§4. Циклические и разрешимые расширения

4.1. Круговые поля. Поле $\mathbb{K}_n \stackrel{\text{def}}{=} \mathbb{Q}[\zeta_n]$, порождённое как алгебра над $\mathbb{Q}$ примитивным корнем n-той степени из единицы $\zeta_n \stackrel{\text{def}}{=} e^{2\pi i/n} \in \mathbb{C}$ называется n-тым *круговым*[1] полем. Будучи полем разложения сепарабельного многочлена $x^n - 1 \in \mathbb{Q}[x]$, корни которого образуют циклическую мультипликативную группу $\boldsymbol{\mu}_n \subset \mathbb{C}$ комплексных корней n-той степени из единицы, расширение $\mathbb{K}_n \supset \mathbb{Q}$ является расширением Галуа, и каждый автоморфизм $\sigma \in \operatorname{Gal}\mathbb{K}_n/\mathbb{Q}$ переводит образующую ζ_n группы $\boldsymbol{\mu}_n$ в какую-нибудь образующую группы $\boldsymbol{\mu}_n$, т. е. действует по правилу $\sigma\colon \zeta_n \mapsto \zeta_n^{m(\sigma)}$, где $m(\sigma) \in (\mathbb{Z}/(n))^\times$ обратим в кольце вычетов[2] $\mathbb{Z}/(n)$. Это задаёт гомоморфное вложение группы Галуа кругового поля в мультипликативную группу обратимых элементов кольца вычетов:

$$\operatorname{Gal}\mathbb{K}_n/\mathbb{Q} \hookrightarrow \big(\mathbb{Z}/(n)\big)^\times, \quad \sigma \mapsto m(\sigma). \tag{4-1}$$

Поскольку множество $R_n \stackrel{\text{def}}{=} \{\zeta_n^m \mid \text{нод}(n,m) = 1\} \subset \boldsymbol{\mu}_n$ всех первообразных корней степени n из единицы переводится группой $\operatorname{Gal}\mathbb{K}_n/\mathbb{Q}$ в себя, *n-тый круговой многочлен*

$$\Phi_n(x) \stackrel{\text{def}}{=} \prod\nolimits_{\xi\in R_n} (x - \xi)$$

инвариантен относительно группы Галуа и тем самым лежит в $\mathbb{Q}[x]$. Будучи полиномами от корней многочлена $x^n - 1$, все коэффициенты многочлена $\Phi_n(x)$ целы над $\mathbb{Z}$, и значит[3], $\Phi_n(x) \in \mathbb{Z}[x]$. Например,

$$\begin{aligned}
&\Phi_2(x) = x + 1\\
&\Phi_3(x) = (x-\omega)(x-\omega^2) = x^2 + x + 1\\
&\Phi_4(x) = (x-i)(x+i) = x^2 + 1\\
&\Phi_5(x) = (x^5 - 1)/(x-1) = x^4 + x^3 + x^2 + x + 1\\
&\Phi_6(x) = (z-\zeta_6)(x-\zeta_6^{-1}) = x^2 - x + 1 \quad \text{и т. д.}
\end{aligned}$$

Поле $\mathbb{K}_n$ является полем разложения многочлена Φ_n и $\operatorname{Gal}\mathbb{K}_n/\mathbb{Q} = \operatorname{Gal}\Phi_n/\mathbb{Q}$.

4.1.1. Элементы Фробениуса. При простом $p \nmid n$ многочлен $x^n - 1$ сепарабелен над $\mathbb{F}_p$. Редукция $\overline{\Phi}_n$ многочлена Φ_n по модулю p тоже сепарабельна над $\mathbb{F}_p$, т. к. $\overline{\Phi}_n$ делит $x^n - 1$. Обозначим через $\mathcal{O} \subset \mathbb{K}_n$ кольцо целых[4] над $\mathbb{Z}$ элементов кругового поля, а через $\mathcal{O}/(p)$ — его редукцию по модулю p. Сопоставление $\xi \mapsto \overline{\xi} = \xi \pmod p \in \mathcal{O}/(p)$ задаёт биекцию между множеством комплексных первообразных корней $R_n \subset \mathcal{O} \subset \mathbb{K}_n \subset \mathbb{C}$ и множеством корней многочлена $\overline{\Phi}_n$ в его поле разложения над $\mathbb{F}_p$. Последнее порождается этими корнями как алгебра над $\mathbb{F}_p$ и является конечным расширением Галуа поля $\mathbb{F}_p$ с циклической группой Галуа, порождённой автоморфизмом Фробениуса[5] $\overline{\xi} \mapsto \overline{\xi}^p$. По теор. 3.4 в группе Галуа $\operatorname{Gal}\Phi_n/\mathbb{Q}$ имеется такая перестановка $\sigma \in \operatorname{Aut} R_n$ комплексных первообразных корней, что $\overline{\sigma(\xi)} = \overline{\xi}^p$. Мы заключаем, что автоморфизм мультипликативной группы $\boldsymbol{\mu}_n \subset \mathbb{K}_n$, заданный правилом

$$F_p\colon \boldsymbol{\mu}_n \xrightarrow{\sim} \boldsymbol{\mu}_n, \quad \xi \mapsto \xi^p, \tag{4-2}$$

---

[1] Или *циклотомическим*.

