_1)(2 + \zeta + \zeta^{-1}, \alpha_1\beta_1)\left(a, \varepsilon_2\alpha_1\left(2\alpha_1 - \frac{\zeta - \zeta^{-1}}{i}\right)\right) \in \mathrm{Br}(k).$$

Доказателство: Ще приложим математическа индукция по n. При $n = 1$ имаме $\zeta = -1$, и нека $\alpha_1 = 2, \beta_1 = 0 : {\alpha_1}^2 + a{\beta_1}^2 = 2 - \zeta - \zeta^{-1} = 4$. Тогава получаваме препятствието $(-1, \varepsilon_1)(a, 2\varepsilon_2) \in \mathrm{Br}(k)$, което може още да бъде пресметното с помощта на теорема 5.2.1 за $b = -1$.

Нека сега задачата за вложимост е разрешима за $n-1$. В частност, съпътстващата задача $(K/k, D_{2^{n+2}}, \mu_{2^{n-1}})$ е разрешима (тук $\varepsilon_1 = \varepsilon_2 = 1$). Тогава ζ^2 е примитивен корен на единицата от степен 2^{n-1} и $2 - \zeta^2 - \zeta^{-2} = (\frac{\zeta - \zeta^{-1}}{i})^2$, така че можем да положим $\alpha_1 = \frac{\zeta - \zeta^{-1}}{i}$ и $\beta_1 = 0$. Така според индукционното допускане, препятствието на задачата $(K/k, D_{2^{n+2}}, \mu_{2^{n-1}})$ е

$$\begin{aligned}
&((\zeta + \zeta^{-1})^2, 0)\left(a, \frac{\zeta - \zeta^{-1}}{i}\left(2\frac{\zeta - \zeta^{-1}}{i} - \frac{\zeta^2 - \zeta^{-2}}{i}\right)\right) \\
&= \left(a, \frac{\zeta - \zeta^{-1}}{i}\left(2\frac{\zeta - \zeta^{-1}}{i} - \frac{\zeta - \zeta^{-1}}{i}(\zeta + \zeta^{-1})\right)\right) \\
&= \left(a, \left(\frac{\zeta - \zeta^{-1}}{i}\right)^2 (2 - \zeta - \zeta^{-1})\right) = (a, 2 - \zeta - \zeta^{-1}) \in \mathrm{Br}(k).
\end{aligned}$$

Нататък,

$$\begin{aligned}
&(2 - \zeta - \zeta^{-1})(2 + \zeta + \zeta^{-1}) = 4 - (\zeta + \zeta^{-1})^2 \\
&= 2 - \zeta^2 - \zeta^{-2} = \left(\frac{\zeta - \zeta^{-1}}{i}\right)^2 \in k^2
\end{aligned}$$

и

$$\begin{aligned}
&\left(1 + \frac{\zeta + \zeta^{-1}}{2}\right)^2 + \left(\frac{\zeta - \zeta^{-1}}{2i}\right)^2 = 1 + \zeta + \zeta^{-1} \\
&+ \frac{\zeta^2 + \zeta^{-2}}{4} + \frac{1}{2} - \frac{\zeta^2 + \zeta^{-2}}{4} + \frac{1}{2} = 2 + \zeta + \zeta^{-1}.
\end{aligned}$$

Следователно, $2 + \zeta + \zeta^{-1}$ и $2 - \zeta - \zeta^{-1}$ са едновременно суми на два квадрата в k. Така получаваме $(-a, 2 - \zeta - \zeta^{-1}) = 1 \in \mathrm{Br}(k)$ (или, еквивалентно, $(-a, 2 + \zeta + \zeta^{-1}) = 1 \in \mathrm{Br}(k)$) е необходимо условие за разрешимостта на задачата за вложимост $(K/k, G, \mu_{2^n})$ при $n > 1$.

Нека сега $\alpha_2 \in k^*$ и $\beta_2 \in k$ са такива, че $\alpha_2^2 + a\beta_2^2 = 2 + \zeta + \zeta^{-1}$. Връзката между α_2, β_2 и α_1, β_1, съответно, се задава чрез

$$\alpha_1^2 + a\beta_1^2 = 2 - \zeta - \zeta^{-1} = \frac{2 - \zeta^2 - \zeta^{-2}}{2 + \zeta + \zeta^{-1}} = (2 + \zeta + \zeta^{-1})\left(\frac{\zeta - \zeta^{-1}}{i(2 + \zeta + \zeta^{-1})}\right)^2.$$

Полагаме $\gamma = \frac{\zeta - \zeta^{-1}}{i(2 + \zeta + \zeta^{-1})} \in k, \alpha_2 = \frac{\alpha_1}{\gamma}, \beta_2 = \frac{\beta_1}{\gamma}$, и получаваме $\alpha_2^2 + a\beta_2^2 = 2 + \zeta + \zeta^{-1}$.

Нека Γ е алгебрата на кръстосаното произведение, която представя препятствието. Тогава Γ се поражда от два елемента u и v над K, така че $u^4 = \zeta, v^2 = \varepsilon_1, vu = \varepsilon_2 u^{-1}v = \varepsilon_2\zeta^{-1}u^3v, ux = \sigma(x)u$ и $vx = \tau(x)v$ за $x \in K$. Тогава Γ съдържа следните три кватернионни подалгебри:

$$\begin{aligned}
&Q_1 : i_1 = i, && j_1 = v\\
&Q_2 : i_2 = (1+\zeta^{-1})u^2, && j_2 = \sqrt[4]{a}(\alpha_2 + \beta_2\sqrt{a} + \varepsilon_2(1+\zeta^{-1})u^2)\\
&Q_3 : i_3 = \sqrt{a}, && j_3 = [-(1+i)(1+\zeta^{-1}) + \alpha_2(1+i) + (1-i)\beta_2\sqrt{a}]u\\
& && \quad + \varepsilon_2\zeta^{-1}[-(1-i)(1+\zeta) + \alpha_2(1-i) + (1+i)\beta_2\sqrt{a}]u^3.
\end{aligned}$$

Пресмятанията показват, че $i_1^2 = -1, j_1^2 = \varepsilon_1, i_2^2 = 2+\zeta+\zeta^{-1}, j_2^2 = 2\alpha_2\beta_2 a, i_3^2 = a$ и $j_3^2 = \varepsilon_2 4\alpha_2(2\alpha_2 - 2 - \zeta - \zeta^{-1})$. Също, $i_s j_s = -j_s i_s,\ 1 \le s \le 3$ и пораждащите на всяка алгебра комутират с пораждащите на останалите две алгебри. Ние сме принудени, обаче да пропуснем детайлите по тази обемиста проверка.

Така накрая получаваме:

$$\begin{aligned}
[\Gamma] &= [Q_1][Q_2][Q_3] = (-1,\varepsilon_1)(2+\zeta+\zeta^{-1}, \alpha_2\beta_2)(a, \varepsilon_2\alpha_2(2\alpha_2 - 2 - \zeta - \zeta^{-1}))\\
&= (-1,\varepsilon_1)(2+\zeta+\zeta^{-1}, \alpha_1\beta_1)\left(a, \varepsilon_2\frac{\alpha_1}{\gamma}\left(2\frac{\alpha_1}{\gamma} - 2 - \zeta - \zeta^{-1}\right)\right)\\
&= (-1,\varepsilon_1)(2+\zeta+\zeta^{-1}, \alpha_1\beta_1)\left(a, \varepsilon_2\alpha_1\left(2\alpha_1 - \frac{\zeta - \zeta^{-1}}{i}\right)\right) \in \mathrm{Br}(k).
\end{aligned}$$

□

Забележка 5.2.3. Ако се случи така, че за $n \ge 3$ да имаме $\alpha_1 = 0$ и $a\beta_1^2 = 2-\zeta-\zeta^{-1}$, то можем да положим $\alpha_1' = \frac{2}{3+\zeta+\zeta^{-1}}(\frac{\zeta-\zeta^{-1}}{i})$ и $\beta_1' = \frac{1+\zeta+\zeta^{-1}}{3+\zeta+\zeta^{-1}}\beta_1$, откъдето ${\alpha_1'}^2 + a{\beta_1'}^2 = 2-\zeta-\zeta^{-1}$. За $n = 2$ това работи добре, ако k има характеристика $\neq 3$ – тогава имаме $\alpha_1' = \frac{4}{3}$ и $\beta_1' = \frac{1}{3}\beta_1$. Ако k има характеристика 3, можем да положим $\alpha_1' = a - 1/a$ и $\beta_1' = (a + 1/a)\beta_1$, значи ${\alpha_1'}^2 + a{\beta_1'}^2 = 2$.

Забележка 5.2.4. За $n \ge 3$ имаме, че $\zeta^{2^s} + \zeta^{-2^s} \in k$ и $2 \in k^2$. От доказателството получаваме още, че $(a, 2 - \zeta^{2^s} - \zeta^{-2^s}) = 1 \in \mathrm{Br}(k),\ 0 \le s \le n-1$, е необходимо за разрешимостта на задачата за вложимост.

Да разгледаме сега груповото разширение

$$1 \longrightarrow C_{2^n} \longrightarrow G \underset{\substack{x\mapsto\sigma\\ y\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1, \tag{5.9}$$

където G се поражда от елемент x от ред 2^{n+2} и елемент y. Тогава имаме четири нееквивалентни групови разширения повдигащи елемент от ред 4 до елемент от ред 2^{n+2}:

(5.10а) $$1 \longrightarrow C_{2^n} \longrightarrow D_{2^{n+3}} \underset{\substack{x\mapsto\sigma\\ y\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1,$$

(5.10б) $$1 \longrightarrow C_{2^n} \longrightarrow Q_{2^{n+3}} \underset{\substack{x\mapsto\sigma\\ y\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1,$$

(5.10в) $$1 \longrightarrow C_{2^n} \longrightarrow SD_{2^{n+3}} \underset{\substack{x\mapsto\sigma\\ y\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1,$$

(5.10г) $$1 \longrightarrow C_{2^n} \longrightarrow SD_{2^{n+3}} \underset{\substack{x\mapsto\sigma\\ yx\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1.$$

Да предположим отново, че $\zeta+\zeta^{-1} \in k$ и $i(\zeta-\zeta^{-1}) \in k$, така че положението на ζ в K/k се определя от положението на i. Да припомним, че $K/k = k(\sqrt{r(\alpha+\beta\sqrt{a})}, \sqrt{b})/k$, където $r \in k^*$ и $\alpha, \beta \in k$ са такива, че $\alpha^2 - a\beta^2 = ab$.

Ще пресметнем препятствията на задачите за вложимост съответстващи на четирите групови разширения (5.10а)-(5.10г) във всичките пет възможни случая.

1. $i \in k$. Тогава $\zeta \in k$, значи $\sigma\zeta = \tau\zeta = \zeta, \chi^\sigma = \chi$ и $\chi^\tau = \chi^{-1}$. Следователно $F_\chi = \langle\sigma\rangle$ и $K_\chi = k(\sqrt{b})$. Според теорема 1.6.1 задачите за вложимост съответстващи на груповите разширения (5.10а)-(5.10г) са разрешими $\Leftrightarrow$ задачите за вложимост зададени с $K/k(\sqrt{b})$ и (5.3), съответно с K/k и

   $$1 \longrightarrow C_2 \hookrightarrow D_{16} \cong G/C_{2^{n-1}} \longrightarrow D_8 \longrightarrow 1$$

   са разрешими. Тук $K/k(\sqrt{b}) = k(\sqrt[4]{a'})/k(\sqrt{b})$ за $a' = [2r(\beta - i\sqrt{b})]^2 a$. Според теорема 5.2.1 и лема 5.1.1, препятствията за всяка задача за вложимост са: $(ab, 2)(-b, r\alpha) \in \mathrm{Br}(k)$ и $(a, \alpha')(\zeta, \alpha'\beta') \in \mathrm{Br}(k(\sqrt{b}))$, където трябва да имаме $\alpha' \in k(\sqrt{b})^*, \beta' \in k(\sqrt{b})$, така че $\alpha'^2 - a\beta'^2 = \zeta$.

2. $a = -1$. Тогава $\sigma\zeta = \zeta^{-1}, \tau\zeta = \zeta, \chi^\sigma = \chi^\tau = \chi^{-1}$. Следователно, $F_\chi = \langle\sigma^2, \tau\sigma\rangle \cong C_2 \times C_2$ и $K_\chi = k(i\sqrt{b})$. Задачата за вложимост $(K/k, G, C_{2^n})$ е разрешима $\Leftrightarrow$ задачите $(K/k(i\sqrt{b}), \pi^{-1}C_2^2, \mu_{2^n})$ и $(K/k, D_{16}, \mu_2)$ са разрешими. Тогава трябва

да имаме $(-b, 2\alpha r) = 1 \in \mathrm{Br}(k)$ и препятствията на всяка задача се пресмятат както следва:

(5.10а), $\pi^{-1}C_2^2 \cong D_{2^{n+2}}$: задачата $(k(\sqrt{a'}, i)/k(i\sqrt{b}), D_{2^{n+2}}, \mu_{2^n})$ за $a' = (\varphi + \psi)^2 = 2r(\alpha + i\sqrt{b})$ е разрешима $\Leftrightarrow$ задачата $(k(\sqrt[4]{a''}, i)/k(i\sqrt{b}), D_{2^{n+2}}, \mu_{2^{n-1}})$ е разрешима за някое $a'' = r'^2 a', r' \in k(i\sqrt{b})$. Така препятствието на задачата $(K/k, D_{2^{n+3}}, C_{2^n})$ е $(a'', 2 - \zeta - \zeta^{-1}) = (2r(\alpha + i\sqrt{b}), 2 - \zeta - \zeta^{-1}) \in \mathrm{Br}(k(i\sqrt{b}))$.

(5.10б), $\pi^{-1}C_2^2 \cong Q_{2^{n+2}}$: задачата $(k(\sqrt{a'}, i)/k(i\sqrt{b}), Q_{2^{n+2}}, \mu_{2^n})$ за $a' = 2r(\alpha + i\sqrt{b})$ е разрешима $\Leftrightarrow$ задачата $(k(\sqrt[4]{a''}, i)/\ k(i\sqrt{b}), Q_{2^{n+2}}, \mu_{2^{n-1}})$ е разрешима за някое $a'' = r'^2 a', r' \in k(i\sqrt{b})$. Така препятствието на задачата $(K/k, Q_{2^{n+3}}, C_{2^n})$ е $(-1, -1)(2r(\alpha + i\sqrt{b}), 2 - \zeta - \zeta^{-1}) \in \mathrm{Br}(k(i\sqrt{b}))$.

(5.10в), $\pi^{-1}C_2^2 \cong Q_{2^{n+2}}$: препятствието на задачата $(K/k, SD_{2^{n+3}}, C_{2^n})$ е $(-1, -1)$ $(2r(\alpha + i\sqrt{b}), 2 - \zeta - \zeta^{-1}) \in \mathrm{Br}(k(i\sqrt{b}))$.

(5.10г), $\pi^{-1}C_2^2 \cong D_{2^{n+2}}$: препятствието на задачата $(K/k, SD_{2^{n+3}}, C_{2^n})$ е $(2r(\alpha + i\sqrt{b}), 2 - \zeta - \zeta^{-1}) \in \mathrm{Br}(k(i\sqrt{b}))$.

3. $b = -1$. Този случай е разгледан в теорема 5.2.2. Можем да считаме, че $r = \beta = 1$ и $\alpha = 0$. Трябва да съществуват $\alpha_1 \in k^*, \beta_1 \in k$ такива, че $\alpha_1^2 + a\beta_1^2 = 2 - \zeta - \zeta^{-1}$. Тогава препятствията са:

   (5.10а): $(2 + \zeta + \zeta^{-1}, \alpha_1\beta_1)\left(a, \alpha_1\left(2\alpha_1 - \frac{\zeta - \zeta^{-1}}{i}\right)\right) \in \mathrm{Br}(k)$.

   (5.10б): $(-1, -1)(2 + \zeta + \zeta^{-1}, \alpha_1\beta_1)\left(a, \alpha_1\left(2\alpha_1 - \frac{\zeta - \zeta^{-1}}{i}\right)\right) \in \mathrm{Br}(k)$.

   (5.10в): $(2 + \zeta + \zeta^{-1}, \alpha_1\beta_1)\left(a, -\alpha_1\left(2\alpha_1 - \frac{\zeta - \zeta^{-1}}{i}\right)\right) \in \mathrm{Br}(k)$.

   (5.10г): $(-1, -1)(2 + \zeta + \zeta^{-1}, \alpha_1\beta_1)\left(a, -\alpha_1\left(2\alpha_1 - \frac{\zeta - \zeta^{-1}}{i}\right)\right) \in \mathrm{Br}(k)$.

4. $ab = -1$. Тогава $\sigma\zeta = \zeta^{-1}, \tau\zeta = \zeta^{-1}, \chi^\sigma = \chi^{-1}$ и $\chi^\tau = \chi$. Следователно, $F_\chi = \langle \sigma^2, \tau \rangle \cong C_2 \times C_2$ и $K_\chi = k(\sqrt{a})$. Задачата за вложимост $(K/k, G, C_{2^n})$ е разрешима $\Leftrightarrow$ задачите $(K/k(\sqrt{a}), \pi^{-1}C_2^2, \mu_{2^n})$ и $(K/k, D_{16}, \mu_2)$ са разрешими. Тогава трябва да имаме $(-b, \alpha r) = 1 \in \mathrm{Br}(k)$ и препятствията на всяка задача се пресмятат както преди:

   (5.10а), $\pi^{-1}C_2^2 \cong D_{2^{n+2}}$: препятствието на задачата $(K/k, D_{2^{n+3}}, C_{2^n})$ е $(r(\alpha + \beta\sqrt{a}), 2 - \zeta - \zeta^{-1}) \in \mathrm{Br}(k(\sqrt{a}))$.

   (5.10б), $\pi^{-1}C_2^2 \cong Q_{2^{n+2}}$: препятствието на задачата $(K/k, Q_{2^{n+3}}, C_{2^n})$ е $(-1, -1)$ $(r(\alpha + \beta\sqrt{a}), 2 - \zeta - \zeta^{-1}) \in \mathrm{Br}((k(\sqrt{a}))$.

(5.10в), $\pi^{-1}C_2^2 \cong D_{2^{n+2}}$: препятствието на задачата $(K/k,\ D_{2^{n+3}}, C_{2^n})$ е $(r(\alpha + \beta\sqrt{a}), 2 - \zeta - \zeta^{-1}) \in \mathrm{Br}(k(\sqrt{a}))$.

(5.10г), $\pi^{-1}C_2^2 \cong Q_{2^{n+2}}$: препятствието на задачата $(K/k,\ D_{2^{n+3}}, C_{2^n})$ е $(-1,-1)$ $(r(\alpha + \beta\sqrt{a}), 2 - \zeta - \zeta^{-1}) \in \mathrm{Br}(k(\sqrt{a}))$.

5. a, b и -1 са квадратично независими. Нека κ поражда $\mathrm{Gal}(K(i)/K)$, и да отъждествим $\mathrm{Gal}(K/k)$ с $\mathrm{Gal}(K(i)/k(i))$. Тогава задачата $(K/k, G, C_{2^n})$ е разрешима $\Leftrightarrow$ задачата за вложимост зададена с $K(i)/k(i)$ и

$$1 \longrightarrow C_{2^n} \longrightarrow G \times C_2 \longrightarrow D_8 \times C_2 \longrightarrow 1$$

е разрешима. Тук $(D_8 \times C_2)_\chi = \langle \sigma, \tau\kappa \rangle \cong D_8$ и $K(i)_\chi = k(i\sqrt{b})$. Тогава можем да образуваме съпътстващата задача от втори тип, зададена с $K(i)/k(i\sqrt{b})$ и

$$1 \longrightarrow \mu_{2^n} \longrightarrow G \underset{\substack{y \mapsto \tau\kappa}}{\overset{x \mapsto \sigma}{\longrightarrow}} D_8 \longrightarrow 1.$$

Трябва да имаме $(ab, 2)(-b, \alpha r) = 1 \in \mathrm{Br}(k), \alpha_1 \in k(i\sqrt{b})^*, \beta_1 \in k(i\sqrt{b})$, така че $\alpha_1^2 + a'\beta_1^2 = 2 - \zeta - \zeta^{-1}$, и $K(i) = k(i\sqrt{b})(\sqrt[4]{a'}, i)$, където $a' = [2r(\alpha + i\sqrt{b})]^2 a$. Тогава препятствията са:

(5.10а): $(2 + \zeta + \zeta^{-1}, \alpha_1\beta_1)\left(a, \alpha_1\left(2\alpha_1 - \frac{\zeta - \zeta^{-1}}{i}\right)\right) \in \mathrm{Br}(k(i\sqrt{b}))$.

(5.10б): $(-1,-1)(2 + \zeta + \zeta^{-1}, \alpha_1\beta_1)\left(a, \alpha_1\left(2\alpha_1 - \frac{\zeta - \zeta^{-1}}{i}\right)\right) \in \mathrm{Br}(k(i\sqrt{b}))$.

(5.10в): $(2 + \zeta + \zeta^{-1}, \alpha_1\beta_1)\left(a, -\alpha_1\left(2\alpha_1 - \frac{\zeta - \zeta^{-1}}{i}\right)\right) \in \mathrm{Br}(k(i\sqrt{b}))$.

(5.10г): $(-1,-1)(2 + \zeta + \zeta^{-1}, \alpha_1\beta_1)\left(a, -\alpha_1\left(2\alpha_1 - \frac{\zeta - \zeta^{-1}}{i}\right)\right) \in \mathrm{Br}(k(i\sqrt{b}))$.