[2] Напомню, что мультипликативные образующие циклической группы $\boldsymbol{\mu}_n$ имеют вид ζ^m, где $\text{нод}(n,m) = 1$, и называются *первообразными* корнями n-той степени из единицы, см. раздел 2.4.3 на с. 50 лекций [Алг 1].

[3] См. прим. 1.1 на стр. 5.

[4] См. прим. 1.3 на стр. 6.

[5] См. прим. 3.2 на стр. 25 и доказательство сл. 3.3 на стр. 34.

продолжается до автоморфизма кругового поля $\mathbb{K}_n$ над $\mathbb{Q}$. Он называется *p-элементом Фробениуса* в группе Галуа кругового поля.

Применяя к корню $\zeta_n \in R_n$ автоморфизмы F_p со всевозможными простыми $p \nmid n$, а также их итерации, можно получить все первообразные корни: любой из них имеет вид ζ_n^m для некоторого $m = p_1^{m_1} \dots p_k^{m_k}$, взаимно простого с n, и равен $F_{p_1}^{m_1} \dots F_{p_k}^{m_k} \zeta_n$. Мы заключаем, что группа Галуа кругового многочлена транзитивно действует на его корнях. Суммируем всё сказанное.

Предложение 4.1
Круговой многочлен Φ_n имеет целые коэффициенты, неприводим над $\mathbb{Q}$ и является минимальным многочленом первообразного корня ζ_n над $\mathbb{Q}$, а вложение (4-1) является изоморфизмом группы Галуа $\operatorname{Gal} \Phi_n/\mathbb{Q}$ с мультипликативной группой обратимых вычетов $\mathbb{Z}/(n)^\times$. В частности, $[\mathbb{K}_n : \mathbb{Q}] = \varphi(n)$, где φ — функция Эйлера.

Доказательство. Если бы многочлен Φ_n был приводим над $\mathbb{Q}$, его группа Галуа переводила бы множество корней каждого неприводимого множителя в себя и не могла бы транзитивно действовать на корнях многочлена Φ_n. Из транзитивности действия группы $\operatorname{Gal} \Phi_n$ на корнях вытекает неравенство $|\operatorname{Gal} \Phi_n| \geqslant \deg \Phi_n = \varphi(n) = |(\mathbb{Z}/(n))^\times|$, гарантирующее сюръективность вложения (4-1). □

4.1.2. Круговые поля $\mathbb{K}_p$ с простым $p > 2$. В этом разделе мы обсудим некоторые вытекающие из теории Галуа свойства круговых полей $\mathbb{K}_p$, где $p > 2$ — простое. Всюду далее мы полагаем $\zeta = \zeta_p = e^{2\pi i/p}$.

Пример 4.1 (квадратичное подполе поля $\mathbb{K}_p$)
В мультипликативной группе $\mathbb{F}_p^\times$ есть ровно одна подгруппа индекса 2, а именно — группа ненулевых квадратов $\mathbb{F}_p^{\times 2} \stackrel{\text{def}}{=} \{x^2 \mid x \in \mathbb{F}_p^\times\}$. В самом деле, любая подгруппа $H \lhd \mathbb{F}_p^\times$ индекса 2 автоматически нормальна, и поскольку фактор по ней изоморфен мультипликативной группе $\{\pm 1\}$, единственным квадратом в которой является 1, все $(p-1)/2$ квадратов[1] группы $\mathbb{F}_p^\times$ лежат в H и таким образом полностью её исчерпывают. Мы заключаем, что в группе Галуа $\operatorname{Gal} \Phi_p/\mathbb{Q} \simeq \mathbb{F}_p^\times$ имеется единственная подгруппа индекса 2, и изоморфизм из форм. (4-1) на стр. 35 переводит её в группу ненулевых квадратов поля $\mathbb{F}_p$. Эта подгруппа соответствует по Галуа единственному квадратичному расширению $\mathbb{Q} \subset \mathbb{K}$, содержащемуся в круговом поле $\mathbb{Q}[\zeta]$. Чтобы описать его явно, подставим в круговой многочлен

$$1 + x + \dots + x^{p-1} = \prod_{k=1}^{p-1} (x - \zeta^k)$$

значение $x = 1$ и сгруппируем в произведении справа пары сомножителей, отвечающих обратным друг другу корням:

$$p = \prod_{k=1}^{(p-1)/2} (1 - \zeta^k)(1 - \zeta^{-k}) = \prod_{k=1}^{(p-1)/2} (-\zeta^{-k}) \cdot (1 - \zeta^k)^2 . \tag{4-3}$$

[1] См. пример 1.8 на с. 32 лекций [Алг 1].

Поскольку 2 обратимо по модулю p, существует такое $m \in \mathbb{Z}$, что

$$-\sum_{k=1}^{(p-1)/2} k = \frac{1-p^2}{8} \equiv 2m \,(\mathrm{mod}\, p)\ .$$

Полагая $\alpha = \zeta^m$ и $\beta = \prod_{k=1}^{(p-1)/2}(1-\zeta^k)$, можно переписать равенство (4-3) в виде

$$(-1)^{(p-1)/2} p = \alpha^2 \beta^2\,,$$

откуда $\sqrt{(-1)^{(p-1)/2}p} = \alpha\beta \in \mathbb{Q}[\zeta]$. Мы заключаем, что искомое квадратичное расширение порождается квадратным корнем из $(-1)^{(p-1)/2}p$.

Пример 4.2 (квадратичный закон взаимности)
Пусть $p, q > 2$ — простые натуральные числа. Положим $q_* = (-1)^{\frac{q-1}{2}} q$, $\mathbb{L}_q = \mathbb{Q}[x]/(x^2 - q_*)$ и будем обозначать через $\mathcal{O}_q \subset \mathbb{L}_q$ кольцо целых, а через $[z]_p$ — класс элемента $z \in \mathcal{O}_q$ в $\mathcal{O}_q/(p)$.

Упражнение 4.1. Убедитесь, что $\mathcal{O}_q/(p) \simeq \mathbb{F}_p[x]/(x^2 - q_*)$.

Это факторкольцо является целым расширением поля $\mathbb{F}_p$. По предл. 1.2 на стр. 6 оно является полем, если и только если в нём нет делителей нуля. Последнее равносильно неприводимости многочлена $x^2 - q_*$ над $\mathbb{F}_p$, что происходит ровно тогда, когда $q_* \notin \mathbb{F}_p^{\times 2}$. В этом случае $\mathcal{O}_q/(p) \simeq \mathbb{F}_{p^2}$ и автоморфизм Фробениуса $\vartheta \mapsto \vartheta^p$ действует на нём нетривиально. Если же $q_* \in \mathbb{F}_p^{\times 2}$, то $x^2 - q_*$ распадается на два различных линейных множителя, и $\mathcal{O}_q/(p) \simeq \mathbb{F}_p \oplus \mathbb{F}_p$, а Фробениус действует на этом кольце тождественно. В прим. 4.1 мы видели, что поле $\mathbb{L}_q$ вложено в круговое поле $\mathbb{K}_q = \mathbb{Q}[\zeta_q]$, где $\zeta_q = e^{2\pi i/q} \in \mathbb{C}$. Элемент Фробениуса[1] $F_p : \zeta_q \to \zeta_q^p$ из группы Галуа $\mathrm{Gal}\,\mathbb{K}_q/\mathbb{Q}$ переводит подполе $\mathbb{L}_q$, кольцо $\mathcal{O}_q$ и идеал (p) в себя, а его приведение по модулю (p) действует на $\mathcal{O}_q/(p)$ предыдущим автоморфизмом Фробениуса. Это действие тривиально, если и только если p-элемент Фробениуса кругового поля $\mathbb{K}_q$ тривиально действует на корнях многочлена $x^2 - q_*$, т. е. оставляет поле $\mathbb{L}_q \subset \mathbb{K}_q$ неподвижным. Последнее означает, что p-элемент Фробениуса является квадратом в группе Галуа $\mathrm{Gal}\,\mathbb{K}_q/\mathbb{Q} \simeq \mathbb{F}_q^\times$. Мы заключаем, что $q_* = (-1)^{\frac{q-1}{2}} q \in \mathbb{F}_p^{\times 2}$ тогда и только тогда, когда $p \in \mathbb{F}_q^{\times 2}$. Этот факт известен как *квадратичный закон взаимности*.