Нека сега $k(\sqrt{a}, \sqrt{b})/k$ е C_2^2 разширение, породено от елементи ρ_1 и ρ_2 такива, че

$$\rho_1 : \sqrt{a} \mapsto -\sqrt{a}, \sqrt{b} \mapsto \sqrt{b};\ \rho_2 : \sqrt{a} \mapsto \sqrt{a}, \sqrt{b} \mapsto -\sqrt{b}.$$

Да разгледаме задачата за вложимост зададена с $k(\sqrt{a}, \sqrt{b})/k$ и

$$1 \longrightarrow C_{2^{n+1}} \longrightarrow G \underset{\substack{y \mapsto \rho_2}}{\overset{x \mapsto \rho_1}{\longrightarrow}} C_2^2 \longrightarrow 1, \tag{5.11}$$

където групата G се поражда от елементи x и y такива, че x има ред $2^{n+2}, y^2 = x^{2^{n+1}}$ или $y^2 = 1$, $yx = x^{-1}y$ или $yx = x^{2^{n+1}-1}y$. Следователно G е изоморфна на някоя

от групите $D_{2^{n+3}}, Q_{2^{n+3}}$ или $SD_{2^{n+3}}$. Очевидно, тази задача е разрешима тогава и само тогава, когато $k(\sqrt{a},\sqrt{b})/k$ може да се вложи в D_8 разширение K/k и задачата $(K/k/k, G, C_{2^n})$ е разрешима.

Отново имаме, че груповото разширение (5.11) поражда четири групови разширения:

(5.12а) $$1 \longrightarrow C_{2^{n+1}} \longrightarrow D_{2^{n+3}} \underset{\substack{x\mapsto\rho_1\\ y\mapsto\rho_2}}{\longrightarrow} C_2^2 \longrightarrow 1,$$

(5.12б) $$1 \longrightarrow C_{2^{n+1}} \longrightarrow Q_{2^{n+3}} \underset{\substack{x\mapsto\rho_1\\ y\mapsto\rho_2}}{\longrightarrow} C_2^2 \longrightarrow 1,$$

(5.12в) $$1 \longrightarrow C_{2^{n+1}} \longrightarrow SD_{2^{n+3}} \underset{\substack{x\mapsto\rho_1\\ y\mapsto\rho_2}}{\longrightarrow} C_2^2 \longrightarrow 1,$$

(5.12г) $$1 \longrightarrow C_{2^{n+1}} \longrightarrow SD_{2^{n+3}} \underset{\substack{x\mapsto\rho_1\\ yx\mapsto\rho_2}}{\longrightarrow} C_2^2 \longrightarrow 1.$$

Ще напишем препятствията на Брауеровите задачи за $b = -1$, съответстващи на разширенията (5.12а)-(5.12г).

Нека ζ е примитивен 2^{n+1}-ти корен на единицата $(n > 1)$, за който $\zeta + \zeta^{-1} \in k$ и $i(\zeta - \zeta^{-1}) \in k$, така че можем да положим $\alpha_1 = \frac{\zeta-\zeta^{-1}}{i}, \beta_1 = 0 : \alpha_1^2 + a\beta_1^2 = (\frac{\zeta-\zeta^{-1}}{i})^2 = 2 - \zeta^2 - \zeta^{-2}$. Препятствията тогава са:

(5.12а): $(a, 2 - \zeta - \zeta^{-1}) \in \mathrm{Br}(k)$.

(5.12б): $(-1,-1)(a, 2 - \zeta - \zeta^{-1}) \in \mathrm{Br}(k)$.

(5.12в): $(a, -2 + \zeta + \zeta^{-1}) \in \mathrm{Br}(k)$.

(5.12г): $(-1,-1)(a, -2 + \zeta + \zeta^{-1}) \in \mathrm{Br}(k)$.

Ще продължим с изследване на задачата за вложимост зададена с $k(\sqrt{b})/k$ и

(5.13) $$1 \longrightarrow C_{2^{n+2}} \longrightarrow G \longrightarrow C_2 \longrightarrow 1,$$

където групата G отново е изоморфна на някоя от групите $D_{2^{n+3}}, Q_{2^{n+3}}$ или $SD_{2^{n+3}}$. Очевидно, тази задача е разрешима тогава и само тогава, когато съществува $a \in k$ такова, че a и b са квадратично независими, и задачата зададена с $k(\sqrt{a},\sqrt{b})/k$ и (5.11) е разрешима.

Нека ζ е примитивен 2^{n+2}-ти корен на единицата $(n > 1)$, така че $\zeta + \zeta^{-1} \in k$ и $i(\zeta - \zeta^{-1}) \in k$, и нека $|k/k^2| \geq 4$. Можем отново да намерим препятствията на Брауеровите задачи за $b = -1$.

(5.12а): Имаме $(a, 2-\zeta^2-\zeta^{-2}) = 1 \in \mathrm{Br}(k)$ за всяко $a \in k$ такова, че a и -1 са квадратично независими. Следователно, нямаме препятствие и е лесно да се провери, че $k(\sqrt[2^{n+2}]{a}, i)/k$ е решение на задачата за вложимост $(k(i)/k, D_{2^{n+3}}, \mu_{2^{n+2}})$.

(5.12б): Препятствието е $(-1,-1) \in \mathrm{Br}(k)$.

(5.12в): $(a,-1) \in \mathrm{Br}(k)$.

(5.12г): $(-a,-1) \in \mathrm{Br}(k)$.

По този начин, задачата за вложимост $(k(i)/k, D_{2^{n+3}}, \mu_{2^{n+2}})$ е разрешима $\Leftrightarrow$ $|k/k^2| \geq 4$; $(k(i)/k, Q_{2^{n+3}}, \mu_{2^{n+2}})$ е разрешима $\Leftrightarrow$ $|k/k^2| \geq 4$ и $(-1,-1) \in \mathrm{Br}(k)$; и $(k(i)/k, SD_{2^{n+3}}, \mu_{2^{n+2}})$ е разрешима $\Leftrightarrow |k/k^2| \geq 4$ и k не е квадратично затворено.

Накрая, за $\zeta = i$ можем да разгледаме груповите разширения

$$1 \longrightarrow C_4 \longrightarrow G \underset{\substack{x\mapsto\sigma \\ y\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1, \tag{5.14}$$

където G е изомофрна на някоя от групите D_{32}, SD_{32} или Q_{32}. Тогава препятствието на Брауеровата задача е

$$(-1, \varepsilon_1)(2, \alpha_1\beta_1)(a, \varepsilon_2\alpha_1(\alpha_1-1)) \in \mathrm{Br}(k),$$

където $\alpha_1 \in k^*, \beta_1 \in k$ са такива, че $\alpha_1^2 + a\beta_1^2 = 2$. Това потвърждава резултата на Ледет [Le2].

Груповото разширение (5.14) отново поражда четири разширения:

$$1 \longrightarrow C_4 \longrightarrow D_{32} \underset{\substack{x\mapsto\sigma \\ y\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1, \tag{5.15а}$$

$$1 \longrightarrow C_4 \longrightarrow Q_{32} \underset{\substack{x\mapsto\sigma \\ y\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1, \tag{5.15б}$$

$$1 \longrightarrow C_4 \longrightarrow SD_{32} \underset{\substack{x\mapsto\sigma \\ y\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1, \tag{5.15в}$$

$$1 \longrightarrow C_4 \longrightarrow SD_{32} \underset{\substack{x\mapsto\sigma \\ yx\mapsto\tau}}{\longrightarrow} D_8 \longrightarrow 1. \tag{5.15г}$$

Сега ще дадем някоко примера на Брауерови задачи съответстващи на груповите разширения (5.15а)-(5.15г) над полето на рационалните числа $\mathbb{Q}$.

Пример 5.2.5. Да разгледаме задачата за вложимост $(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}, G, \mu_4)$. Полагаме $\alpha_1 = \frac{4}{3}, \beta_1 = \frac{1}{3} : \alpha_1^2 + 2\beta_1^2 = 2$, така че препятствието е $(-1, \varepsilon_1)(2, \frac{4}{9})(2, \varepsilon_2 \frac{4}{9}) = (-1, \varepsilon_1) \in \mathrm{Br}(\mathbb{Q})$. Следователно, задачите за вложимост зададени с (5.15а) и (5.15в) са разрешими, но задачите заедени с (5.15б) и (5.15г) не са. □

Пример 5.2.6. Да разгледаме задачата за вложимост $(\mathbb{Q}(\sqrt[4]{7}, i)/\mathbb{Q}, G, \mu_4)$. Полагаме $\alpha_1 = \beta_1 = \frac{1}{2} : \alpha_1^2 + 7\beta_1^2 = 2$, така че препятствието е $(-1, \varepsilon_1)(2, \frac{1}{4})(7, -\varepsilon_2 \frac{1}{4}) = (-1, \varepsilon_1)(7, -\varepsilon_2)$. Препятствията на останалите задачи за вложимост са:

(5.15а): $(7, -1) \neq 1 \in \mathrm{Br}(\mathbb{Q})$.

(5.15б): $(-7, -1) \neq 1 \in \mathrm{Br}(\mathbb{Q})$.

(5.15в): $(-1, 1)(7, 1) = 1 \in \mathrm{Br}(\mathbb{Q})$.

(5.15г): $(-1, -1) \neq 1 \in \mathrm{Br}(\mathbb{Q})$.

Следователно, задачите зададени с (5.15а), (5.15б) и (5.15г) не са разрешими, но задачата зададена с (5.15в) е разрешима. □

Разбира се, за произволно рационално число a е трудно да се определи дали произведението на тези три кватернионни алгебри се разпада в $\mathrm{Br}(\mathbb{Q})$. Пресмятания с помощта на компютър ни дават следващият пример, където задачата за вложимост зададена с (5.15а) е разрешима, но останалите задачи не са.

Пример 5.2.7. Да разгледаме задачата за вложимост $(\mathbb{Q}(\sqrt[4]{-27887}, i)/\mathbb{Q}, G, \mu_4)$. Полагаме $\alpha_1 = 167, \beta_1 = 1 : \alpha_1^2 - 27887\beta_1^2 = 2$. Както знаем от [Mi10], можем да свържем разпадането на кватернионните алгебри в $\mathrm{Br}(\mathbb{Q})$ със символите на Льожандър. Тъй като $\left(\frac{2}{167}\right) = 1$, получаваме $(\alpha_1\beta_1, 2) = (167, 2) = 1 \in \mathrm{Br}(\mathbb{Q})$. Имаме $-27887 = -79 \cdot 353$ и $\alpha_1(\alpha_1 - 1) = 2 \cdot 83 \cdot 167$, така че препятствието е $(-1, \varepsilon_1)(-79 \cdot 353, \varepsilon_2 2 \cdot 83 \cdot 167) \in \mathrm{Br}(\mathbb{Q})$. Да забележим, че $167 \equiv 7\ (8), 79 \equiv 7\ (8)$ и $353 \equiv 1\ (8)$. Сега, $\left(\frac{2}{79}\right) = \left(\frac{2}{353}\right) = 1$, откъдето $(-79 \cdot 353, 2) = 1$; $\left(\frac{83}{79}\right) = \left(\frac{167}{79}\right) = 1$ и $\left(\frac{-79}{83}\right) = \left(\frac{-79}{167}\right) = 1$, откъдето $(-79, 83 \cdot 167) = 1$. Накрая, $\left(\frac{167}{353}\right) = \left(\frac{353}{167}\right) = 1$, откъдето $(353, 167) = 1$; $\left(\frac{83}{353}\right) = \left(\frac{353}{83}\right) = 1$, откъдето $(353, 83) = 1$.

По този начин, ако $\varepsilon_2 = 1$, то препятствието е $(-1, \varepsilon_1)(-79 \cdot 353, 2 \cdot 83 \cdot 167) = (-1, \varepsilon_1)(353,\ 83 \cdot 167) = (-1, \varepsilon_1)(353, 83) = (-1, \varepsilon_1) = 1 \in \mathrm{Br}(\mathbb{Q}) \Leftrightarrow \varepsilon_1 = 1$. Ако $\varepsilon_2 = -1$ и предположим, че $(-1, \varepsilon_1)(-79 \cdot 353, -2 \cdot 83 \cdot 167) = 1 \in \mathrm{Br}(\mathbb{Q})$, то в частност, $79 \cdot 353$ е сума на три целочислени квадрата, което е невъзможно, понеже $79 \cdot 353 \equiv 7\ (8)$. Следователно, задачата $(\mathbb{Q}(\sqrt[4]{-27887}, i)/\mathbb{Q}, D_{32}, \mu_4)$ е разрешима, но останалите задачи не са. □

5.3 Препятствия за реализирането на модулярната 2-група

Да припомним, че модулярната група от ред 2^n $(n \geq 4)$ има следното представяне:

$$M_{2^n} = \langle x, y \mid x^{2^{n-1}} = y^2 = 1, yx = x^{2^{n-2}+1}y \rangle.$$

Нека $K = k(\varphi)$ и нека $L/k = k(\varphi, \sqrt{b})/k$ е $C_4 \times C_2$ разширение, където $\varphi = \sqrt{r(a+\sqrt{a})}, \psi = \sqrt{r(a-\sqrt{a})}$ и $a = 1 + c^2;\ a, b, c, r \in k^*$. Нека $\mathrm{Gal}(L/k)$ се поражда от елементи σ и τ такива, че $\sigma : \varphi \mapsto \psi, \sqrt{b} \mapsto \sqrt{b}$; $\tau : \varphi \mapsto \varphi, \sqrt{b} \mapsto -\sqrt{b}$.

Лема 5.3.1. *Препятствието на задачата за вложимост $(L/k, M_{16}, C_2)$ съответстваща на груповото разширение*

$$1 \longrightarrow C_2 = \langle x^4 \rangle \hookrightarrow M_{16} \longrightarrow C_4 \times C_2 \longrightarrow 1 \tag{5.16}$$

е $(a, 2b)(-1, r) \in \mathrm{Br}(k)$.

Доказателство: Препятствието се представя от цикличната алгебра $\Gamma = (L, C_4 \times C_2, -1) = L[u, v]$, където $u^4 = -1, v^2 = 1, vu = -uv, ux = \sigma(x)u$ и $vx = \tau(x)v,\ x \in L$. Имаме следните три кватернионни подалгебри в Γ:

$$\begin{aligned} Q_1 &: i_1 = \sqrt{a}, \quad j_1 = u + u^3, \\ Q_2 &: i_2 = u^2, \quad\ \ j_2 = (\varphi + \psi u^2)\sqrt{a}, \\ Q_3 &: i_3 = \sqrt{b}, \quad j_3 = \sqrt{a}v. \end{aligned}$$

Не е трудно да се провери, че Q_1, Q_2 и Q_3 се централизират една друга, значи $[\Gamma] = [Q_1][Q_2][Q_3] = (a, -2)(-1, 2ra^2)(b, a) = (a, 2b)(-1, r) \in \mathrm{Br}(k)$. □

В термините на нормени изображения, задачата за вложимост $(L/k, M_{16}, C_2)$ е разрешима тогава и само тогава, когато $-1/b^2 \in N_{K/k}(K^*)$ (виж [Le1, Example 3.3]).

Както досега, ще разгледаме задачи за вложимост с циклично 2-ядро. За следващата лема ще въведем някои означения: Нека $\zeta \in k$ е примитивен 2^n-ти корен на единицата $(n \geq 2)$, нека $K = k(\sqrt[4]{a})$, и нека $L/k = k(\sqrt[4]{a}, \sqrt{b})/k$ е $C_4 \times C_2$ разширение, където C_4 се поражда от σ, а C_2 се поражда от τ, така че $\sigma\sqrt[4]{a} = i\sqrt[4]{a},\ \sigma\sqrt{b} = \sqrt{b};\ \tau\sqrt[4]{a} = \sqrt[4]{a},\ \tau\sqrt{b} = -\sqrt{b}$.

Лема 5.3.2. ([Mi2, Lemma 3.2]) *За да бъде разрешима задачата за вложимост $(L/k, M_{2^{n+3}}, \mu_{2^n})$, съответстваща на груповото разширение*

$$1 \longrightarrow \mu_{2^n} = \langle x^4 \rangle \hookrightarrow M_{2^{n+3}} \longrightarrow C_4 \times C_2 \longrightarrow 1 \tag{5.17}$$

е необходимо да съществуват $\alpha \in k^*, \beta \in k$ *такива, че* $\alpha^2 - a\beta^2 = \zeta$. *В този случай препятствието е* $(a, \alpha b)(\zeta, \alpha\beta) \in \mathrm{Br}(k)$.

Доказателство: Ако задачата за вложимост, съответстваща на (5.17) е разрешима, то съпътстващата задача зададена с L/k и

$$1 \longrightarrow \mu_{2^{n-1}} \hookrightarrow C_{2^{n+1}} \times C_2 \longrightarrow C_4 \times C_2 \longrightarrow 1$$

също е разрешима. Тъй като ζ^2 е примитивен корен на единицата от степен 2^{n-1}, препятствието е $(a, \zeta) \in \mathrm{Br}(k)$, според теорема 5.1.1. По този начин трябва да имаме $\alpha^2 - a\beta^2 = \zeta$ за някои $\alpha \in k^*$ и $\beta \in k$.

Препятствието на първоначалната задача се представя от алгебрата $\Gamma = (L, C_4 \times C_2, \zeta) = k[\sqrt[4]{a}, \sqrt{b}, u, v]$, където $u^4 = \zeta, v^2 = 1, vu = -uv, ux = \sigma(x)u$ и $vx = \tau(x)v$, $\forall x \in L$. Следните три кватернионни алгебри се съдържат в Γ:

$$\begin{aligned} Q_1 : i_1 &= \sqrt{a}, \quad j_1 = (\alpha + \beta\sqrt{a} + iu^2)u, \\ Q_2 : i_2 &= u^2, \quad\ \ j_2 = \sqrt[4]{a}(\alpha + i\beta\sqrt{a} + u^2) \\ Q_3 : i_3 &= \sqrt{b}, \quad j_3 = \sqrt{a}v. \end{aligned}$$

Тъй като Q_1, Q_2 и Q_3 се централизират взаимно, получаваме

$$[\Gamma] = [Q_1][Q_2][Q_3] = (a, 2\alpha i\zeta)(\zeta, 2\alpha\beta ia)(b, a) = (a, \alpha b)(\zeta, \alpha\beta) \in \mathrm{Br}(k).$$

Да отбележим, че новополученото препятствие се съгласува при $n = 1$ с лема 5.3.1: полагаме $i \in k, \alpha = i, \beta = 0, \zeta = -1$ и получаваме $(a, \alpha b)(\zeta, \alpha\beta) = (a, ib) = (a, 2b) \in \mathrm{Br}(k)$. □

Нека сега $\zeta + \zeta^{-1}$ и $i(\zeta - \zeta^{-1})$ са в k. Ще разгледаме пет случая, според местоположението на i в $L(i)$. Елементите σ и τ действат тривиално на пораждащия на ядрото x^4, така че можем да приложим следствие 1.6.2.

1. $i \in k$. Според лема 5.3.2, препятствието на задачата за вложимост зададена с $L/k = k(\sqrt[4]{a}, \sqrt{b})/k$ и (5.17) е $(a, \alpha b)(\zeta, \alpha\beta) \in \mathrm{Br}(k)$, където $\alpha^2 - a\beta^2 = \zeta$, за някои $\alpha \in k^*$ и $\beta \in k$.

2. $a = -1$. Трябва да имаме $-1 = u^2 + v^2$ за някои $u, v \in k^*$ и $L = k(\sqrt{a'}, \sqrt{b})$, където $a' = r(1 - iu),\ r \in k^*$. Тогава задачата $(L/k, M_{2^{n+3}}, C_{2^n})$ съответстваща на

(5.18) $$1 \longrightarrow C_{2^n} \hookrightarrow M_{2^{n+3}} \longrightarrow C_4 \times C_2 \longrightarrow 1$$

е разрешима тогава и само тогава, когато задачите $(L/k(i), C_{2^{n+1}} \times C_2, \mu_{2^n})$ и $(L/k, C_8 \times C_2, C_2)$ са разрешими. Препятствията са: $(r(1-iu), \zeta) \in \mathrm{Br}(k(i))$ и $(-1, r) \in \mathrm{Br}(k)$.

3. $b = -1$. Можем да запишем $L/k = k(\sqrt{r(a+\sqrt{a})}, i)/k$ и $L/k(i) = k(\sqrt[4]{a'}, i)/k(i)$, където $a' = [2r(1-ic)]^2 a$. Тогава задачата зададена с L/k и (5.18) е разрешима тогава и само тогава, когато задачите $(L/k(i), C_{2^{n+2}}, \mu_{2^n})$ и $(L/k, C_8 \times C_2, C_2)$ са разрешими. Препятствията са: $(a, \alpha')(\zeta, \alpha'\beta') \in \mathrm{Br}(k(i))$ и $(a, 2)(-1, r) \in \mathrm{Br}(k)$, където $\alpha'^2 - a'\beta'^2 = \zeta$ за някои $\alpha' \in k(i)^*$ и $\beta' \in k(i)$.

4. $ab = -1$. Можем отново да запишем $L/k = k(\sqrt{r(a+\sqrt{a})}, i)/k$ и $L/k(i) = k(\sqrt[4]{a'}, i)/k(i)$, където $a' = [2r(1-ic)]^2 a$. Не е трудно да се види, че препятствията са същите както в предишния случай.

5. a, b и -1 са квадратично независими. Според следствие 1.6.3 задачата зададена с L/k и (5.18) е разрешима тогава и само тогава, когато задачите $(L(i)/k(i), M_{2^{n+3}}, C_{2^n})$ и $(L/k, C_8 \times C_2, C_2)$ са разрешими. Препятствията са: $(a, \alpha' b)(\zeta, \alpha'\beta') \in \mathrm{Br}(k(i))$ и $(a, 2)(-1, r) \in \mathrm{Br}(k)$, където $\alpha'^2 - a'\beta'^2 = \zeta$ за някои $\alpha' \in k(i)^*$ и $\beta' \in k(i)$. Тук означаваме $L(i)/k(i) = k(\sqrt[4]{a'}, i)/k(i)$, където $a' = [2r(1-ic)]^2 a$ и $K = k(\varphi)$.