Пример 4.3 (гауссова сумма в поле $\mathbb{K}_p$)
Альтернативный способ указать образующую квадратичного подполя в $\mathbb{K}_p$ состоит в том, чтобы написать элемент $\vartheta \in \mathbb{Q}[\zeta] \in \mathbb{K}_p$, инвариантный относительно подгруппы квадратов G^2 в группе Галуа $G = \mathrm{Gal}\,\mathbb{K}_p/\mathbb{Q} \simeq \mathbb{F}_p^\times$ и меняющий знак под действием всех остальных автоморфизмов из G. Это легко сделать при помощи *символа Лежандра*[2]

$$\left[\frac{n}{p}\right] \stackrel{\text{def}}{=} n^{\frac{p-1}{2}} \,(\mathrm{mod}\ p) = \begin{cases} 0 & \text{если } p \mid n \\ 1 & \text{если } [n]_p \in \mathbb{F}_p^{\times 2} \\ -1 & \text{если } [n]_p \in \mathbb{F}_p^\times \smallsetminus \mathbb{F}_p^{\times 2}\,. \end{cases}$$

Упражнение 4.2. Убедитесь, что квадратичный закон взаимности из предыдущего прим. 4.2 можно переписать в виде $\left[\frac{p}{q}\right] \cdot \left[\frac{q}{p}\right] = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

[1] См. прим. 4.1 на стр. 36.
[2] См. пример 1.8 на с. 32 учебника [Алг 1] и задачу АЛ2◇10 из листка 2 прошлогоднего курса алгебры.

Положим

$$\vartheta = \sum_{\sigma\in G^2} \sigma(\zeta_n) - \sum_{\sigma\notin G^2} \sigma(\zeta_n) = \sum_{m=1}^{n-1} \left[\frac{m}{n}\right] \cdot \zeta_n^m . \tag{4-4}$$

Правая часть формулы (4-4) называется *Гауссовой суммой*. Поскольку число ϑ^2 инвариантно относительно группы Галуа, оно лежит в $\mathbb{Q}$, и его след $\mathrm{Sp}(\vartheta^2) = \vartheta^2 \cdot [\mathbb{Q}[\zeta] : \mathbb{Q}] = \vartheta^2(p-1)$. С другой стороны, скалярный квадрат $\mathrm{sp}(\vartheta,\vartheta) = \mathrm{Sp}(\vartheta^2)$ нетрудно вычислить в координатах относительно аффинного базиса $1, \zeta, \ldots, \zeta^{p-1}$ поля $\mathbb{Q}[\zeta]$ над $\mathbb{Q}$.

Упражнение 4.3. Покажите, что каждый вектор $\alpha \in \mathbb{Q}[\zeta]$ однозначно представляется в виде $\alpha = a_0 + a_1\zeta + \ldots + a_{p-1}\zeta^{p-1}$, где числа $a_i \in \mathbb{Q}$ имеют нулевую сумму, и билинейная форма следа $\mathrm{sp}(\alpha,\beta) = \mathrm{Sp}(\alpha\beta)$ принимает на таких векторах $\alpha = \sum_{i=0}^{p-1} a_i\zeta^i$ и $\beta = \sum_{j=0}^{p-1} b_i\zeta^j$ значение $p(a_0b_0 + a_1b_{p-1} + a_2b_{p-2} + \ldots + a_{p-1}b_1)$.

Тем самым,

$$\mathrm{sp}(\vartheta,\vartheta) = p\sum_{k=1}^{p-1} \left[\frac{k}{p}\right]\left[\frac{-k}{p}\right] = \left[\frac{-1}{p}\right]\cdot p(p-1) = (-1)^{(p-1)/2}p(p-1)$$

Мы заключаем, что $\vartheta^2 = (-1)^{(p-1)/2}p$, что согласуется с прим. 4.1.

Пример 4.4 (кольцо целых кругового поля $\mathbb{K}_p$)
В условиях и обозначениях предыдущих двух примеров покажем, что число

$$\alpha = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2} \in \mathbb{K}_p$$

лежит в кольце целых $\mathcal{O} \subset \mathbb{K}_p$, если и только если все $a_i \in \mathbb{Z}$. Так как все $\zeta^k \in \mathcal{O}$ и

$$\operatorname{tr}\zeta^k = \begin{cases} p-1 \text{ при } k = 0 \\ -1 \text{ при } 1 \leqslant k \leqslant p-1\,, \end{cases}$$