Можем да обобщим препятствията на задачите за вложимост, съответстващи на (5.18) в следната

Теорема 5.3.3. ([Mi2, Theorem 3.3]) *Нека ζ е примитивен 2^n-ти корен на единицата такъв, че $\zeta + \zeta^{-1} \in k$ и $(\zeta - \zeta^{-1})/i \in k$. Нека $L/k = k(\sqrt{r(a+\sqrt{a})}, \sqrt{b})/k$ е $C_4 \times C_2$ разширение за $a = 1 + c^2$, $b, r \in k^*$. Тогава задачата за вложимост зададена с L/k и груповото разширение* (5.18) *има следните препятствия за $n \geq 2$:*

1. *$i \in k$ (т.е., $\zeta \in k$) : $(a, \alpha b)(\zeta, r\alpha\beta) \in \mathrm{Br}(k)$, където трябва да съществуват $\alpha \in k^*, \beta \in k$ такива, че $\alpha^2 - a\beta^2 = \zeta$.*

2. *$a = -1$: $(-1, r) \in \mathrm{Br}(k)$ и $(r(1-iu), \zeta) \in \mathrm{Br}(k(i))$, където трябва да имаме $-1 = u^2 + v^2$ за някои $u, v \in k$ и $L = k(\sqrt{r(1-iu)}, \sqrt{b})$.*

3. *$b = -1$ или $ab = -1$: $(a, 2)(-1, r) \in \mathrm{Br}(k)$ и $(a, \alpha)(\zeta, r(1-ic)\alpha\beta) \in \mathrm{Br}(k(i))$, където трябва да съществуват $\alpha \in k(i)^*, \beta \in k(i)$ такива, че $\alpha^2 - a\beta^2 = \zeta$.*

4. a, b *и* -1 *са квадратично независими:* $(a,2)(-1,r) \in \mathrm{Br}(k)$ *и* $(a,\alpha b)(\zeta, r(1-ic)\alpha\beta) \in \mathrm{Br}(k(i))$*, където трябва да съществуват* $\alpha \in k(i)^*, \beta \in k(i)$ *такива, че* $\alpha^2 - a\beta^2 = \zeta$*.*

Пример 5.3.4. Нека $\zeta \in k$ е примитивен корен на единицата от степен 2^{n+1}. Тогава можем да положим $\alpha = \zeta, \beta = 0 \ : \ \alpha^2 - a\beta^2 = \zeta^2$, така че препятствието на задачата за вложимост съответстваща на (5.18) е $(a,\alpha b)(\zeta^2, r\alpha\beta) = (a,\zeta b) \in \mathrm{Br}(k)$. Ако $b = \zeta \notin k^2$, то задачата за вложимост съответстваща на (5.18) е разрешима и $k(\sqrt[2^{n+2}]{a}, \sqrt{\zeta})$ е едно нейно решение. □

Частният случай $\sqrt{\zeta} \in k$ ще разгледаме в следната

Теорема 5.3.5. ([Mi2, Proposition 3.4]) *Нека* $\zeta = \zeta_{2^{n+2}} \in k$ *е примитивен корен на единицата от степен* 2^{n+2}*. Тогава препятствието на задачата за вложимост* $(K/k, M_{2^{n+3}}, \mu_{2^n})$ *е* $(a,b) \in \mathrm{Br}(k)$*. Нека* $(a,b) = 1 \in Br(k)$ *и да предположим, че* $\gamma, \delta \in k^*$ *са такива, че* $\gamma^2 - b\delta^2 = a$*. Нека* $\omega = \gamma + \sqrt{b}\delta$ *и* $\theta = \sqrt[4]{a}/\omega^{2^{n-1}}$*. Тогава* $M/k = K(\sqrt[2^n]{\theta})/k$ *е разширение на Галоа, което е решение на задачата за вложимост* $(K/k, M_{2^{n+3}}, \mu_{2^n})$*.*

Доказателство: От предишния пример следва, че препятствието е $(a,b) \in \mathrm{Br}(k)$, понеже $\zeta^2 \in k^2$ е примитивен корен на единицата от степен 2^{n+1}. Нека сега $(a,b) = 1 \in \mathrm{Br}(k)$ и да предположим, че $\gamma, \delta \in k^*$ са такива, че $\gamma^2 - b\delta^2 = a$. Нека $\omega = \gamma + \sqrt{b}\delta$ и $\theta = \sqrt[4]{a}/\omega^{2^{n-1}}$. Имаме

$$\sigma(\theta)/\theta = i = \zeta^{2^n}$$

и

$$\tau(\theta)/\theta = \frac{(\gamma^2 - b\delta^2)^{2^{n-1}}}{(\gamma + \sqrt{b}\delta)^{2^n}} = a_\tau^{2^n},$$

където $a_\tau = \sqrt{a}/(\gamma + \sqrt{b}\delta) \in K$. Сега можем да положим за пораждащите x и y на $M_{2^{n+3}}$: $x(\sqrt[2^n]{\theta}) = \sqrt[2^n]{\theta}\zeta$ и $y(\sqrt[2^n]{\theta}) = \sqrt[2^n]{\theta}a_\tau$, така че $x|_K = \sigma$ и $y|_K = \tau$. Тогава $x^{2^{n+2}}(\sqrt[2^n]{\theta}) = \sqrt[2^n]{\theta}$ и $y^2(\sqrt[2^n]{\theta}) = \sqrt[2^n]{\theta}$, откъдето $|x| = 2^{n+2}$ и $|y| = 2$. Нататък, $yx(\sqrt[2^n]{\theta}) = \sqrt[2^n]{\theta}a_\tau\zeta$ и $x^{2^{n+1}+1}(\sqrt[2^n]{\theta}) = x(-\sqrt[2^n]{\theta}) = -\sqrt[2^n]{\theta}\zeta$, откъдето $x^{2^{n+1}+1}y(\sqrt[2^n]{\theta}) = \sqrt[2^n]{\theta}a_\tau\zeta$, значи $yx = x^{2^{n+1}+1}y$. Следователно, M/k е разширение на Галоа, което е решение на задачата за вложимост $(K/k, M_{2^{n+3}}, \mu_{2^n})$. □

В горната теорема дадохме едно конкретно модулярно разширение от степен 2^{n+3} над k, при предположението, че примитивен корен на единицата от степен 2^{n+2}

се съдържа в k. В следващия параграф ще опишем всички $M_{2^{n+3}}$ и $C_{2^{n+2}} \times C_2$ разширения, които съдържат квадратично разширение L/F такова, че примитивен корен на единицата ζ от степен 2^{n+2} е в L (F е произволно поле с характеристика различна от 2).

5.4 Разширения на Галоа, реализиращи модулярната 2-група

Нека F е произволно поле с характеристика $\neq 2$. Нека $n \geq 1$ е цяло число, $m = 2^{n+2}$ и да предположим, че ζ е примитивен m-ти корен на единицата, който се съдържа в квадратичното разширение $L = F(\sqrt{a})$ на F. Нашата цел е да опишем всички разширения на Галоа M, реализиращи групите M_{2m} и $C_m \times C_2$ като групи на Галоа над F, така че $L \subset M$ и M е циклично над L. Ще използваме съществено резултатите от [HLW].

Нека M е циклично разширение от степен m над L. Тогава $M = L(\alpha^{1/m})$ за някое $\alpha \in L^*$ според теорията на Кумер. Ако $\mathrm{Gal}(L/F) = \{1, \sigma\}$, то M е нормално над F само когато $\sigma(\alpha) = \alpha^t \beta^m$, където $\beta \in L^*$ и $t^2 \equiv 1 \pmod{m}$. За да построим явно всички такива разширения на Галоа M/F, трябва да направим детайлно описание на всички елементи α, удовлетворяващи условието $\sigma(\alpha) = \alpha^t \beta^m$.

Нека сега G е групата породена от елементи σ и τ такива, че

$$\begin{aligned} &1)\ |\tau| = m,\ \sigma \notin \langle \tau \rangle; \\ &2)\ \sigma\tau\sigma^{-1} = \tau^j,\ \sigma^2 = \tau^l; \\ &3)\ j^2 \equiv 1 \pmod{m} \text{ и } l(j-1) \equiv 0 \pmod{m}. \end{aligned} \tag{5.19}$$

По този начин можем да зададем всяка група от ред $2m$, която има циклична подгрупа от ред m. Например, ако $j \equiv m/2+1$ и $l \equiv 0$, получаваме модулярната група M_{2m}; ако $j \equiv 1$ и $l \equiv 0$, получаваме групата $C_m \times C_2$. Добре известно е, че има четири такива неабелови групи – модулярната, диедралната, полудиедралната и кватернионната групи; и две абелови групи – $C_m \times C_2$ и C_{2m}.

Да означим с (G, j, l) групата описана с (5.19). Съществува само една група с точност до изоморфизъм за $j \equiv m/2 + 1$ – групата M_{2m}, и две групи за $j \equiv 1$ – $C_m \times C_2$ и C_{2m}. Групата $C_m \times C_2$ се появява само ако l е четно, а групата C_{2m} се появява само ако l е нечетно.

Когато пишем $\alpha^{1/m}$ или $\sqrt[m]{\alpha}$, за $\alpha \in L^*$, ще предполагаме, че един конкретен m-ти корен на α е бил избран и фиксиран. Тъй като L съдържа примитивен m-ти корен на единицата ζ, то $M = L(\sqrt[m]{\alpha})$ е полето на разлагане на $x^m - \alpha$ над L и оттук M/L е разширение на Галоа. Ако $[M : L] = m$, то $\mathrm{Gal}(M/L) \cong C_m$. Нататък, $\sigma(\zeta) = \zeta^r$, където r е цяло число такова, че $\gcd(r, m) = 1$. Това ни дефинира $r \pmod{m}$ такова, че $r^2 \equiv 1$, понеже $\zeta = \sigma^2(\zeta) = \zeta^{r^2}$.

Ще казваме, че M/F реализира (G, j, l) ако M/F е разширение на Галоа с група на Галоа $(G, j, l) = \langle \tau, \sigma \rangle$, $L \subset M$, $\mathrm{Gal}(M/L) = \langle \tau \rangle$, където σ и τ имат съотношенията $\sigma\tau\sigma^{-1} = \tau^j$ и $\sigma^2 = \tau^l$. (Тук със σ означаваме също така и разширението на $\sigma \in \mathrm{Gal}(L/F)$ до автоморфизъм в $\mathrm{Gal}(M/F)$.)

Сега ще изложим няколко леми, които са частни случаи на [HLW, Lemma 4.1, Th. 3.4, Pr. 4.4, 4.5, 4.8].

Лема 5.4.1. *Ако $\delta, \delta' \in L^*$ и $\sigma(\delta)/\delta = \sigma(\delta')/\delta'$, то $\delta' = b\delta$ където $b \in F$.*

Лема 5.4.2. *Да предположим, че $\zeta \in L$. Нека $M = L(\sqrt[m]{\alpha})$, където $\alpha \in L$, и да предположим, че $[M : L] = m$. Тогава следните твърдения са еквивалентни:*

1. *M/F реализира (G, j, l).*
2. *$\sigma(\alpha) = \alpha^t\beta^m$, където $t \equiv jr \pmod m$ и $\alpha^{(t^2-1)/m}\beta^t\sigma(\beta) = \zeta^{l_1}$, където $l_1 \equiv l \pmod{\gcd(j+1, m)}$.*

Лема 5.4.3. *Ако $a \notin -F^2$ (т.е. $L = F(\sqrt{a}) \neq F(\sqrt{-1})$), то $F \cap L^m = F^m \cup a^{m/2}F^m$.*

Лема 5.4.4. *Нека $L = F(\sqrt{-1})$, и да предположим, че $\zeta \in L$ е примитивен корен на единицата от степен 2^{n+2}, $n \geq 0$. Тогава $F \cap L^{2^{n+1}} = F^{2^{n+1}} \cup -F^{2^{n+1}}$.*

Лема 5.4.5. *$L \neq F(\sqrt{-1})$ (т.е. $\sqrt{-1} \in F$) тогава и само тогава, когато $r \equiv 1 \pmod{2^{n+1}}$. В този случай, $\zeta^2 \in F$; освен това, $\zeta \in F$ тогава и само тогава, когато $r \equiv 1 \pmod{2^{n+2}}$.*

Ние можем да ограничим стойностите на t, j и r върху множеството $\{1, -1, 2^{n+1}+1, 2^{n+1}-1\}$. Модулярната група M_{2m} тогава се появява точно когато $j \equiv 2^{n+1}+1$ ($n \geq 1$), $t^2 \equiv 1$ и $t \equiv jr$. Именно, стойностите на t и r са:

1. $t = 1, r \equiv 2^{n+1} + 1$;
2. $t = -1, r \equiv 2^{n+1} - 1$;
3. $t = 2^{n+1} + 1, r \equiv 1$;
4. $t = 2^{n+1} - 1, r \equiv -1$.

Групата $C_m \times C_2$ се появява точно когато $j \equiv 1$ (т.е. $t \equiv r$) и l е четно.

5.4.1 $L \neq F(\sqrt{-1})$

От лема 5.4.5 следва, че $L \neq F(\sqrt{-1})$ тогава и само тогава, когато $r \equiv 1 \pmod{2^{n+1}}$, така че модулярната група се появява само ако $t = 1$ и $r \equiv 2^{n+1} + 1$, или $t = 2^{n+1} + 1$ и $r \equiv 1$.

Както обикновено, когато се конструират разширения на Галоа, важна роля играят нормените изображения. Норменото изображение $N = N_{L/F} : L \longrightarrow F^*$ дефинираме чрез $N(x) = x\sigma(x), \forall x \in L^*$. Следващата теорема ни дава явно описание на всички M_{2m} разширения в случая $a \neq_2 -1$.

Теорема 5.4.6. ([Mi2, Theorem 6.1]) *Нека $\alpha \in L^*$. Тогава $M/F = L(\sqrt[m]{\alpha})/F$ е M_{2m} разширение за $a \neq_2 -1$ тогава и само тогава, когато*

$$\alpha = \begin{cases} c(1+\gamma^m), & \text{ако } r \equiv 2^{n+1}+1; c \in F^*, \gamma \in L^*, N(\gamma)^m = 1, 1+\gamma^m = b\delta^2, \\ & b \in F^*, \delta \in L^*, \ u\ bc \notin F^2 \cup aF^2, \\ N(\delta)\eta^2/\delta^{2^{n+1}}, & \text{ако } r \equiv 1; \delta, \eta \in L^*, \eta \in F \cup \sqrt{a}F, \ u\ N(\delta) \notin F^2 \cup aF^2. \end{cases}$$

Доказателство: Да предположим, че α се задава както в условието. Ако $\alpha = c(1+\gamma^m)$, то $\sqrt{\alpha} = \pm\sqrt{bc}\delta$, значи $L(\sqrt{\alpha}) = F(\sqrt{bc}, \sqrt{a})$ е биквадратично разширение над F. Не е трудно да се провери, че $[M : L] = m$. Нататък, $\sigma(\alpha)/\alpha = 1/\gamma^m = \beta^m \neq -1$ за $\beta = 1/\gamma$. Следователно, $\sigma(\alpha) = \alpha\beta^m$, значи $M/F = L(\sqrt[m]{\alpha})/F$ е M_{2m} разширение.

Ако $\alpha = N(\delta)\eta^2/\delta^{2^{n+1}}$, то $\sqrt{\alpha} = \pm\sqrt{N(\delta)}\eta/\delta^{2^n}$, значи $L(\sqrt{\alpha}) = F(\sqrt{N(\delta)}, \sqrt{a})$ е биквадратично разширение над F. Тук отново $[M : L] = m$. Нататък,

$$\sigma(\alpha)/\alpha^{2^{n+1}} = \alpha\delta^{2^{2n+2}}/\sigma(\delta^{2^{n+2}})\eta^{2^{n+2}} = \alpha\beta^m,$$

където $\beta = \delta^{2^n}/\sigma(\delta)\eta$. Следователно, $\sigma(\alpha) = \alpha^{2^{n+1}+1}\beta^m$, значи M/F е M_{2m} разширение.

Нека сега $M/F = L(\sqrt[m]{\alpha})/F$ е M_{2m} разширение. Ако $r \equiv 2^{n+1}+1$ и $\sigma(\alpha) = -\alpha$, то $\sigma(\alpha) = -\alpha = \alpha\beta^m$ за $\beta \in L$. Следователно, $-1 = \beta^m \in L^m$ и понеже $\sigma(\sqrt{a}) = -\sqrt{a}$, от лема 5.4.1 следва, че $\alpha = b\sqrt{a}, b \in F^*$. Тогава $L(\sqrt{\alpha}) = F(\sqrt{b\sqrt{a}}, \sqrt{a})$ е циклично разширение над F. Но $L(\sqrt{\alpha})$ е неподвижното подполе на τ^2, което трябва да бъде биквадратично разширение над F – достигаме до противоречие.

Ако $r \equiv 2^{n+1}+1$ и $\sigma(\alpha) \neq -\alpha$, то $t = 1$ и $\sigma(\alpha) = \alpha\beta^m$, където $1 + \beta^m \neq 0$. Нека $\gamma = \sigma(\beta)$, значи $1+\gamma^m \neq 0$. От $\beta^m = \sigma(\alpha)/\alpha$ следва, че $\beta^m\sigma(\beta^m) = N(\beta^m) = N(\gamma^m) = 1$. Нататък,

$$\sigma(\alpha)/\alpha = \beta^m = \frac{1+\beta^m}{1+\sigma(\beta^m)} = \frac{\sigma(1+\gamma^m)}{1+\gamma^m},$$

откъдето според лема 5.4.1 следва, че $\alpha = c(1+\gamma^m)$ за някое $c \in F^*$.

Ако $r \equiv 1$, то $t = 2^{n+1}+1$ и $\sigma(\alpha) = \alpha^{2^{n+1}+1}\beta^{2^{n+2}}$ за $\beta \in L$. Нека $k = 2^{n+1}(k \geq 4$, понеже $n \geq 1)$. Тогава $\sigma(\alpha) = \alpha^{k+1}\beta^{2k}$ и $\sigma(\alpha)/\alpha = (\alpha\beta^2)^k$. Нека $\omega = N(\alpha\beta^2)$. Тогава $\omega^k = N(\sigma(\alpha)/\alpha) = 1$, значи ω е степен на ζ^2. Тъй като $\zeta \in F$ за $r \equiv 1$, получаваме в частност, че $\omega \in F^2$. Нека $\gamma = \alpha\beta^2$. Тогава

$$\sigma(\alpha\gamma^{k/2}) = \alpha\gamma^k\sigma(\gamma^{k/2}) = \alpha\gamma^{k/2}N(\gamma)^{k/2} = \alpha\gamma^{k/2}\omega^{k/2}.$$

От $\omega^k = 1$ следва, че $\omega^{k/2} = \pm 1$. Ако $\omega^{k/2} = -1$, получаваме $\alpha\gamma^{k/2} \in \sqrt{a}F, N(\alpha\gamma^{k/2}) \in -aF^2, N(\alpha) \in -aF^2, N(\alpha\beta^2) \in -aF^2$, и $\omega \in -aF^2 = aF^2 \neq F^2$ (понеже $-1 = \zeta^k \in F^2$) – противоречие. Следователно $\omega^{k/2} = 1$. Сега, от $\sigma(\alpha\gamma^{k/2}) = \alpha\gamma^{k/2}$ следва, че $\alpha\gamma^{k/2} = b \in F^*$ и $\alpha\beta^2 = b\beta^2\gamma^{-k/2} = b\delta^2$, където $\delta = \beta/\gamma^{k/4}$. Тъй като $b^2N(\delta)^2 = N(b\delta^2) = N(\alpha\beta^2) = \omega$, имаме, че $b^kN(\delta^k) = \omega^{k/2} = 1$. Следователно,

$$\sigma(\alpha)/\alpha = (\alpha\beta^2)^k = \delta^{2k}/N(\delta)^k = \delta^k/\sigma(\delta)^k$$

и $\sigma(\alpha\delta^k) = \alpha\delta^k$, значи $\alpha\delta^k = d \in F$. Сега, от $\sigma(\alpha)/\alpha = (\delta/\sigma(\delta))^k$ следва, че $\alpha\beta^2 = \omega'\delta/\sigma(\delta) = \omega' c/\sigma(\delta)^2$, където $(\omega')^k = 1$ и $c = N(\delta)$. Нататък, $\alpha/d = \delta^{-k} \in L^2$ и $\alpha/c = \omega'/(\sigma(\delta)^2\beta^2) \in L^2$, откъдето $d/c \in L^2 \cap F$. Нека $\eta^2 = d/c \in L^2 \cap F = F^2 \cup aF^2$, следователно $\eta \in F \cup \sqrt{a}F$, и $\alpha = c\eta^2/\delta^k$.

Останалото следва от факта, че неподвижното подполе $F(\sqrt{\alpha}, \sqrt{a})$ на τ^2 трябва да бъде биквадратично разширение над F. □

Следващата теорема ни дава описание на всички $C_m \times C_2$ разширения.

Теорема 5.4.7. ([Mi2, Theorem 6.2]) *Нека $\alpha \in L^*$. Тогава $M/F = L(\sqrt[m]{\alpha})/F$ е $C_m \times C_2$ разширение за $a \neq_2 -1$ тогава и само тогава, когато*

$$\alpha = \begin{cases} b\gamma^m, & r \equiv 1; b \in F^*, \gamma \in L^*, \ u\ b \notin F^2 \cup aF^2, \\ N(\delta)\eta^2/\delta^{2^{n+1}}, & ако\ r \equiv 2^{n+1}+1; \delta, \eta \in L^*, \eta \in F \cup \sqrt{a}F, \ u \\ & N(\delta) \notin F^2 \cup aF^2. \end{cases}$$

Доказателство: Да предположим, че α се задава чрез формулата от условието. Ако $\alpha = b\gamma^m$, където $b \in F^*, \gamma \in L^*$ и $r \equiv 1$, то $\sqrt{\alpha} = \sqrt{b}\gamma^{m/2}$, значи $L(\sqrt{\alpha})$ е биквадратично над F и $[M : L] = m$. Нататък, $\sigma(\alpha)/\alpha = (\sigma(\gamma)/\gamma)^m$, т.е. $\sigma(\alpha) = \alpha\beta^m$, където $\beta = \sigma(\gamma)/\gamma$. Следователно, $M/F = L(\sqrt[m]{\alpha})/F$ е или $C_m \times C_2$ или C_{2m} разширение. Лема 5.4.2 ни дава, че $\alpha^{(t^2-1)/m}\beta^t\sigma(\beta) = \zeta^{l_1}$, където $l_1 \equiv l \pmod{\gcd(j+1, m)}$. В този случай, $t = 1, \beta\sigma(\beta) = 1$ и $l \equiv 0 \pmod{\gcd(j+1, m)}$, следователно l е четно, значи M/F е $C_m \times C_2$ разширение.

Ако $\alpha = N(\delta)\eta^2/\delta^{2^{n+1}}, \delta \in L^*, \eta \in F \cup \sqrt{a}F$ и $r \equiv 2^{n+1}+1$, получаваме с аналогични разсъждения както в теорема 5.4.6, че M/F е нормално и $[M:L] = m$. Нататък, $\sigma(\alpha) = \alpha^{2^{n+1}+1}\beta^{2^{n+2}}$, където $\beta = \delta^{2^n}/\sigma(\delta)\eta$, следователно $t = 2^{n+1}+1$ и $j \equiv 1$. От $\zeta^{l_1} = \alpha^{2^n+1}\beta^{2^{n+1}+1}\sigma(\beta) = \eta/\sigma(\eta) = \pm 1 \in \langle\zeta^2\rangle$ следва, че M/F е $C_m \times C_2$ разширение.

Да предположим сега, че $M/F = L(\sqrt[m]{\alpha})/F$ е $C_m \times C_2$ разширение. Ако $r \equiv 1$, то $t = 1$, значи $\sigma(\alpha) = \alpha\beta^m, \beta \in L^*$. Нататък, $\zeta^{l_1} = \beta\sigma(\beta) = \zeta^{2s}$, за някое $s \geq 1$. Тогава $\beta/\zeta^s\sigma(\beta/\zeta^s) = 1$ и от теорема 90 на Хилберт следва, че $\beta/\zeta^s = \sigma(\gamma)/\gamma$, за някое $\gamma \in L^*$. Следователно, $\beta^m = \sigma(\gamma^m)/\gamma^m = \sigma(\alpha)/\alpha$ и лема 5.4.1 ни дава, че $\alpha = b\gamma^m$, за някое $b \in F^*$.

Ако $r \equiv 2^{n+1}+1$, то $t = 2^{n+1}+1$. Нека $k = 2^{n+1}$. Тогава $\sigma(\alpha) = \alpha^{k+1}\beta^{2k}$, за някое $\beta \in L^* (k \geq 4)$, откъдето $\sigma(\alpha)/\alpha = (\alpha\beta^2)^k$. Нека $\omega = N(\alpha\beta^2)$. Тогава $\omega^k = N(\sigma(\alpha)/\alpha) = 1$. Тъй като ω е степен на ζ^2, имаме $\omega \in L^2 \cap F = F^2 \cup aF^2$. Нека $\rho = \alpha^{(t^2-1)/m}\beta^t\sigma(\beta) = \zeta^{l_1}$, където $l_1 \equiv l \pmod{\gcd(j+1, m)}$. Тъй като l е четно, $\rho \in \langle\zeta^2\rangle$. Следователно, $\rho = \alpha^{k/2+1}\beta^{k+1}\sigma(\beta)$ и $N(\alpha) = \alpha^{k+2}\beta^{2k} = \rho^2/N(\beta^2) \in F^2$, понеже $\zeta^2 \in L^2 \cap F = F^2 \cup aF^2$ и $\zeta^4 \in F^2$. Сега, $\omega^k = 1$ ни дава, че $\omega^{k/2} = \pm 1$. Ако $\omega^{m/2} = -1$, получаваме аналогично на теорема 5.4.6, че $N(\alpha) \in aF^2 \neq F^2$ – противоречие. Следователно, $\omega^{m/2} = 1$. Останалата част на доказателството е аналогична на теорема 5.4.6. □

5.4.2 $L = F(\sqrt{-1})$

Лема 5.4.5 ни дава, че $L = F(\sqrt{-1})$ точно когато $r \equiv -1 \pmod{2^{n+1}}$, т.е. $r \equiv -1 \pmod m$ или $r \equiv 2^{n+1}-1 \pmod m$, така че модулярната група се появява само ако $t = -1$ и $r \equiv 2^{n+1}-1$, или $t = 2^{n+1}-1$ и $r \equiv -1$.

Теорема 5.4.8. ([Mi2, Theorem 7.1]) *Нека $\alpha \in L^*$. Тогава $M/F = L(\sqrt[m]{\alpha})/F$ е M_{2m} разширение за $a =_2 -1$ тогава и само тогава, когато*

$$\alpha = \begin{cases} \pm b^{m/2}N(\gamma)/\gamma^2, & \text{ако } r \equiv 2^{n+1}-1; b \in F^*, \gamma \in L^* \text{ и } N(\gamma) \notin F^2 \cup -F^2, \\ c^{2^n+1}/\delta^2, & \text{ако } r \equiv -1; c \in F^*, \delta \in L^*, N(\delta) = \pm c \text{ и } c \notin F^2 \cup -F^2. \end{cases}$$

Доказателство: Да предположим, че α се задава чрез формулата от условието. Ако $\alpha = \pm b^{m/2}N(\gamma)/\gamma^2, b \in F^*, \gamma \in L^*$ и $r \equiv 2^{n+1}-1$, то $\sqrt{\alpha} = \pm b^{m/4}\sqrt{N(\gamma)}/\gamma$ или $\pm ib^{m/4}\sqrt{N(\gamma)}/\gamma$, значи $L(\sqrt{\alpha})$ е биквадратично над F и $[M:L] = m$. Нататък, $N(\alpha) = b^m$, т.е. $\sigma(\alpha) = \alpha^{-1}b^m$. Следователно, $M/F = L(\sqrt[m]{\alpha})/F$ е M_{2m} разширение.

Ако $\alpha = c^{2^n+1}/\delta^2, c \in F^*, N(\delta) = \pm c$ и $r \equiv -1$, то отново $[M : L] = m$ и

$$\sigma(\alpha)/\alpha^{2^{n+1}} = \alpha^{-1}(\delta/c^{2^{n-1}})^{2^{n+2}}.$$

Нека $\beta = \delta/c^{2^{n-1}}$. Тогава $\sigma(\alpha) = \alpha^{2^{n+1}-1}\beta^m$, откъдето $M/F = L(\sqrt[m]{\alpha})/F$ е M_{2m} разширение.

Да предположим сега, че $M/F = L(\sqrt[m]{\alpha})/F$ е M_{2m} разширение. Ако $r \equiv 2^{n+1}-1$, то $t = -1$, значи $\sigma(\alpha) = \alpha^{-1}\beta^m$, за някое $\beta \in L^*$. Тогава $N(\alpha) = \beta^m \in F$. От $N(\alpha) = \sigma(N(\alpha)) = [\sigma(\beta)]^m$ следва, че $[\sigma(\beta)]^m = \beta^m$, така че $\sigma(\beta) = \beta\omega$, където $\omega^m = 1$, т.е. $\omega \in \langle\zeta\rangle$. Нататък, $\sigma^2(\beta) = \beta = \beta\omega\sigma(\omega)$, откъдето $\omega\sigma(\omega) = 1$. Сега, от $\sigma(\zeta) = \zeta^r$ следва, че $1 = \omega\sigma(\omega) = \omega^{r+1} = \omega^{m/2} = 1$, т.е. $\omega \in \langle\zeta^2\rangle$. Тогава имаме $\sigma(\beta^{m/2}) = \beta^{m/2}\omega^{m/2} = \beta^{m/2} \in F$, значи $(\alpha/\beta^{m/2})\sigma(\alpha/\beta^{m/2}) = N(\alpha/\beta^{m/2}) = 1$. Теорема 90 на Хилберт тогава ни дава, че $\alpha/\beta^{m/2} = \sigma(\gamma)/\gamma$, за някое $\gamma \in L^*$, откъдето $\alpha = \beta^{m/2}N(\gamma)/\gamma^2$. Остава да намерим конкретните стойности на $\beta \in L^*$. Имаме, че $\omega = \zeta^{2s}, s \geq 1$, и $\sigma(\beta) = \beta\omega = \beta\zeta^{2s}$. Тогава

$$\beta\sigma(\beta) = \beta^2\zeta^{2s} = (\beta\zeta^s)^2 \in L^2 \cap F = F^2 \cup -F^2,$$

откъдето $\beta^2\zeta^{2s} = \pm b^2, b \in F$. Следователно, $\beta^{m/2} = b^{m/2}(\zeta^s)^{m/2} = \pm b^{m/2}$.

Сега, ако $r \equiv -1$, то $t = 2^{n+1} - 1$. Нека $k = 2^{n+1}$ $(n \geq 1)$. Имаме тогава $\sigma(\alpha) = \alpha^{k-1}\beta^{2k}$ и $N(\alpha) = (\alpha\beta^2)^k \in F \cap L^k = F^k \cup -F^k$, според лема 5.4.4. Ако $(\alpha\beta^2)^k \in F^k$, то $\alpha\beta^2 = c\omega$, където $\omega^k = 1, c \in F$, значи $\omega \in \langle\zeta^2\rangle$. Ако заменим β с $\beta\omega^{-1/2}$, равенството $\sigma(\alpha) = \alpha^{k-1}\beta^{2k}$ няма да се промени, така че ще предполагаме, че $\alpha\beta^2 = c \in F$. Нека $\delta = c^{k/4}\beta$. Тогава

$$\alpha = c/\beta^2 = c^{k/2+1}/(c^{k/2}\beta^2) = c^{k/2+1}/\delta^2$$

и

$$N(\delta^2) = N(c^{k/2}\beta^2) = c^k N(c/\alpha) = c^2,$$

откъдето $N(\delta) = \pm c$. Ако $(\alpha\beta^2)^k \in -F^k$, то $\alpha\beta^2 = \zeta c\omega$, където $c \in F$ и $\omega^k = 1$. Отново, можем да заменим β с $\beta\omega^{-1/2}$ и да предположим, че $\alpha\beta^2 = \zeta c$. Тогава $N(\alpha) = (\alpha\beta^2)^k = -c^k \in -F^2 \neq F^2$, следователно $N(\alpha\beta^2) \in -F^2$, но $N(\zeta c) = N(c) \in F^2$ – противоречие. По този начин, ако $r \equiv -1$, остава възможността $\alpha = c^{k/2+1}/\delta^2, c \in F$ и $N(\delta) = \pm c$.

Останалото следва от факта, че неподвижното подполе $F(\sqrt{\alpha}, \sqrt{-1})$ на τ^2 трябва да бъде биквадратично разширение на F. Това доказва теоремата. □

Накрая, следващата теорема ни дава описание на всички $C_m \times C_2$ разширения.

Теорема 5.4.9. ([Mi2, Theorem 7.2]) *Нека $\alpha \in L^*$. Тогава $M/F = L(\sqrt[m]{\alpha})/F$ е $C_m \times C_2$ разширение за $a =_2 -1$ тогава и само тогава, когато*

$$\alpha = \begin{cases} \pm b_1^{m/2} N(\gamma_1)/\gamma_1^2, & \text{ако } r \equiv -1; b_1 \in F^*, \gamma_1 \in L^* \text{ и } N(\gamma_1) \notin F^2 \cup -F^2, \\ c^{2^n+1}/\gamma^2, & \text{ако } r \equiv 2^{n+1}-1; c \in F^*, \gamma \in L^*, N(\gamma) = \pm c \text{ и} \\ & c \notin F^2 \cup -F^2. \end{cases}$$

Доказателство: Да предположим, че α се задава с формулата от условието. Ако $\alpha = \pm b_1^{m/2} N(\gamma_1)/\gamma_1^2$, където $b_1 \in F^*, \gamma_1 \in L^*$ и $r \equiv -1$, то $[M : L] = m$ и също $N(\alpha) = b_1^m = \beta^m$, където $\beta = b_1$. Следователно, $\sigma(\alpha) = \alpha^{-1}\beta^m$, значи $M/F = L(\sqrt[m]{\alpha})/F$ е или $C_m \times C_2$ или C_{2m} разширение. Нека $\rho = \alpha^{(t^2-1)/m}\beta^t\sigma(\beta) = \zeta^{l_1}$, където $l_1 \equiv l \pmod{\gcd(j+1, m)}$. Тогава имаме $\rho = \sigma(\beta)/\beta = 1$, откъдето l_1 е четно и M/F е $C_m \times C_2$ разширение.

Ако $\alpha = c^{2^n+1}/\gamma^2$, където $c \in F^*, \gamma \in L^*, N(\gamma) = \pm c$ и $r \equiv 2^{n+1}-1$, то $[M : L] = m$ и също $\sigma(\alpha) = \alpha^{k-1}\beta^{2k}$, където $k = 2^{n+1}$ и $\beta = \gamma/c^{k/4}$. Тъй като $t = k-1$, то $M/F = L(\sqrt[m]{\alpha})/F$ е или $C_m \times C_2$ или C_{2m} разширение. Тогава имаме $t^2 - 1 = k/2 - 1$ и

$$\rho = \alpha^{k/2-1}\beta^{k-1}\sigma(\beta) = (\alpha\beta^2)^{k/2}N(\beta)/(\alpha\beta^2) = \pm 1 \in \langle\zeta^2\rangle,$$

откъдето M/F е $C_m \times C_2$ разширение.

Да предположим сега, че $M/F = L(\sqrt[m]{\alpha})/F$ е $C_m \times C_2$ разширение. Ако $r \equiv -1$, то $t = -1$ и $\sigma(\alpha) = \alpha^{-1}\beta^m$, където $\beta \in L^*$. Следователно, $N(\alpha) = \beta^m \in L^m \cap F$. Очевидно, $\sigma(\beta^m) = [\sigma(\beta)]^m = \beta^m$, което ни дава $\sigma(\beta) = \beta\omega$, където $\omega^m = 1$, т.е. $\omega \in \langle\zeta\rangle$. Тъй като $\sigma(\zeta) = \zeta^r = \zeta^{-1}$, получаваме $N(\omega) = 1$. Тогава имаме $\omega^{m/2} = \pm 1$. Ако $\omega^{m/2} = 1$, аналогично на теорема 5.4.8 получаваме, че $\alpha = \pm b_1^{m/2} N(\gamma_1)/\gamma_1^2$, където $b_1 \in F^*$ и $\gamma_1 \in L^*$. Ако $\omega^{m/2} = -1$, то $\omega \notin \langle\zeta^2\rangle$ и $\sigma(\beta^{m/2}) = -\beta^{m/2}$, откъдето $\beta^{m/2} = b_3\sqrt{-1}$, за някое $b_3 \in F^*$. Тогава $N(\alpha/\beta^{m/2}) = -1, N(\alpha^2/\beta^m) = 1$ и теорема 90 на Хилберт ни дава $\alpha^2/\beta^m = \sigma(\gamma_2)/\gamma_2$, за някое $\gamma_2 \in L^*$. Следователно, $\alpha^2 = \beta^m\sigma(\gamma_2)/\gamma_2 = \beta^m N(\gamma_2)/\gamma_2^2$, значи $N(\gamma_2) \in L^2 \cap F = F^2 \cup -F^2$, т.е. $N(\gamma_2) = \pm\delta^2$, за някое $\delta \in F^*$. По този начин, $\alpha = \pm\beta^{m/2}\delta/\gamma_2$, където $\gamma_2 \in L^*$ и $N(\gamma_2) = \pm\delta^2$.

Сега трябва да конкретизираме стойностите на β, за които $\beta^{m/2} = b_3\sqrt{-1}, b_3 \in F^*$ и $N(\alpha) \in L^m$. Имаме, че $N(\alpha) = b_3^2\delta^2/N(\gamma_2)$, така че е нужно да разгледаме два случая. Ако $N(\gamma_2) = \delta^2$, то $N(\alpha) = b_3^2 = -\beta^m \in L^m$, откъдето $-1 \in L^m$. Следователно, $\sqrt{-1} \in L^{m/2}$ и $b_3\sqrt{-1} \in L^{m/2}$, значи $b_3 \in L^{m/2} \cap F = F^{m/2} \cup -F^{m/2}$ според лема 5.4.4, т.е. $b_3 = \pm b_2^{m/2}$, за някое $b_2 \in F^*$. Получаваме $\alpha = \pm b_2^{m/2}\sqrt{-1}\delta/\gamma_2$. Ако $N(\gamma_2) = -\delta^2$, то $N(\alpha) = -b_3^2 = \beta^m \in L^m$. Нататък, $\rho = \alpha^{(t^2-1)/m}\beta^t\sigma(\beta) = \sigma(\beta)/\beta = \zeta^{l_1}$, следователно

$\rho^{m/2} = \sigma(\beta^{m/2})/\beta^{m/2} = -1 = (\zeta^{l_1})^{m/2}$, откъдето l_1 е нечетно, което е противоречие. Сега, от това, че $L(\sqrt{\alpha})$ е биквадратично над F следва, че α трябва да изглежда по същия начин, както в случая $\omega^{m/2} = 1$.

Накрая, ако $r \equiv 2^{n+1} - 1$, то $t = 2^{n+1} - 1$. Нека $k = 2^{n+1}$. Тогава имаме $\sigma(\alpha) = \alpha^{k-1}\beta^{2k}$, значи $N(\alpha) = (\alpha\beta^2)^k \in F \cap L^k = F^k \cup -F^k$. Ако $(\alpha\beta^2)^k \in F^k$, то можем по идентичен начин с теорема 5.4.8 да получим, че $\alpha = c^{k/2+1}/\gamma^2$ и $N(\gamma) = \pm c$. Ако $(\alpha\beta^2)^k \in -F^k$, то $\alpha\beta^2 = \zeta c\omega$, където $c \in F^*, \omega^k = 1$ и ние можем отново да заменим β с $\beta\omega^{-1/2}$ и да предполагаме, че $\alpha\beta^2 = \zeta c$. Нататък, $\rho = \alpha^{k/2-1}\beta^{k-1}\sigma(\beta) = \zeta^{l_1}$. Нека $\gamma = c^{k/4}\beta$. Тогава $\rho = (\alpha\beta^2)^{k/2}\sigma(\beta)/(\alpha\beta) = \zeta^{k/2-1}N(\gamma)/c$. От $N(\gamma^2) = c^2$ следва, че $N(\gamma) = \pm c$. Следователно, $\rho = \pm\zeta^{k/2-1} = \zeta^{l_1}$, значи l_1 е нечетно – противоречие.

Останалото отново следва от това, че неподвижното подполе $F(\sqrt{\alpha}, \sqrt{-1})$ на τ^2 трябва да бъде биквадратично разширение на F. $\square$

Глава 6
Препятствия за реализиране на неабеловите 2-групи, имащи циклична подгрупа с индекс 4

Крайните неабелови групи от ред 2^n, които имат циклична подгрупа с индекс 4, но нямат циклична с индекс 2 са класифицирани от Ниномия в [Ni, Theorem 2]. Техните представяния са следните:

(I) $n \geq 4$

$G_1 = \langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^4 = 1, \tau^{-1}\sigma\tau = \sigma^{1+2^{n-3}} \rangle$,
$G_2 = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \lambda^2 = 1, \sigma^{2^{n-3}} = \tau^2, \tau^{-1}\sigma\tau = \sigma^{-1}, \sigma\lambda = \lambda\sigma, \tau\lambda = \lambda\tau \rangle$,
$G_3 = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1}\sigma\tau = \sigma^{-1}, \sigma\lambda = \lambda\sigma, \tau\lambda = \lambda\tau \rangle$,
$G_4 = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \sigma\tau = \tau\sigma, \sigma\lambda = \lambda\sigma, \lambda^{-1}\tau\lambda = \sigma^{2^{n-3}}\tau \rangle$,
$G_5 = \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \sigma\tau = \tau\sigma, \lambda^{-1}\sigma\lambda = \sigma\tau, \tau\lambda = \lambda\tau \rangle$.