мы заключаем, что $\mathrm{sp}(\alpha, \zeta^{-k} - \zeta) = \operatorname{tr}(\alpha\zeta^{-k}) - \operatorname{tr}(\alpha\zeta) = pa_k \in \mathbb{Z}$ при всех $0 \leqslant k \leqslant p-2$. Таким образом, для любого $\alpha \in \mathcal{O}$ число $p\alpha$ лежит в $\mathbb{Z}$-линейной оболочке чисел ζ^k с $0 \leqslant k \leqslant p-2$. Последняя совпадает с $\mathbb{Z}$-линейной оболочкой чисел $(1-\zeta)^k$ с $0 \leqslant k \leqslant p-2$, ибо матрица перехода от одних чисел к другим треугольная с ±1 на диагонали. Положим $\eta = 1-\zeta$, и пусть

$$p\alpha = b_0 + b_1\eta + b_2\eta^2 + \ldots + b_{p-2}\eta^{p-2}\,, \text{ где } b_i \in \mathbb{Z}\,. \tag{4-5}$$

Упражнение 4.4. Покажите, что число $(1-\zeta^m)/(1-\zeta^n)$ является обратимым элементом кольца $\mathcal{O}$ при всех $1 \leqslant m, n \leqslant p-1$.

Условимся писать $\alpha \sim \beta$, если числа $\alpha, \beta \in \mathcal{O}$ отличаются обратимым множителем[1] из $\mathcal{O}$. Из упр. 4.4 вытекает, что $\eta \sim 1-\zeta^k$ при всех $1 \leqslant k \leqslant p-1$, откуда

$$p = \Phi_p(1) = \prod_{k=1}^{p-1}(1-\zeta^k) \sim \eta^{p-1}\,. \tag{4-6}$$

[1] Напомню, что такие числа называются *ассоциированными*, и что условие $\alpha \sim \beta$ равносильно равенству главных идеалов $(\alpha) = (\beta)$ в кольце $\mathcal{O}$, см. упражнение 14.5 на с. 74 лекций [Алг 1].

Упражнение 4.5 (норма и след). Пусть $\mathbb{F} \supset \Bbbk$ — расширение Галуа степени n с группой Галуа $G = \operatorname{Gal}\mathbb{F}/\Bbbk$, и $\vartheta \in \mathbb{F}$. Обозначим через $\chi_\vartheta(t)$ и $\mu_\vartheta(t)$ характеристический и минимальный многочлены оператора умножения на $\vartheta\colon \mathbb{F} \to \mathbb{F}$, $x \mapsto \vartheta x$. Покажите, что

$$\chi_\vartheta(t) = \prod_{g\in G}(t - g(\vartheta)) = \mu_\vartheta(t)^{n/d}\,,\ \text{где } d = \deg_\Bbbk \vartheta\,,$$

и выведите отсюда, что[1] $\operatorname{Sp}(\vartheta) = \sum_{g\in G} g(\vartheta)$ и $N(\vartheta) = \prod_{g\in G} g(\vartheta)$.

Из упр. 4.5 вытекает, что $N(\eta) = \prod_{k=1}^{p-1}(1-\zeta^k) = \Phi_p(1) = p$, а из равенств (4-6) и (4-5) — что число $b_0 \in \mathbb{Z}$ делится в кольце $\mathcal{O}$ на η. В силу мультипликативности нормы, $N(b_0) = b_0^{p-1}$ делится в кольце $\mathbb{Z}$ на p, откуда и само b_0 делится на $p \sim \eta^{p-1}$. Теперь, приводя равенство (4-5) по модулю (η^2), заключаем, что b_1 делится на η, а значит, и на $p = N(\eta) \sim \eta^{p-1}$. Продолжая в том же духе, получим, что все коэффициенты b_i в разложении (4-5) делятся на p, и тем самым α выражается через степени η^k, а с ними — и через степени ζ^k с целыми коэффициентами.

4.2. Циклические расширения. Элемент ζ произвольного поля $\Bbbk$ называется *примитивным* или *первообразным* корнем степени m из единицы, если $\zeta^m = 1$, но $\zeta^i \neq 1$ при $0 < i < m$. Если поле $\Bbbk$ содержит такой корень ζ, то циклическая мультипликативная группа корней уравнения $x^m = 1$ в поле $\Bbbk$ имеет порядок m и порождается элементом ζ, а множество образующих этой группы есть множество всех примитивных корней из единицы степени m. В частности, многочлен $x^m - 1$ в этом случае сепарабелен. Поэтому m не делится на $\operatorname{char}(\Bbbk)$, и все многочлены $x^d - a \in \Bbbk[x]$ степени $d|m$ тоже сепарабельны. Всюду в этом разделе мы по умолчанию считаем, что в поле $\Bbbk$ имеется примитивный корень степени m из единицы и обозначаем циклическую мультипликативную группу корней m-той степени из единицы через $\boldsymbol{\mu}_m \subset \Bbbk^\times$.

Упражнение 4.6 (разность степеней). Убедитесь, что $x^n - y^n = \prod_{\xi\in\boldsymbol{\mu}_n}(x - \xi y)$ в $\Bbbk[x,y]$.

Теорема 4.1
Пусть $a \in \Bbbk^\times$, $f(x) = x^m - a$, и в поле $\Bbbk$ имеется примитивный корень степени m из единицы. Тогда группа Галуа $G = \operatorname{Gal} f/\Bbbk$ канонически изоморфна подгруппе $\boldsymbol{\mu}_n \subset \boldsymbol{\mu}_m$ для некоторого $n|m$, и в этом случае $a = b^{m/n}$ для некоторого $b \in \Bbbk$, а разложение f на неприводимые множители в $\Bbbk[x]$ имеет вид $f = \prod_{\vartheta\in\boldsymbol{\mu}_{m/n}}(x^n - \vartheta b)$.

Доказательство. Фиксируем алгебраическое замыкание $\overline{\Bbbk}$ поля $\Bbbk$ и какой-нибудь корень $\alpha \in \overline{\Bbbk}$ двучлена f. Все m корней двучлена f имеют вид $\xi\alpha$, где $\xi \in \boldsymbol{\mu}_m$. Если $g \in G$ переводит α в $\xi_g\alpha$, то и на остальные корни двучлена f автоморфизм g действует умножением на ξ_g:

$$g(\xi\alpha) = \xi g(\alpha) = \xi\xi_g\alpha = \xi_g \cdot \xi\alpha\,.$$

Мы получаем инъективный гомоморфизм групп

$$G \hookrightarrow \boldsymbol{\mu}_m\,,\quad g \mapsto \xi_g = g(\alpha)/\alpha\,, \tag{4-7}$$

позволяющий рассматривать G как подгруппу в $\boldsymbol{\mu}_m$, причём вложение (4-7) не зависит от выбора корня α двучлена f, так как $g(\xi\alpha)/(\xi\alpha) = \xi g(\alpha)/(\xi\alpha) = g(\alpha)/\alpha$ для всех $\xi \in \boldsymbol{\mu}_m$. Поскольку группа $\boldsymbol{\mu}_m$ циклическая порядка m, группа G тоже циклическая порядка $n|m$.

[1] Напомню, что *следом* $\operatorname{Sp}(\vartheta)$ и *нормой* $N(\vartheta)$ элемента $\vartheta \in \mathbb{F}$ называются соответственно след и определитель оператора умножения на $\vartheta\colon \mathbb{F} \to \mathbb{F}$, $x \mapsto \vartheta x$, см. прим. 1.3 на стр. 6.

Упражнение 4.7. Пусть $\zeta \in \boldsymbol{\mu}_m$ — примитивный корень степени m из единицы. Убедитесь, что для каждого $n \mid m$ в $\boldsymbol{\mu}_m$ имеется ровно одна подгруппа G порядка n, она порождается элементом $\eta = \zeta^k$, где $k = m/n$, а фактор $\boldsymbol{\mu}_m / G \simeq \mathbb{Z}/(k)$ состоит из классов $G\zeta^i$, где $0 \leqslant i \leqslant k-1$.

Смежные классы $G\zeta^i \subset \boldsymbol{\mu}_m$ биективно соответствуют Галуа-орбитам корней $\zeta^i\alpha$, каждая из которых задаёт Галуа-инвариантный неприводимый множитель

$$f_i(x) \stackrel{\text{def}}{=} \prod_{\nu=0}^{n-1}(x - \eta^\nu\zeta^i\alpha) \in \Bbbk[x]\,, \text{ где } \eta = \zeta^k\,,$$

двучлена f. По упр. 4.6 на стр. 39 $f_i(x) = x^n - b_i$, где $b_i = \zeta^{in}\alpha^n \in \Bbbk$. В частности, $\alpha^n = b_0 \in \Bbbk$. Тем самым разложение двучлена f на неприводимые множители в $\Bbbk[x]$ имеет вид

$$x^m - a = \prod_{i=0}^{k-1}(x^n - b_i) = \prod_{i=0}^{k-1}(x^n - \zeta^{in}b_0) = \prod_{\vartheta\in\boldsymbol{\mu}_k}(x^n - \vartheta b_0)\,,$$

откуда $a = b_0^k$ по упр. 4.6 на стр. 39. □

Упражнение 4.8. В условиях теор. 4.1 покажите, что поля разложения двучленов $x^m - a$ и $x^m - b$ в $\overline{\Bbbk}$ совпадают если и только если $a = b^r c^m$, где $c \in \Bbbk$, $r \in \mathbb{Z}$ и нод$(r, m) = 1$.

Определение 4.1
Расширение Галуа $\mathbb{K} \supset \Bbbk$ называется *циклическим степени* m, если $\operatorname{Gal}\mathbb{K}/\Bbbk$ является циклической группой m-того порядка.