(II) $n \geq 5$

$$
\begin{aligned}
G_6 &= \langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^4 = 1, \tau^{-1}\sigma\tau = \sigma^{-1} \rangle, \\
G_7 &= \langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^4 = 1, \tau^{-1}\sigma\tau = \sigma^{-1+2^{n-3}} \rangle, \\
G_8 &= \langle \sigma, \tau : \sigma^{2^{n-2}} = 1, \sigma^{2^{n-3}} = \tau^4, \tau^{-1}\sigma\tau = \sigma^{-1} \rangle, \\
G_9 &= \langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^4 = 1, \sigma^{-1}\tau\sigma = \tau^{-1} \rangle, \\
G_{10} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1}\sigma\tau = \sigma^{1+2^{n-3}}, \sigma\lambda = \lambda\sigma, \tau\lambda = \lambda\tau \rangle, \\
G_{11} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1}\sigma\tau = \sigma^{-1+2^{n-3}}, \sigma\lambda = \lambda\sigma, \tau\lambda = \lambda\tau \rangle, \\
G_{12} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \sigma\tau = \tau\sigma, \lambda^{-1}\sigma\lambda = \sigma^{-1}, \lambda^{-1}\tau\lambda = \sigma^{2^{n-3}}\tau \rangle, \\
G_{13} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \sigma\tau = \tau\sigma, \lambda^{-1}\sigma\lambda = \sigma^{-1}\tau, \tau\lambda = \lambda\tau \rangle,
\end{aligned}
$$

$$
\begin{aligned}
G_{14} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = 1, \sigma^{2^{n-3}} = \lambda^2, \sigma\tau = \tau\sigma, \lambda^{-1}\sigma\lambda = \sigma^{-1}\tau, \tau\lambda = \lambda\tau \rangle, \\
G_{15} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1}\sigma\tau = \sigma^{1+2^{n-3}}, \lambda^{-1}\sigma\lambda = \sigma^{-1+2^{n-3}}, \tau\lambda = \lambda\tau \rangle, \\
G_{16} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1}\sigma\tau = \sigma^{1+2^{n-3}}, \lambda^{-1}\sigma\lambda = \sigma^{-1+2^{n-3}}, \\
&\quad \lambda^{-1}\tau\lambda = \sigma^{2^{n-3}}\tau \rangle, \\
G_{17} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1}\sigma\tau = \sigma^{1+2^{n-3}}, \lambda^{-1}\sigma\lambda = \sigma\tau, \tau\lambda = \lambda\tau \rangle, \\
G_{18} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = 1, \lambda^2 = \tau, \tau^{-1}\sigma\tau = \sigma^{1+2^{n-3}}, \lambda^{-1}\sigma\lambda = \sigma^{-1}\tau \rangle.
\end{aligned}
$$

(III) $n \geq 6$

$$
\begin{aligned}
G_{19} &= \langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^4 = 1, \tau^{-1}\sigma\tau = \sigma^{1+2^{n-4}} \rangle, \\
G_{20} &= \langle \sigma, \tau : \sigma^{2^{n-2}} = \tau^4 = 1, \tau^{-1}\sigma\tau = \sigma^{-1+2^{n-4}} \rangle, \\
G_{21} &= \langle \sigma, \tau : \sigma^{2^{n-2}} = 1, \sigma^{2^{n-3}} = \tau^4, \sigma^{-1}\tau\sigma = \tau^{-1} \rangle, \\
G_{22} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \sigma\tau = \tau\sigma, \lambda^{-1}\sigma\lambda = \sigma^{1+2^{n-4}}\tau, \lambda^{-1}\tau\lambda = \sigma^{2^{n-3}}\tau \rangle, \\
G_{23} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \sigma\tau = \tau\sigma, \lambda^{-1}\sigma\lambda = \sigma^{-1+2^{n-4}}\tau, \lambda^{-1}\tau\lambda = \sigma^{2^{n-3}}\tau \rangle, \\
G_{24} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = \lambda^2 = 1, \tau^{-1}\sigma\tau = \sigma^{1+2^{n-3}}, \lambda^{-1}\sigma\lambda = \sigma^{-1+2^{n-4}}, \tau\lambda = \lambda\tau \rangle, \\
G_{25} &= \langle \sigma, \tau, \lambda : \sigma^{2^{n-2}} = \tau^2 = 1, \sigma^{2^{n-3}} = \lambda^2, \tau^{-1}\sigma\tau = \sigma^{1+2^{n-3}}, \lambda^{-1}\sigma\lambda = \sigma^{-1+2^{n-4}}, \\
&\quad \tau\lambda = \lambda\tau \rangle,
\end{aligned}
$$

(IV) $n = 5$

$$G_{26} = \langle \sigma, \tau, \lambda : \sigma^8 = \tau^2 = 1, \sigma^4 = \lambda^2, \tau^{-1}\sigma\tau = \sigma^5, \lambda^{-1}\sigma\lambda = \sigma\tau, \tau\lambda = \lambda\tau \rangle.$$

6.1 Препятствията за групите $G_1, \ldots, G_{17}$ и G_{26}

6.1.1 Групата G_{17}

Да вземем групата $\mathcal{G}$ породена от елементи $b_1, \ldots, b_6$ такива, че $b_1^{2^{n-3}} = 1, b_1^2 = b_4, b_2^2 = 1, [b_2, b_1] = b_3, b_3^2 = 1, [b_3, b_1] = b_5, [b_3, b_2] = 1, b_4^{2^{n-4}} = 1, [b_4, b_2] = b_5, [b_4, b_3] = b_6, b_5^2 = 1, [b_5, b_1] = b_6, b_6^2 = 1, [b_5, b_2] = [b_5, b_3] = [b_5, b_4] = 1$ и b_6 е централен. Полагаме $E_4 = \langle b_5, b_6 \rangle \cong C_2^2$. Да забележим, че $b_1 b_5 b_1^{-1} = b_5 b_6$ и $b_i b_5 b_i^{-1} = b_5$ за $i = 2, \ldots, 6$. Да разгледаме груповото разширение

$$1 \longrightarrow E_4 \longrightarrow \mathcal{G} \underset{\substack{b_1 \mapsto x \\ b_2 \mapsto y}}{\longrightarrow} G \longrightarrow 1, \tag{6.1}$$

където G е изоморфна на групата $\widetilde{C_{2^{n-3}} \times C_2}$ от лема 4.3.11, породена от елементи x, y и z такива, че $x^{2^{n-3}} = y^2 = z^2 = 1, yx = xyz, z$ – централен. Нататък, полагаме $H = \langle x^2, y, z\rangle \cong C_{2^{n-4}} \times C_2^2$ и $\mathcal{H} = \langle b_2, \ldots, b_6 | b_2^2 = b_3^2 = b_5^2 = b_6^2 = 1, b_4^{2^{n-4}} = 1, [b_4, b_2] = b_5, [b_4, b_3] = b_6\rangle$ – про-образът на H в $\mathcal{G}$. Очевидно, $\mathcal{H}$ лежи в централизатора на E_4 в $\mathcal{G}$. Имаме груповото разширение $1 \longrightarrow E_4 \longrightarrow \mathcal{H} \longrightarrow H \longrightarrow 1$. Означаваме с c_1 2-кокласът в $H^2(G, \mu_2)$, представящ груповото разширение

$$1 \longrightarrow E_4/\langle b_6\rangle \cong \mu_2 \longrightarrow \mathcal{G}/\langle b_6\rangle \underset{\substack{\sigma\mapsto x\\ \tau\mapsto y}}{\longrightarrow} G \longrightarrow 1,$$

където $\mathcal{G}/\langle b_6\rangle$ е изоморфна на групата $G'_{17} \cong \langle \sigma, \tau, \lambda, \rho \mid \sigma^{2^{n-3}} = \tau^2 = \lambda^2 = \rho^2 = 1, \tau^{-1}\sigma\tau = \sigma\rho, \lambda^{-1}\sigma\lambda = \sigma\tau, [\tau, \lambda] = [\rho, \sigma] = [\rho, \tau] = [\rho, \lambda] = 1\rangle$ за $\sigma = b_1, \tau = b_3, \lambda = b_2, \rho = b_5$. Означаваме с c_2 2-кокласът в $H^2(H, \mu_2)$, представящ груповото разширение

$$1 \longrightarrow E_4/\langle b_5\rangle \cong \mu_2 \longrightarrow \mathcal{H}/\langle b_5\rangle \underset{\substack{b_1\mapsto x\\ b_2\mapsto y}}{\longrightarrow} H \longrightarrow 1,$$

където $\mathcal{H}/\langle b_5\rangle \cong \widetilde{C_{2^{n-4}} \times C_2 \times C_2}$. От теорема 2.3.8 имаме, че $c_1 = \mathrm{cor}_{G/H}(c_2)$. Нататък, всяко G-разширение L'/F трябва да съдържа $D \curlywedge C$ разширение L/F, понеже $G/\langle\sigma^4\rangle \cong D \curlywedge C$.

От теорема 2.2.1 получаваме, че препятствието на задачата за вложимост $(L'/K, \mathcal{H}/\langle b_5\rangle \cong \widetilde{C_{2^{n-4}} \times C_2} \times C_2 \times C_2, \mu_2)$ е равно на препятствието на задачата $(L/K, D_8 \times C_2, \mu_2)$, което в случая е $(2r(\alpha_1 - \sqrt{a}), 2s(\beta_1 + \sqrt{a}))_K \in \mathrm{Br}_2(K)$. Следователно, препятствието на задачата за вложимост съответстваща на c_1 е същото както на задачата $(L/F, G_{(32,6)}, \mu_2)$ (виж теорема 3.2.12).

Накрая, да забележим, че са в сила изоморфизмите $G'_{17}/\langle\rho\rangle \cong G_{17}/\langle\sigma^{2^{n-3}}\rangle$ и $G_{17} \cong G'^{(2^{n-2},\sigma)}_{17}$.

6.1.2 Групите G_{13} и G_{14}

За забележим първо, че $G_{14} = G_{13}^{(4,\lambda)}$. Следователно, ще се концентрираме само на групата G_{13}.

Нека групата $\mathcal{G}$ се поражда от елементи σ, τ, λ и ρ такива, че $\sigma^{2^{n-2}} = \tau^2 = \lambda^2 = \rho^2 = 1, [\tau, \sigma] = \rho, \lambda^{-1}\sigma\lambda = \sigma^{-1}\tau, [\tau, \sigma] = [\lambda, \tau] = 1, \rho$ – централен. Дефинираме $E_4 = \langle\tau, \rho\rangle \cong C_2^2, G = \mathcal{G}/E_4 \cong D_{2^{n-1}}, \mathcal{H} = \langle\sigma^2, \tau, \lambda, \rho\rangle, H = \mathcal{H}/E_4 = \langle\sigma^2, \lambda\rangle \cong D_{2^{n-2}}$. Получаваме сега, че $\mathcal{H}$ лежи в централизатора на E_4 в $\mathcal{G}$ и $\sigma\tau\sigma^{-1} = \tau\rho$.

Означаваме с c_1 2-кокласът в $H^2(G,\mu_2)$, представящ груповото разширение

$$1 \longrightarrow E_4/\langle\rho\rangle \cong \mu_2 \longrightarrow \mathcal{G}/\langle\rho\rangle \cong G_{13} \underset{\substack{\sigma\mapsto\sigma\\ \tau\mapsto\tau}}{\longrightarrow} G \cong D_{2^{n-1}} \longrightarrow 1$$

и с c_2 2-кокласът в $H^2(H,\mu_2)$, представящ груповото разширение

$$1 \longrightarrow E_4/\langle\tau\rangle \cong \mu_2 \longrightarrow \mathcal{H}/\langle\tau\rangle \underset{\substack{\lambda\mapsto\lambda\\ \rho\mapsto\rho}}{\longrightarrow} H \cong D_{2^{n-2}} \longrightarrow 1,$$

където $\mathcal{H}/\langle\tau\rangle$ се поражда от елементи σ^2, λ, ρ такива, че $(\sigma^2)^{2^{n-3}} = \lambda^2 = \rho^2 = 1, \lambda^{-1}\sigma^2\lambda = \sigma^{-2}\rho, \rho$ – централен. Следователно, $\mathcal{H}/\langle\tau\rangle$ е изоморфна на групата G_{13} от ред 2^{n-1}. От теорема 2.3.8 следва, че $c_1 = \mathrm{cor}_{G/H}(c_2)$. Тъй като корестрикцията е транзитивно изображение, по индукция получаваме, че $c_1 = \mathrm{cor}_{G/H_0}(c_0)$, където c_0 е 2-кокласът в $H^2(D_8,\mu_2)$, представящ груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow D \curlywedge C \longrightarrow H_0 \cong D_8 \longrightarrow 1.$$

Препятствието на задачата за вложимост зададена с c_0 и D_8 разширение съдържащо $K(\sqrt{a_1'}, \sqrt{a_2'})/K$ е $(a_1', -1) \in \mathrm{Br}_2(K)$. Прилагайки на всяка стъпка проекционната формула и [Fr, (2.22)], получаваме, че $(a_1, -1)$ е препятствието на задачата за вложимост зададена с c_1 и някое $D_{2^{n-1}}$ разширение, където $F(\sqrt{a_1}, \sqrt{a_2})/F$ се съдържа в това $D_{2^{n-1}}$ разширение.

6.1.3 Групите $G_1, \ldots, G_{12}$ и G_{15}, G_{16}

Ще разгледаме сега групите $G_1 - G_{12}$ и G_{15}, G_{16}. Да забележим първо, че четири от групите са директни произведения: $G_2 \cong Q_{2^{n-1}} \times C_2, G_3 \cong D_{2^{n-1}} \times C_2, G_{10} \cong M_{2^{n-1}} \times C_2, G_{11} \cong SD_{2^{n-1}} \times C_2$. По тази причина ще се фокусираме върху останалите 10 групи.

Нека $M_{2^{n-1}} \times C_2 \cong \langle\sigma,\tau,\rho \mid \sigma^{2^{n-2}} = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^{1+2^{n-3}}, \rho\sigma = \sigma\rho, \rho\tau = \tau\rho\rangle$. Тогава $(M_{2^{n-1}} \times C_2)/\langle\rho\rangle \cong G_1/\langle\tau^2\rangle \cong M_{2^{n-1}}$ и лесно се вижда, че $G_1 = (M_{2^{n-1}} \times C_2)^{(4,\tau)}$. Аналогично, имаме $G_6 = (D_{2^{n-1}} \times C_2)^{(4,\tau)}, G_7 = (SD_{2^{n-1}} \times C_2)^{(4,\tau)}, G_8 = (Q_{2^{n-1}} \times C_2)^{(4,\tau)}$.

Групите G_i за $i = 4, 5, 9, 12, 15, 16$ имат фактор-групи, които са директни про-

изведения:

$$G_4/\langle\sigma^{2^{n-3}}\rangle \cong C_{2^{n-3}} \times C_2^2 = \langle\sigma,\tau,\lambda \mid \sigma^{2^{n-3}} = \tau^2 = \lambda^2 = 1, \sigma\tau = \tau\sigma, \sigma\lambda = \lambda\sigma, \tau\lambda = \lambda\tau\rangle;$$
$$G_5/\langle\tau\rangle \cong C_{2^{n-2}} \times C_2 = \langle\sigma,\lambda \mid \sigma^{2^{n-2}} = \lambda^2 = 1, \sigma\lambda = \lambda\sigma\rangle;$$
$$G_9/\langle\tau^2\rangle \cong C_{2^{n-2}} \times C_2 = \langle\sigma,\tau \mid \sigma^{2^{n-2}} = \tau^2 = 1, \sigma\tau = \tau\sigma\rangle;$$
$$G_{12}/\langle\sigma^{2^{n-3}}\rangle \cong G_{15}/\langle\sigma^{2^{n-3}}\rangle \cong G_{16}/\langle\sigma^{2^{n-3}}\rangle \cong D_{2^{n-2}} \times C_2 = \langle\sigma,\tau,\lambda \mid \sigma^{2^{n-3}} = \tau^2 = \\ = \lambda^2 = 1, \sigma\tau = \tau\sigma, \lambda^{-1}\sigma\lambda = \sigma^{-1}, \tau\lambda = \lambda\tau\rangle.$$

Ще предполагаме отсега нататък, че основното поле F съдържа примитивен корен на единицата ζ от степен 2^{n-3}. От [Fr, (7.10)] следва, че препятствието на влагането на циклично разширение от степен 2^{n-3}, съдържащо квадратичното разширение $F(\sqrt{a_1})$, в циклично разширение от степен 2^{n-2} е $(a_1,\zeta) \in \mathrm{Br}_2(F)$; препятствието на влагането на диедрално разширение от степен 2^{n-2}, съдържащо биквадратичното разширение $F(\sqrt{a}_1,\sqrt{a}_2)$, в диедрално разширение от степен 2^{n-1} е $(a,a_1)(a_2,\zeta) \in \mathrm{Br}_2(F)$ за елемент $a \in F$, който е описан в [Fr, Example 5, (2.22)].

Сега можем да приложим теорема 2.2.1 за да получим препятствията за реализирането на групите G_i за $i = 4,5,9,12,15,16$ като групи на Галоа над F.

Необходимото и достатъчно условие за реализирането на всяка група G_i като група на Галоа над F се състои от две препятствия. Първото препятствие е на задачата за вложимост зададена с $1 \longrightarrow \mu_2 \longrightarrow G_i \longrightarrow G \longrightarrow 1$, а второто е за съществуването на G разширения над F. Записваме тези препятствия в таблица 6.1. Да отбележим, че кватернионните алгебри от вида $(*,-1)$ винаги се разпадат в $\mathrm{Br}_2(k)$ за $n \geq 5$, понеже сме предположили, че $\zeta = \zeta_{2^{n-3}} \in k$. Да забележим още, че в този случай винаги съществуват $C_{2^{n-3}}$ и $D_{2^{n-2}}$ разширения, според [Fr].

Групата G_{26} е изоморфна на $G_{(32,8)}$. Тук C_4 винаги се реализира, така че трябва да добавим само препятствието за реализирането на $D \leftthreetimes C$.

Таблица 6.1: Препятствията, ако $\zeta = \zeta_{2^{n-3}} \in k$

Група	Препятствия
G_1	$(a_2, -1),\ (\zeta^{-1}a_2, a_1)$
G_4	$(a_1, \zeta)(a_2, a_3)$
G_5	$(a_1, a_2),\ (a_1, \zeta)$
G_6	$(a_2, -1),\ (a, a_1)(a_2, \zeta)$
G_7	$(a_2, -1),\ (a, a_1)(a_2, \zeta)$
G_8	$(a_2, -1),\ (a, a_1)(a_2, \zeta)$
G_9	$(a_1, a_2),\ (a_1, \zeta)$
G_{12}	$(a, a_1)(a_2, \zeta)(a_2, a_3)$
G_{13}	$(a_1, -1),\ (a, a_1)(a_2, \zeta)$
G_{14}	$(a_1, -1),\ (a, a_1)(a_2, \zeta)$
G_{15}	$(a, a_1)(a_2, \zeta)(a_1, a_3)$
G_{16}	$(a, a_1)(a_2, \zeta)(a_2a_1, a_3)$
G_{17}	$(a_1, ds\zeta)(a_2, dr)$
G_{26}	$(a_1, 2ds)(a_2, dr),\ (a_1, a_2)$

6.2 Препятствията за групите $G_{18}, \ldots, G_{25}$

Лесно се проверява, че подгрупата $\langle\sigma^2\rangle$ е нормална във всяка една от групите $G_{18}, \ldots, G_{25}$.

Теорема 6.2.1. ([Mi12, Proposition 4.1]) *Нека групата G е изоморфна на някоя от групите G_i за $i = 18, \ldots, 25$, и да означим $A = \langle\sigma^2\rangle$. Нека полето k съдържа примитивен корен на единицата ζ от степен 2^{n-3}, нека $F = G/A$, и нека K/k е разширение на Галоа с група на Галоа F. Задачата за вложимост $(K/k, G, A)$ е подходящо разрешима тогава и само тогава, когато условието за съгласуваност се удовлетворява.*

Доказателство: Нека $G \cong G_{18}$. Действието на F върху A се задава с $(\sigma^2)^\tau = \sigma^2$ и $(\sigma^2)^\lambda = (\sigma^2)^m$ за $m = -1 - 2^{n-4}$. Тъй като k съдържа примитивен корен на единицата от степен 2^{n-3}, действието на F върху групата на характерите $\widehat{A}$ е същото. Очевидно, $m^2 \equiv 1 \pmod{2^{n-3}}$, така че можем да приложим теорема 1.5.2. Следователно, условието за съгласуваност е достатъчно за слабата разрешимост на задачата $(K/k, G, A)$. Да забележим, че A се съдържа в подгрупата на Фратини $\Phi(G) \cong [G, G] \cdot G^2$ на G. Добре известно е, че ако ядрото се съдържа в подгрупата на Фратини на G, то слабата разрешимост води до подходяща разрешимост (виж [ИЛФ, §1.6, Следствие 5]).

Можем да постъпим по същия начин с останалите групи, понеже за всяка група действието на F върху A удовлетворява условията на теорема 1.5.2. $\square$

С помощта на горната теорема, ще намерим необходими и достатъчни условия за реализирането на групите G_i като групи на Галоа над произволно поле k, съдържащо примитивен корен на единицата ζ от степен 2^{n-3}. Тези резултати са получени в статията [Mi12].

6.2.1 Групата G_{18}

Имаме груповото разширение

$$1 \longrightarrow \langle\sigma^2\rangle \longrightarrow G_{18} \xrightarrow{\alpha} F \longrightarrow 1, \tag{6.2}$$

където F е изоморфна на диедралната група D_8 от ред 8, и е породена от елементи x, y със съотношенията $x^4 = y^2 = 1, y^{-1}xy = x^{-1}$, където $\alpha : \sigma \mapsto y, \lambda \mapsto x$.

Нататък, нека K/k е произволно D_8 разширение. Да разгледаме задачата за вложимост $(K/k, G_{18}, \langle\sigma^2\rangle)$ зададена с (6.2) и K/k. Тогава K/k съдържа биквадратично разширение $k(\sqrt{a_1}, \sqrt{a_2})$, където $k(\sqrt{a_2})$ е неподвижното подполе на $\langle x\rangle$. Добре известно е (виж [Le1]), че препятствието за влагането на $k(\sqrt{a_1}, \sqrt{a_2})/k$ в D_8 разширение е $(a_1, a_1a_2) \in \mathrm{Br}(k)$.

Да предположим сега, че $(a_1, a_1a_2) = 1 \in \mathrm{Br}(k)$. Нека $\alpha_1 \in k$ и $\alpha_2 \in k^*$ са такива, че $a_1a_2 = \alpha_1^2 - a_1\alpha_2^2$. Тогава

$$K/k = k(\sqrt{r(\alpha_1 - \alpha_2\sqrt{a_1})}, \sqrt{a_2})/k \tag{6.3}$$

за някое $r \in k^*$. Полагаме $\varphi = \alpha_1 - \alpha_2\sqrt{a_1}$ и $\varphi' = \alpha_1 + \alpha_2\sqrt{a_1}$. Според [Le1, Section 4] можем да считаме, че x и y действат по този начин:

$$\begin{aligned} x &: \sqrt{r\varphi} \mapsto \sqrt{r\varphi'},\ \sqrt{r\varphi'} \mapsto -\sqrt{r\varphi},\ \sqrt{a_2} \mapsto \sqrt{a_2}, \\ y &: \sqrt{r\varphi} \mapsto \sqrt{r\varphi},\ \sqrt{r\varphi'} \mapsto -\sqrt{r\varphi'},\ \sqrt{a_2} \mapsto -\sqrt{a_2}. \end{aligned}$$

Както отбелязахме в края на параграф 1.5, условието за съгласуваност е еквивалентно на разрешимостта на всички съпътстващи Брауерови задачи.

Да разгледаме всички съпътстващи задачи от първи тип. От съотношението $\lambda^{-1}\sigma\lambda = \sigma^{-1}\tau$ получаваме, че има само една брауерова задача от първи тип. Тя се задава от груповото разширение

$$1 \longrightarrow \langle\sigma^2\rangle/\langle\sigma^4\rangle \cong \mu_2 \longrightarrow G_{18}/\langle\sigma^4\rangle \xrightarrow{\alpha} F \longrightarrow 1,$$

където $G_{18}/\langle\sigma^4\rangle$ е изоморфна на $D \leftthreetimes C$ – пулбекът на групите D_8 и C_4. Според [Le1, Example 4.6], препятствието на задачата за вложимост $(K/k, D \leftthreetimes C, \mu_2)$ е $(a_1, -1) \in \mathrm{Br}(k)$. Тъй като $\sqrt{-1}$ е в k, препятствието $(a_1, -1)$ винаги се разпада.

Една съпътстваща брауерова задача от втори тип можем да получим по следния начин. Означаваме с F_1 подгрупата на F, породена от x^2 и y. Да вземем рестрикцията на (6.2):

$$1 \longrightarrow \langle\sigma^2\rangle \longrightarrow \alpha^{-1}(F_1) \xrightarrow{\alpha} F_1 \longrightarrow 1,$$

където $\alpha^{-1}(F_1)$ е подгрупата на G_{18} породена от елементите σ и τ. Имаме съотношенията $\sigma^{2^{n-2}} = \tau^2 = 1$ и $\tau^{-1}\sigma\tau = \sigma^{1+2^{n-3}}$, откъдето $\alpha^{-1}(F_1)$ е изоморфна на модулярната група $M(2^{n-1})$. Да отбележим, че $F_1 = \mathrm{Gal}(K/k(\sqrt{a_1}))$. Според пример 4.3.8, препятствието на задачата за вложимост $(K/k(\sqrt{a_1}), M(2^{n-1}), \langle\sigma^2\rangle)$ е $(\zeta^{-1}a_2, r\varphi) \in \mathrm{Br}(k(\sqrt{a_1}))$.

Останалите брауерови задачи са съпътстващи задачи на тази, която току що разгледахме, понеже тя има най-голямо ядро и най-голяма група F_1. По този начин, получаваме, че групата G_{18} се реализира на k тогава и само тогава, когато съществуват $r, \alpha_1, \alpha_2 \in k$ и квадратично независими $a_1, a_2 \in k$ такива, че $a_1a_2 = \alpha_1^2 - a_1\alpha_2^2$ (т.е., $(a_1, a_2) = 1 \in \mathrm{Br}(k)$) и $(\zeta^{-1}a_2, r\varphi) = 1 \in \mathrm{Br}(k(\sqrt{a_1}))$.

6.2.2 Групата G_{19}

Имаме груповото разширение

$$1 \longrightarrow \langle\sigma^2\rangle \longrightarrow G_{19} \xrightarrow{\alpha} F \longrightarrow 1, \tag{6.4}$$

където F е изоморфна на групата $C_4 \times C_2$, и се поражда от елементи x, y със съотношенията $x^4 = y^2 = 1, y^{-1}xy = x$, където $\alpha : \sigma \mapsto y, \tau \mapsto x$.

Нека K/k е произволно $C_4 \times C_2$ разширение. Да разгледаме сега задачата за вложимост $(K/k, G_{19}, \langle\sigma^2\rangle)$ зададена с (6.4) и K/k. Тогава K/k съдържа биквадратично разширение $k(\sqrt{a_1}, \sqrt{a_2})$, където $k(\sqrt{a_2})$ е неподвижното подполе на $\langle x\rangle$. Добре известно е, че препятствието за влагането на $k(\sqrt{a_1})$ в C_4 разширение е $(a_1, a_1) \in \mathrm{Br}(k)$.

Да предположим сега, че $(a_1, a_1) = 1 \in \mathrm{Br}(k)$. Нека $\beta_1 \in k$ и $\beta_2 \in k^*$ са такива, че $a_1 = \beta_1^2 - a_1\beta_2^2$. Тогава

$$K/k = k(\sqrt{r(\beta_1 - \beta_2\sqrt{a_1})}, \sqrt{a_2})/k$$

за някое $r \in k^*$. Полагаме $\psi = \beta_1 - \beta_2\sqrt{a_1}$ и $\psi' = \beta_1 + \beta_2\sqrt{a_1}$. Според [Le1, Example 3.3] можем да считаме, че x и y действат по този начин:

$$\begin{aligned} x &: \sqrt{r\psi} \mapsto \sqrt{r\psi'},\ \sqrt{r\psi'} \mapsto -\sqrt{r\psi},\ \sqrt{a_2} \mapsto \sqrt{a_2}, \\ y &: \sqrt{r\psi} \mapsto \sqrt{r\psi},\ \sqrt{r\psi'} \mapsto \sqrt{r\psi'},\ \sqrt{a_2} \mapsto -\sqrt{a_2}. \end{aligned}$$

Съпътстващата брауерова задача от първи тип, която има най-голямо ядро се задава с груповото разширение

$$1 \longrightarrow \langle\sigma^2\rangle/\langle\sigma^{2^{n-3}}\rangle \cong C_{2^{n-4}} \longrightarrow G_{19}/\langle\sigma^{2^{n-3}}\rangle \xrightarrow{\alpha} F \longrightarrow 1,$$

където $G_{19}/\langle\sigma^{2^{n-3}}\rangle$ е изоморфна на групата $G_{-1,1}$ от теорема 4.3.16. Имаме груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow G_{-1,1} \longrightarrow M(2^{n-2}) \longrightarrow 1, \tag{6.5}$$

така че трябва да съществува $M(2^{n-2})$ разширение. Препятствието за реализирането на модулярната група от ред 2^{n-2} е $(\zeta^{-2}a_2, a_1) \in \mathrm{Br}(k)$, а препятствието на задачата зададена с (6.5) е $(a_2, -1) \in \mathrm{Br}(k)$, според пример 4.3.8 и теорема 4.3.16, съответно.

Да означим сега с F_1 подгрупата на F породена от x^2 и y. Да вземем рестрикцията на (6.4):

$$1 \longrightarrow \langle\sigma^2\rangle \longrightarrow \alpha^{-1}(F_1) \xrightarrow{\alpha} F_1 \longrightarrow 1,$$

където $\alpha^{-1}(F_1)$ е подгрупата на G_{19} породена от елементите σ и $\tau_1 = \tau^2$. Имаме съотношенията $\sigma^{2^{n-2}} = \tau_1^2 = 1$ и $\tau_1^{-1}\sigma\tau_1 = \sigma^{1+2^{n-3}}$, откъдето $\alpha^{-1}(F_1)$ е изоморфна на модулярната група $M(2^{n-1})$. Да забележим, че $F_1 = \mathrm{Gal}(K/k(\sqrt{a_1}))$. Според пример 4.3.8, препятствието на брауеровата задача $(K/k(\sqrt{a_1}), M(2^{n-1}), \langle\sigma^2\rangle)$ е $(\zeta^{-1}a_2, r\psi) \in \mathrm{Br}(k(\sqrt{a_1}))$.

6.2.3 Групата G_{20}

Имаме груповото разширение

$$1 \longrightarrow \langle\sigma^2\rangle \longrightarrow G_{20} \xrightarrow{\alpha} F \longrightarrow 1, \tag{6.6}$$

където F е изоморфна на групата $C_4 \times C_2$, и се поражда от елементи x, y със съотношения $x^4 = y^2 = 1, y^{-1}xy = x$, където $\alpha : \sigma \mapsto y, \tau \mapsto x$.

Нататък, да разгледаме произволна задача за вложимост $(K/k, G_{20}, \langle\sigma^2\rangle)$ зададена с (6.6), където K/k е $C_4 \times C_2$ разширение.

Съпътстващата брауерова задача от първи тип е единствена и тя се задава с груповото разширение

$$1 \longrightarrow \langle\sigma^2\rangle/\langle\sigma^4\rangle \cong \mu_2 \longrightarrow G_{20}/\langle\sigma^4\rangle \xrightarrow{\alpha} F \longrightarrow 1,$$

където $G_{20}/\langle\sigma^4\rangle$ е изоморфна на групата $Q \leftthreetimes C$ – пулбекът на Q_8 и C_4. Според [Le1, Example 4.5], препятствието на задачата $(K/k, Q \leftthreetimes C, \mu_2)$ е $(a_1, a_2) \in \mathrm{Br}(k)$.

Да означим сега с F_1 подгрупата на F породена от x^2 и y. Да вземем рестрикцията на (6.6):

$$1 \longrightarrow \langle\sigma^2\rangle \longrightarrow \alpha^{-1}(F_1) \xrightarrow{\alpha} F_1 \longrightarrow 1,$$

където $\alpha^{-1}(F_1)$ е подгрупата на G_{20} породена от елементи σ и $\tau_1 = \tau^2$. Имаме съотношенията $\sigma^{2^{n-2}} = \tau_1^2 = 1$ и $\tau_1^{-1}\sigma\tau_1 = \sigma^{1+2^{n-3}}$, откъдето $\alpha^{-1}(F_1)$ е изоморфна на модулярната група $M(2^{n-1})$. Следователно, препятствието на брауеровата задача от втори тип е същото както за групата G_{19}.

6.2.4 Групата G_{21}

Имаме груповото разширение

$$1 \longrightarrow \langle\sigma^2\rangle \longrightarrow G_{21} \xrightarrow{\alpha} F \longrightarrow 1, \tag{6.7}$$

където F е изоморфна на диедралната група D_8 от ред 8, и се поражда от елементи x, y със съотношения $x^4 = y^2 = 1, y^{-1}xy = x^{-1}$, където $\alpha : \sigma \mapsto y, \tau \mapsto x$. Нека K/k е D_8 разширение, зададено с (6.3). Тъй като $\sigma^{-2}\tau\sigma^2 = \tau$, задачата $(K/k, G_{21}, \langle\sigma^2\rangle)$ е брауерова.

Означаваме с Γ алгебрата на кръстосаното произведение представляваща препятствието на брауеровата задача $(K/k, G_{21}, \langle\sigma^2\rangle)$. Тогава Γ се поражда над k от елементите на K и елементи u_x, u_y такива, че $u_x a = x(a)u_x, u_y b = y(b)u_y$ за $a, b \in K$, и $u_x^4 = -1, u_y^2 = \zeta, u_y^{-1}u_x u_y = u_x^{-1}$.

Нека $\mathcal{A}$ е подалгебрата на Γ породена над k от елементите u_y и $\sqrt{a_2}$. Очевидно, $\mathcal{A}$ е изоморфна на кватернионната алгебра (ζ, a_2). Тогава Γ е изоморфна на $\mathcal{A} \otimes C_\Gamma(\mathcal{A})$, където $C_\Gamma(\mathcal{A})$ е централизаторът на $\mathcal{A}$ в Γ.

Нека $\mathcal{B}$ е подалгебрата на Γ породена над k от елементите $u_x + u_x^{-1}$ и $\sqrt{a_1}$. Тъй като $u_x^{-2} = -u_x^2$, получаваме, че $\mathcal{B}$ е изоморфна на кватернионната алгебра $(2, a_1)$. Съотношението $u_x u_y = u_y u_x^{-1}$ показва, че $\mathcal{B}$ се съдържа в $C_\Gamma(\mathcal{A})$. Следователно, $\Gamma \cong \mathcal{A} \otimes \mathcal{B} \otimes C_\Gamma(\mathcal{A} \otimes \mathcal{B})$.

Да дефинираме сега $w = \sqrt{r\varphi} + \sqrt{r\varphi'}u_x^2$. От съотношенията $u_x^2 u_y = -u_y u_x^2$, $u_y\sqrt{r\varphi} = \sqrt{r\varphi}u_y$ и $u_y\sqrt{r\varphi'} = -\sqrt{r\varphi'}$ следва, че $w \in C_\Gamma(\mathcal{A})$. Имаме също така $u_x w = wu_x^{-1}$ и $u_x^{-1}w = wu_x$, значи $w \in C_\Gamma(\mathcal{A}\otimes\mathcal{B})$. Аналогично, елементът $\sqrt{a_2}u_x^2$ се съдържа в $C_\Gamma(\mathcal{A}\otimes\mathcal{B})$. Нека $\mathcal{C}$ е подалгебрата на Γ породена над k от елементите w и $\sqrt{a_2}u_x^2$. Не е трудно да се установи, че $\mathcal{C}$ е изоморфна на кватернионната алгебра $(-a_2, 2r\alpha_1)$.

Следователно, Γ е изоморфна на произведението на кватернионните алгебри $(\zeta, a_2)(2, a_1)(-a_2, 2r\alpha_1)$. Тъй като $\zeta \in k$ е примитивен корен на единицата от степен 2^{n-3} $(n \geq 6)$, полето k съдържа примитивен 8-ми корен на единицата и препятствието е еквивалентно на кватернионната алгебра $(a_2, r\alpha_1\zeta) \in \mathrm{Br}(k)$.

6.2.5 Групата G_{22}

Имаме груповото разширение

$$1 \longrightarrow \langle\sigma^2\rangle \longrightarrow G_{22} \xrightarrow{\alpha} F \longrightarrow 1, \tag{6.8}$$

където F е изоморфна на диедралната група D_8 от ред 8, и се поражда от елементи x, y със съотношения $x^4 = y^2 = 1, y^{-1}xy = x^{-1}$, където $\alpha : \sigma \mapsto y, \sigma\lambda \mapsto x$. Нека K/k е D_8 разширение както в (6.3).

Съпътстващата брауерова задача от първи тип, която има най-голямо ядро се задава с груповото разширение

$$1 \longrightarrow \langle\sigma^2\rangle/\langle\sigma^{2^{n-3}}\rangle \cong C_{2^{n-4}} \longrightarrow G_{22}/\langle\sigma^{2^{n-3}}\rangle \xrightarrow{\alpha} F \longrightarrow 1,$$

където $G_{22}/\langle\sigma^{2^{n-3}}\rangle$ е изоморфна на групата $\widetilde{M}(2^{n-2})$ от теорема 4.3.15. Тогава имаме груповото разширение

$$1 \longrightarrow \mu_2 \longrightarrow \widetilde{M}(2^{n-2}) \longrightarrow M(2^{n-2}) \longrightarrow 1, \tag{6.9}$$

така че първо трябва да съществува $M(2^{n-2})$ разширение. Препятствието за реализирането на модулярната група от ред 2^{n-2} е $(\zeta^{-2}a_2, a_1) \in \mathrm{Br}(k)$, а препятствието на задачата, съответстваща на (6.9) е $(a_2, a_1) \in \mathrm{Br}(k)$, според пример 4.3.9 и теорема 4.3.15, съответно.

Да означим сега с F_1 подгрупата на F породена от x^2 и y. Да вземем рестрикцията на (6.8):

$$1 \longrightarrow \langle\sigma^2\rangle \longrightarrow \alpha^{-1}(F_1) \xrightarrow{\alpha} F_1 \longrightarrow 1,$$

където $\alpha^{-1}(F_1)$ е подгрупата на G_{22} породена от елементите σ и τ. Очевидно, $\alpha^{-1}(F_1)$ е изоморфна на групата $C_{2^{n-2}} \times C_2$. Да забележим, че $F_1 = \mathrm{Gal}(K/k(\sqrt{a_1}))$. Добре известно е, че препятствието на брауеровата задача $(K/k(\sqrt{a_1}), C_{2^{n-2}} \times C_2, \langle\sigma^2\rangle)$ е $(a_2, \zeta) \in \mathrm{Br}(k(\sqrt{a_1}))$.

6.2.6 Групата G_{23}

Имаме груповото разширение

$$1 \longrightarrow \langle\sigma^2\rangle \longrightarrow G_{23} \xrightarrow{\alpha} F \longrightarrow 1, \tag{6.10}$$

където F е изоморфна на диедралната група D_8 и се поражда от елементи x, y със съотношения $x^4 = y^2 = 1, y^{-1}xy = x^{-1}$, където $\alpha : \sigma \mapsto y, \sigma\lambda \mapsto x$. Нека K/k е D_8 разширение както в (6.3).

Има само една съпътстваща брауерова задача от първи тип, която се задава с груповото разширение

$$1 \longrightarrow \langle\sigma^2\rangle/\langle\sigma^4\rangle \cong \mu_2 \longrightarrow G_{23}/\langle\sigma^4\rangle \xrightarrow{\alpha} F \longrightarrow 1,$$

където $G_{23}/\langle\sigma^4\rangle$ е изоморфна на пулбека $D \curlywedge C$.

Съпътстващата брауерова задача от втори тип е еквивалентна на съответната задача за групата G_{22}, именно $(K/k(\sqrt{a_1}), C_{2^{n-2}} \times C_2, \langle\sigma^2\rangle)$.

6.2.7 Групите G_{24} и G_{25}

Двете групи имат идентични Брауерови задачи, така че ще опишем препятствията само на групата G_{24}. Имаме груповото разширение

$$1 \longrightarrow \langle\sigma^2\rangle \longrightarrow G_{24} \xrightarrow{\alpha} F \longrightarrow 1, \tag{6.11}$$

където F е изоморфна на групата C_2^3, и се поражда от елементи x, y, z такива, че $\alpha : \sigma \mapsto x, \tau \mapsto y, \lambda \mapsto z$. Тогава всяко C_2^3 разширение K/k има вида

$$K/k = k(\sqrt{a_1}, \sqrt{a_2}, \sqrt{a_3})/k, \tag{6.12}$$

и можем да предполагаме, че x, y и z действат по този начин:

$$\begin{aligned}
x &: \sqrt{a_1} \mapsto -\sqrt{a_1},\ \sqrt{a_2} \mapsto \sqrt{a_2},\ \sqrt{a_3} \mapsto \sqrt{a_3},\\
y &: \sqrt{a_1} \mapsto \sqrt{a_1},\ \sqrt{a_2} \mapsto -\sqrt{a_2},\ \sqrt{a_3} \mapsto \sqrt{a_3},\\
z &: \sqrt{a_1} \mapsto \sqrt{a_1},\ \sqrt{a_2} \mapsto \sqrt{a_2},\ \sqrt{a_3} \mapsto -\sqrt{a_3}.
\end{aligned}$$

Има само една съпътстваща брауерова задача от първи тип, която се задава с груповото разширение

$$1 \longrightarrow \langle\sigma^2\rangle/\langle\sigma^4\rangle \cong \mu_2 \longrightarrow G_{24}/\langle\sigma^4\rangle \xrightarrow{\alpha} F \longrightarrow 1,$$

където $G_{24}/\langle\sigma^4\rangle$ е изоморфна на групата $D_8 \times C_2$.

Да означим сега с F_1 подгрупата на F породена от x и y. Да вземем рестрикцията на (6.11):

$$1 \longrightarrow \langle\sigma^2\rangle \longrightarrow \alpha^{-1}(F_1) \xrightarrow{\alpha} F_1 \longrightarrow 1,$$

където $\alpha^{-1}(F_1)$ е подгрупата на G_{24} породена от елементите σ и τ. Очевидно, $\alpha^{-1}(F_1)$ е изоморфна на модулярната група $M(2^{n-1})$. Да забележим, че $F_1 = \mathrm{Gal}(K/k(\sqrt{a_3}))$. Според пример 4.3.9, препятствието на брауеровата задача $(K/k(\sqrt{a_3}), M(2^{n-1}), \langle\sigma^2\rangle)$ е $(\zeta^{-1}a_2, a_1) \in \mathrm{Br}(k(\sqrt{a_3}))$.

Накрая, ще резюмираме получените препятствия за групите $G_{18} - G_{25}$ в следната таблица.

Таблица 6.2: Препятствията, ако $\zeta = \zeta_{2^{n-3}} \in F$

Група	Препятствия
G_{18}	$(a_1, a_2) \in \mathrm{Br}(k),\ (\zeta^{-1}a_2, r\varphi) \in \mathrm{Br}(k(\sqrt{a_1}))$
G_{19}	$(a_1, a_2) \in \mathrm{Br}(k),\ (\zeta^{-1}a_2, r\psi) \in \mathrm{Br}(k(\sqrt{a_1}))$
G_{20}	$(a_1, a_2) \in \mathrm{Br}(k),\ (\zeta^{-1}a_2, r\psi) \in \mathrm{Br}(k(\sqrt{a_1}))$
G_{21}	$(a_1, a_2) \in \mathrm{Br}(k),\ (a_2, r\alpha_1\zeta) \in \mathrm{Br}(k)$
G_{22}	$(a_1, a_2) \in \mathrm{Br}(k),\ (a_2, \zeta) \in \mathrm{Br}(k(\sqrt{a_1}))$
G_{23}	$(a_1, a_2) \in \mathrm{Br}(k),\ (a_2, \zeta) \in \mathrm{Br}(k(\sqrt{a_1}))$
G_{24}	$(a_1, a_2) \in \mathrm{Br}(k),\ (\zeta^{-1}a_2, a_1) \in \mathrm{Br}(k(\sqrt{a_3}))$
G_{25}	$(a_1, a_2) \in \mathrm{Br}(k),\ (\zeta^{-1}a_2, a_1) \in \mathrm{Br}(k(\sqrt{a_3}))$

6.3 Приложение на препятствията за ньотеровата задача

Нека K е поле и G е крайна група. Нека G действа на рационалното функционално поле $K(x_g : g \in G)$ чрез K автоморфизми така: $g \cdot x_h = x_{gh}$ за произволни $g, h \in G$. Означаваме с $K(G)$ неподвижното подполе $K(x_g : g \in G)^G = \{f \in K(x_g : g \in G) \mid \sigma \cdot f = f, \forall\sigma \in G\}$. Ньотеровата задача тогава се състои в това дали $K(G)$ е рационално (= чисто трансцедентно) над K.