Теорема 4.2
Всякое циклическое расширение степени m любого поля $\Bbbk$, содержащего первообразный корень m-той степени из единицы, является полем разложения неприводимого двучлена $x^m - a$ с $a \in \Bbbk$.

Доказательство. Пусть группа Галуа $G = \operatorname{Gal}\mathbb{K}/\Bbbk$ циклического расширения $\mathbb{K} \supset \Bbbk$ порождена автоморфизмом $g \in \operatorname{Aut}_\Bbbk \mathbb{K}$ порядка m. Фиксируем какой-нибудь первообразный корень m-той степени из единицы $\zeta \in \Bbbk$ и рассмотрим $\Bbbk$-линейный эндоморфизм поля $\mathbb{K}$

$$L_{\zeta,g} \stackrel{\text{def}}{=} \sum_{i=0}^{p-1}\zeta^i g^i :\ \vartheta \mapsto \sum_{i=0}^{p-1}\zeta^i g^i(\vartheta)\,.$$

Упражнение 4.9 (линейная независимость мультипликативных характеров). Покажите, что множество гомоморфизмов произвольной группы G в мультипликативную группу $\Bbbk^\times$ любого поля $\Bbbk$ линейно независимо в пространстве $\Bbbk^G$ всех функций $G \to \Bbbk$.

Из упражнения вытекает, что автоморфизмы $g^0 = \mathrm{Id}, g, g^2, \ldots, g^{m-1}$, будучи различными гомоморфизмами мультипликативных абелевых групп $\mathbb{K}^\times \to \mathbb{K}^\times$, линейно независимы в пространстве функций $\mathbb{K}^\times \to \mathbb{K}$, и тем самым эндоморфизм $L_{\zeta,g}$ ненулевой.

Упражнение 4.10. Убедитесь, что $gL_{\zeta,g} = \zeta^{-1}L_{\zeta,g}$.

Из равенства $\left(g - \zeta^{-1}\right)L_{\zeta,g} = 0$ вытекает, что образ оператора $L_{\zeta,g}$ состоит из собственных векторов оператора g с собственным числом ζ^{-1}, и коль скоро он ненулевой, в поле $\mathbb{K}$ есть такое ненулевое число α, что $g(\alpha) = \zeta^{-1}\alpha$. Галуа-орбита числа α состоит из m различных чисел

$g^i(\alpha) = \zeta^{-i}\alpha$, где $0 \leqslant i \leqslant m-1$, которые являются корнями двучлена $f(x) = x^m - a^m$. Его свободный член $a = \alpha^m$ лежит в $\Bbbk$, поскольку он инвариантен относительно группы Галуа: $g(\alpha^m) = g(\alpha)^m = \zeta^{-m}\alpha^m = \alpha^m$. Так как корни двучлена f образуют одну Галуа-орбиту, он неприводим, а поскольку все они лежат в $\Bbbk[\alpha]$, это примитивное расширение является полем разложения f. Так как $\Bbbk[\alpha] \subset \mathbb{K}$ и оба поля имеют степень m над $\Bbbk$, включение является равенством. □

Пример 4.5 (решение кубического уравнения в радикалах)
Пусть $\operatorname{char}\Bbbk \neq 2, 3$ и многочлен $f(x) = x^3 + px + q$ неприводим и сепарабелен. Обозначим через α, β, γ его корни в $\overline{\Bbbk}$, а через $\mathbb{K} \supset \Bbbk$ — поле, полученное присоединением к $\Bbbk$ примитивного кубического корня ω из единицы и квадратного корня $\delta = (\alpha-\beta)(\beta-\gamma)(\alpha-\gamma) = \sqrt{D}$ из дискриминанта $D = -4p^3 - 27q^2$ многочлена f. Группа Галуа $G = \operatorname{Gal} f/\mathbb{K} \simeq A_3$ циклическая порядка 3. Пусть её образующая τ действует на корни циклом $\alpha \mapsto \beta \mapsto \gamma$. Тогда числа

$$\begin{aligned} 0 &= \alpha + \beta + \gamma \\ \eta &= \alpha + \omega^2\beta + \omega\gamma \\ \zeta &= \alpha + \omega\beta + \omega^2\gamma \end{aligned} \tag{4-8}$$

собственные для τ с собственными значениями 1, ω и ω^2 соответственно, а их кубы

$$\begin{aligned} 0 &= \alpha^3 + \beta^3 + \gamma^3 + 3(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) + 3(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) + 6\alpha\beta\gamma \\ \eta^3 &= \alpha^3 + \beta^3 + \gamma^3 + 3\omega^2(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) + 3\omega(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) + 6\alpha\beta\gamma \\ \zeta^3 &= \alpha^3 + \beta^3 + \gamma^3 + 3\omega(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) + 3\omega^2(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) + 6\alpha\beta\gamma \end{aligned}$$

инвариантны относительно группы Галуа и лежат в $\mathbb{K}$.