Основните резултати относно ньотеровата задача за абелови групи могат да се намерят в статията [Swan]. Наскоро, ньотеровата задача за някои неабелови p-групи беше изследвана в работи като [CHK, CHPK, HK, Ka1, Ka2, Ka3].

В този параграф ще предложим един нов подход към ньотеровата задача, който наподобява обобщението на обратната задача в теорията на Галоа – задачата за вложимост на полета. Нека K е поле и да разгледаме произволно групово разширение

$$1 \longrightarrow A \longrightarrow H \underset{\pi}{\longrightarrow} G \longrightarrow 1. \tag{6.13}$$

Тогава можем да гледаме на $K(G)$ като на подполе на $K(H)$ чрез естественото включване произтичащо от регулярното действие на G върху A-неподвижните елементи в регулярното представяне на H. Дефинираме *ньотеровата задача за вложимост* като даване на отговор на въпроса дали $K(H)$ е рационално над $K(G)$.

По този начин, ако знаем, че $K(G)$ е рационално над K и ако успеем да дадем положителен отговор на ньотеровата задача за вложимост, ще получим рационалността на $K(H)$ над K. Да отбележим, обаче, че рационалността на $K(G)$ над K не е необходима за рационалността на $K(H)$ над K. Наистина, известно е, че междинно поле на чисто трансцедентно разширение не винаги е чисто трансцедентно.

Ньотеровата задача за вложимост не винаги е разрешима, както се вижда например, ако $K = \mathbb{Q}, G = C_4$ и $H = C_8$ [Sa1, Th. 5.11].

Нека отново с $\mathrm{Br}(K)$ да означим групата на Брауер на полето K, и с $\mathrm{Br}_N(K)$ нейната N-торзия за произволно $N > 1$. Следвайки Рокет [Ro], ако $\gamma = [B] \in \mathrm{Br}(K)$ е класът на K-централна проста алгебра B и $m \geq 1$ е кратно на индекса на B, то с $k_m(\gamma)$ ще означаваме m-тото поле на Брауер на γ. Нещо повече, $k_m(\gamma)/K$ е регулярно разширение от степен на трансцедентност $m-1$, което е рационално тогава и само тогава, когато класът γ е тривиален (т.е. B се разпада). Следният резултат в същината си е получен от Солтман в [Sa2, p. 541], но е доказан детайлно от Б. Планс [Pl, Prop. 7].

Теорема 6.3.1. *Нека* $1 \longrightarrow C \longrightarrow H \longrightarrow G \longrightarrow 1$ *е централно групово разширение, на което съответства елемента* $\varepsilon \in H^2(G, C)$. *Нека* K *е безкрайно поле и да означим с* N *експонентата на* C. *Да предположим, че* N *е взаимно просто с характеристиката на* K *и че* K *съдържа* μ_N *– групата на* N*-тите корени на единицата. Нека е дадено разлагането* $C \cong \mu_{N_1} \times \cdots \times \mu_{N_r}$, *и нека съответният изоморфизъм*

$H^2(G,C) \cong \oplus_i H^2(G,\mu_{N_i})$ *изобразява* ε *в* $(\varepsilon)_i$. *Нека също е дадено подпредставяне* V *на регулярното представяне на* G *над* K, *и нека* $\gamma_i \in \mathrm{Br}_N(K(V)^G) \subset \mathrm{Br}(K(V)^G)$ *е инфлацията на* ε_i *по отношение на изоморфизма* $G \cong \mathrm{Gal}(K(V)/K(V)^G)$. *Тогава*

$K(H)$ *е рационално над* $K(V)^G -$ *свободният композит* $k_m(\gamma_1)\cdots k_m(\gamma_r)$,

където m *е реда на* G.

Следващият резултат представлява едно интересно приложение на теорията на препятствията при решаване на ньотеровата задача.

Теорема 6.3.2. ([Mi11, Theorem 2.7]) *Нека* p *е просто, нека* K *е безкрайно поле с характеристика различна от* p, *и нека* K *съдържа всички* p*-ти корени на единицата. Нека* $1 \longrightarrow \mu_p \longrightarrow H \longrightarrow G \longrightarrow 1$ *е неразцепимо централно разширение на крайни групи, на което съответства елемента* $\varepsilon \in H^2(G,\mu_p)$. *Нека* $L = K(x_g : g \in G)$ *е рационалното функционално поле с* G*-действие, зададено от регулярното представяне на* G *над* K. *Да предположим, че задачата за вложимост зададена с* $L/K(G)$ *и груповото разширение* $1 \longrightarrow \mu_p \longrightarrow H \longrightarrow G \longrightarrow 1$ *е разрешима. Тогава* $K(H)$ *е рационално над* $K(G)$.

Доказателство: Препятствието $i(\varepsilon) \in \mathrm{Br}_p(K(G))$ е изоморфно на алгебрата на кръстосаното произведение $[L,G,\varepsilon]$, която се разпада в $\mathrm{Br}_p(K(V)^G)$, понеже задачата за вложимост е разрешима. Следователно, $k_m(i(\varepsilon))$ е рационално над $K(G)$, така че от теорема 6.3.1 получаваме нашия резултат. □

Сега ще използваме горната теорема за да дадем положителен отговор на ньотеровата задача за някои от групите, описани в началото на тази глава.

Теорема 6.3.3. ([Mi11, Theorem 5.5]) *Нека* K *е безкрайно поле с* $char(K) \neq 2$, *което съдържа примитивен корен на единицата* ζ *от степен* 2^{n-3} *за* $n \geq 5$. *Тогава* $K(G_i)$ *е рационално над* K *за* $i = 1,6,7,8,13,14$.

Доказателство: Да забележим, че имаме следните изоморфизми: $G_1/\langle\tau^2\rangle \cong M_{2^{n-1}}, G_6/\langle\tau^2\rangle \cong D_{2^{n-1}}, G_7/\langle\tau^2\rangle \cong SD_{2^{n-1}}, G_8/\langle\tau^2\rangle \cong Q_{2^{n-1}}, G_{13}/\langle\tau\rangle \cong D_{2^{n-1}}, G_{14}/\langle\tau\rangle \cong Q_{2^{n-1}}$.

Нека групата H е изоморфна на някоя от групите $M_{2^{n-1}}, D_{2^{n-1}}, SD_{2^{n-1}}, Q_{2^{n-1}}$, и нека $L/k = K(x_h : h \in H)/K(H)$ е H разширението, получено с помощта на рационалното функционално поле $K(x_h : h \in H)$.

От таблица 6.1 се вижда, че препятствието на задачата за вложимост, зададена с L/k и груповото разширение $1 \longrightarrow \mu_2 \longrightarrow G_i \longrightarrow H \longrightarrow 1$ е $(*,-1) \in \mathrm{Br}(K(H))$ за $i = 1, 6, 7, 8, 13, 14$. Да отбележим, че K съдържа примитивен четвърти корен на единицата, значи препятствието $(*,-1)$ винаги се разпада. Тогава теорема 6.3.2 ни дава рационалността на $K(G_i)$ над K, понеже $K(H)$ е рационално над K, както е известно от [НК]. $\square$

В доказателството на теорема 6.3.3 видяхме примери на задачи за вложимост притежаващи препятствия от вида $(*,-1)$. Предстои ни да дефинираме едно групово разширение, което обобщава тези случаи.

Нека G е крайна група, и нека $\{\sigma_1, \ldots, \sigma_k\}$ е фиксирано (не непременно минимално) пораждащо множество на G със следните свойства: $|\sigma_1| = p$, подгрупата H породена от $\sigma_2, \ldots, \sigma_k$ е нормална в G, и фактор-групата G/H е изоморфна на цикличната група C_p, т.е., $\sigma_1^i \notin H, 1 \leq i < p$. Да вземем груповото разширение

$$1 \longrightarrow \mu_p \longrightarrow \widetilde{G} \underset{\pi}{\longrightarrow} G \longrightarrow 1. \tag{6.14}$$

Да означим със $\widetilde{\sigma}_i = \pi^{-1}(\sigma_i)$ произволен про-образ на σ_i в $\widetilde{G}$ за $i = 1, \ldots k$. Да предположим, че $\widetilde{\sigma}_1^p \in \mu_p, \widetilde{\sigma}_1^p \neq 1$ и всички останали съотношения между пораждащите на групите G и $\widetilde{G}$ са идентични, т.е., $\widetilde{\sigma}_i^{\alpha_i} = \prod_{j\neq 1} \widetilde{\sigma}_j^{\beta_j} \iff \sigma_i^{\alpha_i} = \prod_{j\neq 1} \sigma_j^{\beta_j}$ за $i = 2, 3, \ldots, k$; $\alpha_i, \beta_j \in \mathbb{Z}$; и $[\widetilde{\sigma}_i, \widetilde{\sigma}_j] = \prod_{s\neq 1} \widetilde{\sigma}_s^{\varepsilon_s} \iff [\sigma_i, \sigma_j] = \prod_{s\neq 1} \sigma_s^{\varepsilon_s}$ за $i, j = 1, 2, \ldots, k; \varepsilon_s \in \mathbb{Z}$.

Сега ще докажем следната теорема, която може бъде получена и като следствие от теорема 2.2.4. Накрая, ще докажем и две следствия, касаещи ньотеровата задача.

Теорема 6.3.4. *Нека K е поле с характеристика различна от p, което съдържа примитивен p-ти корен на единицата ζ. Нека групите G и $\widetilde{G}$ са както по-горе, нека L/K е крайно разширение на Галоа с група на Галоа $G = \mathrm{Gal}(L/K)$, и нека $E = L^H = K(\sqrt[p]{b})$ е неподвижното подполе на H. Тогава препятствието на задачата за вложимост зададена с L/K и (6.14) е $(b, \zeta; \zeta) \in \mathrm{Br}_p(K)$.*

Доказателство: Да означим с $\Gamma_1 = (L, G, f_1)$ алгебрата на кръстосаното произведение представяща груповото разширение $1 \longrightarrow \mu_p \longrightarrow \mu_p \times G \longrightarrow G \longrightarrow 1$, и с $\Gamma_2 = (L, G, f_2)$ алгебрата на кръстосаното произведение представяща груповото разширение $1 \longrightarrow \mu_p \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$. Да забележим, че Γ_1 се разпада. Тя се поражда над K от елементите на L и елементите $\{u_\sigma\}_{\sigma\in G}$, където $u_1 = f_1(1,1) = 1, u_\sigma x = \sigma x u_\sigma$

и $u_\sigma u_\tau = u_{\sigma\tau} f_1(\sigma,\tau)$. Цикличната алгебра A породена от елементите на E и елементите $u^i_{\sigma_1} = u_{\sigma_1^i}, i = 1,\dots,p$, се съдържа в Γ_1 и $u^p_{\sigma_1} = u_1 = 1$. Тогава $\Gamma_1 = A \otimes_K C_{\Gamma_1}(A)$. Да забележим, че A също се разпада, понеже тя е алгебрата на кръстосаното произведение представяща груповото разширение $1 \longrightarrow \mu_p \longrightarrow \mu_p \times C_p \longrightarrow C_p \longrightarrow 1$. Следователно, $C_{\Gamma_1}(A)$ също се разпада.

Нататък, Γ_2 се поражда над K от елементите на L и $\{v_\sigma\}_{\sigma\in G}$, където $v_1 = f_2(1,1) = 1, v_\sigma x = \sigma x v_\sigma$ и $v_\sigma v_\tau = v_{\sigma\tau} f_2(\sigma,\tau)$. Цикличната алгебра B породена от елементите на E и елементите $v^i_{\sigma_1} = v_{\sigma_1^i}, i = 1,\dots,p-1$, се съдържа в Γ_2. Тук, обаче $v^p_{\sigma_1} = \zeta^l \neq 1$, където $\widetilde{\sigma}^p_1 = \zeta^l$. Тогава аналогично на Γ_1, имаме $\Gamma_2 = B \otimes_K C_{\Gamma_2}(B)$. От свойствата на съотношенията между пораждащите на G и $\widetilde{G}$ следва, че $[C_{\Gamma_2}(A)] = [C_{\Gamma_2}(B)] = 1 \in \mathrm{Br}_p(K)$. Накрая, $[B] = (b, \zeta; \zeta)$, понаже B е алгебрата на кръстосаното произведение представяща груповото разширение $1 \longrightarrow \mu_p \longrightarrow C_{p^2} \longrightarrow C_p \longrightarrow 1$ (виж параграф 2.1, задачата зададена с (2.2)). □

Следствие 6.3.5. *Нека p е просто число и нека K е безкрайно поле с характеристика различна от p, което съдържа всички корени на единицата от степен p^2. Нека групите G и $\widetilde{G}$ са според описанието дадено след груповото разширение* (6.14). *Нека $L = K(x_g : g \in G)$ е рационално функционално поле с G-действие зададено с регулярното представяне на G над K. Тогава $K(\widetilde{G})$ е рационално над $K(G)$.*

Доказателство: Нека $\zeta \in K$ е примитивен p-ти корен на единицата. Препятствието на задачата за вложимост зададена с $L/K(G)$ и груповото разширение $1 \longrightarrow \mu_p \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$ е от вида $(*, \zeta; \zeta) \in \mathrm{Br}_p(K(G))$. Това препятствие винаги се разпада, понеже K съдържа примитивен корен на единицата от степен p^2. От теорема 6.3.2 сега следва нашият резултат. □

Следствие 6.3.6. *Нека p е просто число, $n \geq 4$ е естествено число и нека K е безкрайно поле с $char(K) \neq p$, което съдържа примитивен корен на единицата ζ от степен p^{n-2}. Тогава $K(G_{\zeta,1})$ е рационално над K където $G_{\zeta,1} \cong \langle x, y \mid x^{p^{n-1}} = y^{p^2} = 1, y^p - $ централен, $yx = x^{q+1}y\rangle$ е групата дефинирана в теорема 4.3.16.*

Доказателство: Според [НК] полето $K(M(p^n))$ е рационално над K. От теорема 4.3.16 (или 6.3.4) следва, че препятствието на задачата за вложимост зададена с груповото разширение $1 \longrightarrow \mu_p \longrightarrow G_{\zeta,1} \longrightarrow M(p^n) \longrightarrow 1$ е $(*, \zeta; \zeta) \in \mathrm{Br}_p(K(G))$. Тъй като K съдържа примитивен корен на единицата от степен p^2, това препятствие винаги се разпада и можем да приложим теорема 6.3.2. □

ПРИЛОЖЕНИЕ: Групи от ред 32

Група	Съотношения	Център	Ранг	Експ.
G_1	$a_1^2a_2^{-1}, a_2^2a_3^{-1}, a_3^2a_4^{-1}, a_4^2a_5^{-1}, a_5^2$	G_1	1	32
G_2	$a_1^2a_4^{-1}, a_2^2a_5^{-1}, [a_2,a_1]a_3^{-1}, a_3^2,$ a_4^2, a_5^2	$\langle a_3, a_4, a_5\rangle$	2	4
G_3	$a_1^2a_3^{-1}, a_2^2a_4^{-1}, a_3^2a_5^{-1}, a_4^2, a_5^2$	G_3	2	8
G_4	$a_1^2a_3^{-1}, a_2^2a_4^{-1}, [a_2,a_1]a_5^{-1}, a_3^2a_5^{-1},$ a_4^2, a_5^2	$\langle a_3, a_4, a_5\rangle$	2	8
G_5	$a_1^2a_4^{-1}, a_2^2, [a_2,a_1]a_3^{-1}, a_3^2, a_4^2a_5^{-1},$ a_5^2	$\langle a_3, a_4, a_5\rangle$	2	8
G_6	$a_1^2a_4^{-1}, a_2^2, [a_2,a_1]a_3^{-1}, a_3^2,$ $[a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2, [a_4,a_1],$ $[a_4,a_2]a_5^{-1}, [a_4,a_3], a_5^2$	$\langle a_5\rangle$	2	8
G_7	$a_1^2a_4^{-1}, a_2^2, [a_2,a_1]a_3^{-1}, a_3^2,$ $[a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2a_5^{-1}$ $[a_4,a_1], [a_4,a_2]a_5^{-1}, [a_4,a_3], a_5^2$	$\langle a_5\rangle$	2	8
G_8	$a_1^2a_4^{-1}, a_2^2a_5^{-1}, [a_2,a_1]a_3^{-1},$ $a_3^2, [a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2a_5^{-1},$ $[a_4,a_1], [a_4,a_2]a_5^{-1}, [a_4,a_3], a_5^2$	$\langle a_5\rangle$	2	8
G_9	$a_1^2a_4^{-1}, a_2^2, [a_2,a_1]a_3^{-1}, a_3^2a_5^{-1},$ $[a_3,a_1]a_5^{-1}, a_4^2, a_5^2$	$\langle a_4, a_5\rangle$	2	8
G_{10}	$a_1^2a_4^{-1}, a_2^2a_5^{-1}, [a_2,a_1]a_3^{-1},$ $a_3^2a_5^{-1}, [a_3,a_1]a_5^{-1}, [a_3,a_2]a_5^{-1},$ a_4^2, a_5^2	$\langle a_4, a_5\rangle$	2	8
G_{11}	$a_1^2a_4^{-1}, a_2^2, [a_2,a_1]a_3^{-1}, a_3^2a_5^{-1},$ $[a_3,a_1]a_5^{-1}, [a_3,a_2]a_5^{-1}, a_4^2a_5^{-1},$ a_5^2	$\langle a_4, a_5\rangle$	2	8
G_{12}	$a_1^2a_4^{-1}, a_2^2a_3^{-1}, [a_2,a_1]a_3^{-1}, a_3^2,$ $a_4^2a_5^{-1}, a_5^2$	$\langle a_3, a_4, a_5\rangle$	2	8
G_{13}	$a_1^2a_4^{-1}, a_2^2a_3^{-1}, [a_2,a_1]a_3^{-1},$ $a_3^2a_5^{-1}, [a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2,$ a_5^2	$\langle a_4, a_5\rangle$	2	8
G_{14}	$a_1^2a_4^{-1}, a_2^2a_5^{-1}a_3^{-1}, [a_2,a_1]a_3^{-1},$ $a_3^2a_5^{-1}, [a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2,$ a_5^2	$\langle a_4, a_5\rangle$	2	8
G_{15}	$a_1^2a_4^{-1}, a_2^2a_3^{-1}, [a_2,a_1]a_3^{-1},$ $a_3^2a_5^{-1}, [a_3,a_1]a_5^{-1}, [a_3,a_2],$ $a_4^2a_5^{-1}, a_5^2$	$\langle a_4, a_5\rangle$	2	8
G_{16}	$a_1^2a_3^{-1}, a_2^2, a_3^2a_4^{-1}, a_4^2a_5^{-1}, a_5^2$	G_{16}	2	16
G_{17}	$a_1^2a_3^{-1}, a_2^2, [a_2,a_1]a_5^{-1}, a_3^2a_4^{-1},$ $a_4^2a_5^{-1}, a_5^2$	$\langle a_3, a_4, a_5\rangle$	2	16

Група	Съотношения	Център	Ранг	Експ.
G_{18}	$a_1^2, a_2^2, [a_2,a_1]a_3^{-1}, a_3^2a_5^{-1}a_4^{-1}, [a_3,a_1]a_4^{-1}, [a_3,a_2]a_4^{-1}, a_4^2a_5^{-1}, [a_4,a_1]a_5^{-1}, [a_4,a_2]a_5^{-1}, [a_4,a_3], a_5^2$	$\langle a_5\rangle$	2	16
G_{19}	$a_1^2a_5^{-1}, a_2^2, [a_2,a_1]a_3^{-1}, a_3^2a_5^{-1}a_4^{-1}, [a_3,a_1]a_4^{-1}, [a_3,a_2]a_4^{-1}, a_4^2a_5^{-1}, [a_4,a_1]a_5^{-1},]a_4,a_3], a_5^2$	$\langle a_5\rangle$	2	16
G_{20}	$a_1^2a_5^{-1}, a_2^2a_5^{-1}, [a_2,a_1]a_3^{-1}, a_3^2a_5^{-1}a_4^{-1}, [a_3,a_1]a_4^{-1}, [a_3,a_2]a_4^{-1}, a_4^2a_5^{-1}, [a_4,a_1]a_5^{-1}, [a_4,a_2]a_5^{-1}, [a_4,a_3], a_5^2$	$\langle a_5\rangle$	2	16
G_{21}	$a_1^2a_4^{-1}, a_2^2a_5^{-1}, a_3^2, a_4^2, a_5^2$	G_{21}	3	4
G_{22}	$a_1^2a_5^{-1}, a_2^2, [a_2,a_1]a_4^{-1}, a_3^2, a_4^2, a_5^2$	$\langle a_3,a_4,a_5\rangle$	3	4
G_{23}	$a_1^2a_5^{-1}, a_2^2a_4^{-1}, [a_2,a_1]a_4^{-1}, a_3^2, a_4^2, a_5^2$	$\langle a_3,a_4,a_5\rangle$	3	4
G_{24}	$a_1^2a_5^{-1}, a_2^2, [a_2,a_1]a_4^{-1}, a_3^2a_4^{-1}, a_4^2, a_5^2$	$\langle a_3,a_4,a_5\rangle$	3	4
G_{25}	$a_1^2a_5^{-1}, a_2^2, [a_2,a_1]a_4^{-1}, a_3^2a_5^{-1}, a_4^2, a_5^2$	$\langle a_3,a_4,a_5\rangle$	3	4
G_{26}	$a_1^2a_5^{-1}, a_2^2a_4^{-1}, [a_2,a_1]a_4^{-1}, a_3^2a_5^{-1}a_4^{-1}, a_4^2, a_5^2$	$\langle a_3,a_4,a_5\rangle$	3	4
G_{27}	$a_1^2, a_2^2, [a_2,a_1]a_4^{-1}, a_3^2, [a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2, a_5^2$	$\langle a_4,a_5\rangle$	3	4
G_{28}	$a_1^2, a_2^2a_4^{-1}, [a_2,a_1]a_4^{-1}, a_3^2, [a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2, a_5^2$	$\langle a_4,a_5\rangle$	3	4
G_{29}	$a_1^2a_4^{-1}, a_2^2a_4^{-1}, [a_2,a_1]a_4^{-1}, a_3^2, [a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2, a_5^2$	$\langle a_4,a_5\rangle$	3	4
G_{30}	$a_1^2, a_2^2, [a_2,a_1]a_4^{-1}, a_3^2a_4^{-1}, [a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2, a_5^2$	$\langle a_4,a_5\rangle$	3	4
G_{31}	$a_1^2, a_2^2a_5^{-1}, [a_2,a_1]a_4^{-1}, a_3^2a_4^{-1}, [a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2, a_5^2$	$\langle a_4,a_5\rangle$	3	4
G_{32}	$a_1^2a_4^{-1}, a_2^2a_5^{-1}, [a_2,a_1]a_4^{-1}, a_3^2a_4^{-1}, [a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2, a_5^2$	$\langle a_4,a_5\rangle$	3	4
G_{33}	$a_1^2, a_2^2a_5^{-1}a_4^{-1}, [a_2,a_1]a_4^{-1}, a_3^2a_4^{-1}, [a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2, a_5^2$	$\langle a_4,a_5\rangle$	3	4
G_{34}	$a_1^2, a_2^2a_4^{-1}, [a_2,a_1]a_4^{-1}, a_3^2a_5^{-1}, [a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2, a_5^2$	$\langle a_4,a_5\rangle$	3	4

Група	Съотношения	Център	Ранг	Експ.
G_{35}	$a_1^2a_4^{-1}, a_2^2a_4^{-1}, [a_2,a_1]a_4^{-1}, a_3^2a_5^{-1}, [a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2, a_5^2$	$\langle a_4, a_5\rangle$	3	4
G_{36}	$a_1^2a_4^{-1}, a_2^2, a_3^2, a_4^2a_5^{-1}, a_5^2$	G_{36}	3	8
G_{37}	$a_1^2a_4^{-1}, a_2^2, [a_2,a_1]a_5^{-1}, a_3^2, a_4^2a_5^{-1}, a_5^2$	$\langle a_3, a_4, a_5\rangle$	3	8
G_{38}	$a_1^2a_4^{-1}, a_2^2, a_3^2, [a_3,a_2]a_5^{-1}, a_4^2a_5^{-1}, a_5^2$	$\langle a_1, a_4, a_5\rangle$	3	8
G_{39}	$a_1^2, a_2^2, [a_2,a_1]a_4^{-1}, a_3^2, a_4^2a_5^{-1}, [a_4,a_1]a_5^{-1}, [a_4,a_2]a_5^{-1}, a_5^2$	$\langle a_3, a_5\rangle$	3	8
G_{40}	$a_1^2a_5^{-1}, a_2^2, [a_2,a_1]a_4^{-1}, a_3^2, a_4^2a_5^{-1}, [a_4,a_1]a_5^{-1}, [a_4,a_2]a_5^{-1}, a_5^2$	$\langle a_3, a_5\rangle$	3	8
G_{41}	$a_1^2a_5^{-1}, a_2^2a_5^{-1}, [a_2,a_1]a_4^{-1}, a_3^2, a_4^2a_5^{-1}, [a_4,a_1]a_5^{-1}, [a_4,a_2]a_5^{-1}, a_5^2$	$\langle a_3, a_5\rangle$	3	8
G_{42}	$a_1^2, a_2^2, [a_2,a_1]a_4^{-1}, a_3^2a_5^{-1}, a_4^2a_5^{-1}, [a_4,a_1]a_5^{-1}, [a_4,a_2]a_5^{-1}, a_5^2$	$\langle a_3, a_5\rangle$	3	8
G_{43}	$a_1^2, a_2^2, [a_2,a_1]a_4^{-1}, a_3^2, [a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2a_5^{-1}, [a_4,a_1]a_5^{-1}, [a_4,a_2]a_5^{-1}, [a_4,a_3], a_5^2$	$\langle a_5\rangle$	3	8
G_{44}	$a_1^2, a_2^2a_5^{-1}, [a_2,a_1]a_4^{-1}, a_3^2, [a_3,a_1]a_5^{-1}, [a_3,a_2], a_4^2a_5^{-1}, [a_4,a_1]a_5^{-1}, [a_4,a_2]a_5^{-1}, [a_4,a_3], a_5^2$	$\langle a_5\rangle$	3	8
G_{45}	$a_1^2a_5^{-1}, a_2^2, a_3^2, a_4^2, a_5^2$	G_{45}	4	4
G_{46}	$a_1^2, a_2^2, [a_2,a_1]a_5^{-1}, a_3^2, a_4^2, a_5^2$	$\langle a_3, a_4, a_5\rangle$	4	4
G_{47}	$a_1^2a_5^{-1}, a_2^2a_5^{-1}, [a_2,a_1]a_5^{-1}, a_3^2, a_4^2, a_5^2$	$\langle a_3, a_4, a_5\rangle$	4	4
G_{48}	$a_1^2, a_2^2, [a_2,a_1]a_5^{-1}, a_3^2a_5^{-1}, a_4^2, a_5^2$	$\langle a_3, a_4, a_5\rangle$	4	4
G_{49}	$a_1^2, a_2^2, [a_2,a_1]a_5^{-1}, a_3^2, [a_3,a_1], [a_3,a_2]a_5^{-1}, a_4^2, [a_4,a_1]a_5^{-1}, [a_4,a_2], [a_4,a_3], a_5^2$	$\langle a_5\rangle$	4	4
G_{50}	$a_1^2, a_2^2a_5^{-1}, [a_2,a_1]a_5^{-1}, a_3^2a_5^{-1}, [a_3,a_1], [a_3,a_2]a_5^{-1}, a_4^2, [a_4,a_1]a_5^{-1}, [a_4,a_2], [a_4,a_3], a_5^2$	$\langle a_5\rangle$	4	4
G_{51}	$a_1^2, a_2^2, a_3^2, a_4^2, a_5^2$	G_{51}	5	2

Литература

[Ба] Башмаков М. И., О задаче погружения полей, *Мат. заметки*, 1968, **4**, № 2, 137-140.

[Ив] К. Ивасава, Локальнаь теория полей классов, Мир, Москва, 1983; English translation: K. Iwasawa, "Local Class Field Theory", Oxford, 1986.

[ИЛФ] Ишханов В. В., Лурье Б. Б., Фаддеев Д. К., "Задача погружения в теории Галуа", Наука, Москва, 1990; English Transl.: V. V. Ishanov, B. B. Lur'e and D. K. Faddeev, "The embedding problem in Galois theory", Amer. Math. Soc., Providence, 1997.

[МЗ] И. Михайлов, Н. Зяпков, "Висша алгебра и теория на Галоа", Фабер, Велико Търново, 2004.

[Ми] И. Михайлов, "2-групи като групи на Галоа", дисертация за присъждане на научната и образователна степен "доктор", Шумен, 2000.

[ПСЧ] А. Попов, П. Сидеров, К. Чакърян, "Ръководство по висша алгебра", Университетско издателство "Климент Охридски", София, 1990.

[Як] Яковлев А. В., Задача погружения полей, *Изв. АН СССР, Сер. мат*, 1964, **150**, № 3, 645-660.

[AFSS] J. K. Arason, B. Fein, M. Schacher and J. Sonn, Cyclic extensions of $K(\sqrt{-1})/k$, *Trans. Amer. Math. Soc.* **313** (1989), 843-851.

[Be] H. Betchel, "The theory of groups", Adison-Wesley Series in Mathematics, 1971.

[Br] G. Brattström, On p-groups as Galois groups, *Math. Scand.* **65** (1989), 165-174.

[CF] J.W.S. Cassels, A. Fröhlich, "Algebraic number theory", Academic press, London and New York, 1967.

[CHK] H. Chu, J. Hu and M. Kang, Noether's problem for dihedral 2-groups, *Comment. Math. Helv.* **79** (2004), 147-159.

[CHPK] H. Chu, J. Hu, Y. Prokhorov and M. Kang, Noether's problem for groups of order 32, *J. Algebra* **320** (2008), 3022-3035.

[DEK] C. Drees, M. Epkenhans, and M. Krüskemper, On the computation of the trace form of some Galois extensions, *J. Algebra* **192** (1997), no. 1, 209-234.

[Fr] A. Fröhlich, Orthogonal representations of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants, *J. Reine Angew. Math.* **360** (1985), 84-123.

[FM] A. Fröhlich and A. M. McEvett, The representations of groups by automorphisms of forms, *J. Alg.* **12** (1969), 114-133.

[FH] W. Fulton, J. Harris, "Representation theory. A first course", Graduate Texts in Mathematics, **129**, Springer-Verlag, New York, 1991.

[GAP] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.10; 2007. (`http://www.gap-system.org`)

[Gi] R. Gillard, Plongement d'une extension d'ordre p ou p^2 dans une surextension non abelienne d'ordre p^3, *J. Reine Angew. Math.* **268-269** (1974), 418-426.

[GS1] Grundman H.G., Smith T.L., Realizability and automatic realizability of Galois groups of order 32, *Cent. Eur. J. Math.*, **8(2)** (2010), 244-–260.

[GS2] Grundman H.G., Smith T.L., Galois realizability of groups of order 64, *Cent. Eur. J. Math.*, **8(5)** (2010), 846-–854.

[GSS] H. G. Grundman, T. L. Smith, and J. R. Swallow, Groups of order 16 as Galois groups, *Expo. Math.* **13** (1995), 289-319.

[Ha] M.Hall, "The theory of groups", Macmillan Company, New York, 1959.

[Har] D. Harbater, Fundamental groups and embedding problems in characteristic p, *Recent Developments in the Inverse Galois Problem (Seattle, WA, 1993), Contemp. Math.* **186** (1995), 353-369.

[HK] S. Hu and M. Kang, Noether's Problem for Some p-groups, in "Rationality problem", edited by F. Bogomolov and Y. Tschinkel, Progress in Math., Birkhauser, Boston, 2008. (available at `http://arxiv.org/abs/0704.1701`)

[HLW] Y.-S. Hwang, D. B. Leep, and A. R. Wadsworth, Galois groups of order $2n$ that contain a cyclic subgroup of order n, *Pacific J. Math.* **212** (2003), 297-319.

[JLY] C. Jensen, A. Ledet and N. Yui, "Generic polynomials: constructive aspects of the inverse Galois problem", Cambridge University Press, 2002.

[Ka1] M. Kang, Noether's problem for dihedral 2-groups II, *Pacific J. Math.* **222** No 2 (2005), 301-316.

[Ka2] M. Kang, Noether's problem for metacyclic p-groups, *Adv. Math.* **203** (2005), 554-567.

[Ka3] M. Kang, Rationality problem for some meta-abelian groups, *J. Algebra* **322** (2009), 1214-1219.

[Ki] I. Kiming, Explicit classifications of some 2-extensions of a field of characteristic different from 2, *Cand. J. Math.* **42** (1990), 825-855.

[KM1] J. Klüners & G. Malle, Explicit Galois Realization of Transitive Groups of Degree up to 15, *J. Symbolic Computation* **30** (2000), 675-716.

[KM2] J. Klüners & G. Malle, A database for field extensions of the rationals, *LMS J. Comput. Math.* **4** (2001), 182–196.

[KR] D.-S. Kang and Z. Reichstein, Trace forms of Galois field extensions in the presence of roots of unity, *J. Reine Angew. Math.* **549** (2002), 79-89.

[La] T. Y. Lam, "The algebraic theory of quadratic forms", Benjamin, Reading, MA, 1973.

[Le1] A. Ledet, On 2-groups as Galois groups, *Canad. J. Math.* **47** (1995), 1253-1273.

[Le2] A. Ledet, Embedding problems with cyclic kernel of order 4, *Israel J. Math.* **106** (1998), 109-131.

[Le3] A. Ledet, Embedding problems and equivalence of quadratic forms, *Math. Scand.* **88** (2001), 279-302.

[Le4] A. Ledet, "Brauer Type Embedding Problems", Fields Institute Monographs **21**, American Mathematical Society, 2005.

[Ma] R. Massy, Construction de p-extensions galoisiennes d'un corps de caractéristique différente de p, *J. of Alg.* **109** (1987), 508-535.

[Me] A. Merkurjev, On the norm residue symbol of degree 2, *Soviet Math. Dokl.* **24** (1981), 546-551.

[Mes] J.-F. Mestre, Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\widetilde{A}_n$, *J. Algebra* **131** (1990), 483-495.

[MeS] A. S. Merkurjev and A. A. Suslin, K-Cohomology of Severi-Brauer Varieties and the norm residue homomorphism, *Izv. Akad. Nauk SSSR*, Ser. Mat. **46** (1982), 1011-1046; English transl. in *Math. USSR Izvestiya* **21** (1983), 307-340.

[Mi1] I. Michailov, Embedding obstructions for the dihedral, semidihedral and quaternion 2-groups, *J. Algebra* **245** (2001), 355-369.

[Mi2] I. Michailov, Embedding obstructions for the cyclic and modular 2-groups, *Math. Balk., New Series*, **21** (2007), Fasc. 1-2, 31-50.

[Mi3] I. Michailov, Four non-abelian groups of order p^4 as Galois groups, *J. Algebra* **307** (2007), 287-299.

[Mi4] I. Michailov, Induced orthogonal representations of Galois groups, *J. Algebra* **322** (2009), 3713-3732.

[Mi5] I. Michailov, On Galois cohomology and realizability of 2-groups as Galois groups, *Cent. Eur. J. Math.*, **9 (2)** (2011), 403–419.

[Mi6] I. Michailov, Exact sequences in the theory of orthogonal representations of groups, *C.R. de' l Academie bulgarie des Sciences*, **62 (9)** (2009), 1057-1062.

[Mi7] I. Michailov, Groups of order 32 as Galois groups, *Serdica Math. J.* **33 (1)** (2007), 1-34.

[Mi8] I. Michailov, Some groups of orders 8 and 16 as Galois groups over the p-adic number field, *Math. Balk., New Series*, **19** (2005), Fasc. 3-4, 367-383.

[Mi9] I. Michailov, Quaternion extensions of order 16, *Serdica Math. J.* **31 (3)** (2005), 217-228.

[Mi10] I. Michailov, Some groups of orders 8 and 16 as Galois groups over $\mathbb{Q}$, *Math. Balk., New Series*, **17** (2003), Fasc. 1-2, 155-170.

[Mi11] I. Michailov, Noether's problem for some groups of order $16n$, *Acta Arith.* **143** (2010), 277-290.

[Mi12] I. Michailov, On Galois cohomology and realizability of 2-groups as Galois groups II, *Cent. Eur. J. Math.*, **9 (6)** (2011), 1333–1343, DOI: 10.2478/s11533-011-0086-z.

[MM1] G. Malle & B. H. Matzat, Realisierung von Gruppen $\mathrm{PSL}_2(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}$, *Math. Ann.* **272** (1985), 549-565.

[MM2] G. Malle & B. H. Matzat, "Inverse Galois Theory Springer Monographs in Mathematics, Springer-Verlag, 1999.

[MR] J. Mináč and Z. Reichstein, Trace forms of Galois extensions in the presence of a fourth root of unity, *Int. Math Res. Not.* (2004), 389-410.

[MS1] J. Mináč and J. Swallow, Galois module structure of pth-power classes of extensions of degree p, *Isr. J. of Math.*, **138** (2003), 29–42.

[MS2] J. Mináč and J. Swallow, Galois embedding problems with cyclic quotient of order p, *Israel J. of Math.*, **145** (2005), 93–112.

[MSS1] J. Mináč, A. Schultz, and J. Swallow, Galois module structure of pth-power classes of cyclic extensions of degree p^n, *Proc. London Math. Soc.*, **92** (2006), 307-341.

[MSS2] J. Mináč, A. Schultz, and J. Swallow, Automatic realizations of Galois groups with cyclic quotient of order p^n, *Journal de Théorie des Nombres de Bordeaux*, **20** (2008), 419-430.

[MZ1] I. Michailov and N.Ziapkov, Embedding obstructions for the generalized quaternion group, *J. Algebra* **226** (2000), 375-389.

[MZ2] I. Michailov, N. Ziapkov, Attendant embedding problems, *C.R. de' l Academie bulgarie des Sciences*, **53 (7)** (2000), 9-12.

[MZ3] I. Michailov, N. Ziapkov, On equivalent embedding problems, *C.R. de' l Academie bulgarie des Sciences*, **53 (8)** (2000), 9-12.

[MZ4] I. Michailov and N. Ziapkov, Embedding problems with Galois groups of order 16, *Math. Balk.* **15** (2001), Fasc. 1-2, 99-108.

[MZ5] I. Michailov and N. Ziapkov, The Inverse Problem Of Galois Theory, *Proceedings of the 37th spring conference of the Union of Bulgarian Mathematicians in Borovets*, 2008, p. 17-28.

[Ni] Y. Ninomiya, Finte p-groups with cyclic subgroups of index p^2, *Math. J. Okayama Univ.* **36** (1994), 1–21.

[No] E. Noether, Gleichingen mit vorgeschriebener Gruppe, *Math. Ann.* **78** (1916), 221-229.

[NSW] J. Neukirch, A. Schmidt & K. Wingberg, "Cohomology of number fields", Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag, 2000.

[Pi] R. S. Pierce, "Associative algebras", Springer-Verlag, New York, 1982.

[Pl] B. Plans, On Noether's problem for central extensions of symmetric and alternating groups, *J. Algebra* **321** (2009), 3704-3713.

[Re] H. Reichardt, Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung, *J. Reine Angew. Math.* **177** (1937), 1-5.

[Ri] C. Riehm, The corestriction af algebraic structures, *Invent. Math.* **11** (1970), 73-98.

[Ro] P. Roquette, On the Galois cohomology of the projective linear group and its applications to the construction of generic splitting fields of algebras, *Math. Ann.* **150** (1963), 411-439.

[Sa1] D.J. Saltman, Generic Galois extensions and problems in field theory, *Adv. Math.* **43** (1982), 250-283.

[Sa2] D.J. Saltman, Twisted multiplicative field invariants, Noether's problem, and Galois extensions, *J. Algebra* **131** (2) (1990), 535-558.

[Sc] W. Scharlau, "Quadratic and hermitian forms", Springer-Verlag, 1985.

[Scho] A. Scholz, Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I, *Math. Z.* **42** (1937), 161-188.

[Schur] I. Schur, Gleichungen ohne Affekt, Sitzungsberichte Akad. Berlin (1930), 443-449.

[Se1] J.-P. Serre, "Cohomologie Galoisienne", Springer Verlag, 1964.

[Se2] J.-P. Serre, "Corps Locaux", Hermann, Paris, 1968.

[Se3] J.-P. Serre, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, Comment. Math. Helv. **59** (1984), 651-676.

[Se4] J.-P. Serre, "Topics in Galois Theory", Research Notes in Mathematics, Jones & Barlett, 1992.

[Sha] I. R. Shafarevich, Construction of fields of algebraic numbers with given solvable Galois group (in Russian), *Izv. Aksd. Nauk SSSR, Ser. Mat.* **18** (1954), 525-578.

[Shi] K.-Y. Shih, On the construction of Galois extensions of function fields and number fields, Math. Ann. **207** (1974), 99-120.

[Sm] T. Smith, Extra-special groups of order 32 as Galois groups, *Can. J. Math.* **46**(4) (1994), 886-896.

[Sp] Speiser A., Zahlentheoretische Satze aus der Gruppentheorie, *Math. Z.*, 1919, Bd. 5, 1-6.

[Sw] J. Swallow, Central p-Extensions of $(p, p, \ldots, p)$-Type Galois groups, *J. of Alg.* **186** (1996), 277-298.

[Swan] R. Swan, Noether's problem in Galois theory, in "Emmy Noether in Bryn Mawr", edited by B. Srinivasan and J. Sally, Springer-Verlag, Berlin, 1983.

[ST] J. Swallow, F. Thiem, Quadratic corestriction, C_2-embedding problems, and explicit construction, *Comm. in Algebra* **30** (2002), 3227-3258.

[Ta] J. Tate, Relations between K_2 and Galois cohomology, *Invent. Math.* **36** (1976), 257-274.

[Th] J. G. Thompson, Some finite groups which appear as $\mathrm{Gal}(L/K)$, where $K \subseteq \mathbb{Q}(\mu_n)$, *J. Algebra* **89** (1984), 437-499.

[Ti] J.-P. Tignol, On the corestriction of central simple algebras, *Math. Z.* **194** (1987), 267-274.

[Vö] H. Völklein, "Groups as Galois Groups, an Introduction", Cambridge Studies in Advanced Mathematics 53, Cambridge University Press, 1996.

[Wa] W. C. Waterhouse, The normal closures of certain Kummer extensions, *Canad. Math. Bul.* **37** (1994), no. 1, 133-139.

[Wi] E. Witt, Konstruction von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der ordnung p^f, *J. Reine angew. Math.* **174** (1936), 237-245.

Азбучен указател