Упражнение 4.11. Убедитесь, что

$$\begin{aligned} \eta^3 &= \frac{-27q + 3\delta(\omega^2 - \omega)}{2} = \frac{-27q - \sqrt{-27D}}{2} \\ \zeta^3 &= \frac{-27q + 3\delta(\omega - \omega^2)}{2} = \frac{-27q + \sqrt{-27D}}{2} \\ \eta\zeta &= -3p\,. \end{aligned}$$

Складывая равенства (4-8) с коэффициентами $(1,1,1)$, $(1,\omega,\omega^2)$ и $(1,\omega^2,\omega)$, получаем

$$\eta + \zeta = 3\alpha\,, \quad \omega\eta + \omega^2\zeta = 3\beta\,, \quad \omega^2\eta + \omega\zeta = 3\gamma\,, \tag{4-9}$$

где значения кубических корней

$$\eta = \sqrt[3]{\frac{-27q - \sqrt{-27D}}{2}} \quad \text{и} \quad \zeta = \sqrt[3]{\frac{-27q + \sqrt{-27D}}{2}}$$

следует выбрать так, чтобы $\eta\zeta = -3p$. Эти формулы известны как *формулы Кардано*.

4.3. Разрешимые расширения. Конечная группа G называется *разрешимой*, если все её композиционные факторы Жордана – Гёльдера[1] являются простыми циклическими группами. Это условие допускает несколько эквивалентных переформулировок[2]: разрешимость группы G равносильна тому, что цепочка последовательных коммутантов[3]

$$G' = [G, G]\,,\ G'' = [G', G']\,,\ G''' = [G'', G'']\,,\ \ldots$$

тривиализуется через конечное число шагов, а также существованию убывающей цепочки подгрупп

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_m = \{e\}\,, \tag{4-10}$$

в которой все факторы G_i/G_{i+1} абелевы.

Упражнение 4.12. Убедитесь в этом, а также в том, что все подгруппы и факторы разрешимой группы G разрешимы, и наоборот, разрешимость нормальной подгруппы $H \lhd G$ и фактора G/H влекут разрешимость G.

Конечное расширение Галуа поля характеристики нуль называется *разрешимым*, если разрешима его группа Галуа.

Теорема 4.3
Пусть[4] $\operatorname{char}(\Bbbk) = 0$ и хотя бы один из корней неприводимого многочлена $f \in \Bbbk[x]$ выражается через элементы поля $\Bbbk$ посредством четырёх арифметических действий и извлечений корней произвольных степеней. Тогда группа $\operatorname{Gal} f/\Bbbk$ разрешима.

Доказательство. Зафиксируем алгебраическое замыкание $\overline{\Bbbk} \supset \Bbbk$. Если корень $\alpha \in \overline{\Bbbk}$ многочлена f выражается в радикалах, то он лежит в подполе $\mathbb{L} \subset \overline{\Bbbk}$, к которому ведёт башня примитивных расширений

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \ldots \subset \mathbb{L}_m = \mathbb{L} \tag{4-11}$$

вида $\mathbb{L}_{i+1} = \mathbb{L}_i[x]/(x^{k_i} - a_i)$, где $a_i \in \mathbb{L}_i$. Для доказательства теоремы достаточно вложить поле $\mathbb{L}$ в поле $\mathbb{L}' \supset \Bbbk$, являющееся расширением Галуа с разрешимой группой $\operatorname{Gal}\mathbb{L}'/\Bbbk$. Тогда поле разложения $\mathbb{K}$ многочлена f будет нормальным над $\Bbbk$ подполем в $\mathbb{L}'$, и его группа Галуа $\operatorname{Gal}\mathbb{K}/\Bbbk = (\operatorname{Gal}\mathbb{L}'/\Bbbk)/(\operatorname{Gal}\mathbb{L}'/\mathbb{K})$, будучи фактором разрешимой группы, тоже будет разрешима. Для построения $\mathbb{L}'$ расширим башню (4-11) до башни $\Bbbk \subset \mathbb{L}'_0 \subset \mathbb{L}'_1 \subset \ldots \subset \mathbb{L}'_m = \mathbb{L}'$, в которой $\mathbb{L}_i \subset \mathbb{L}'_i$ и все $\mathbb{L}'_i$ являются расширениями Галуа поля $\Bbbk$. В качестве $\mathbb{L}'_0$ возьмём поле разложения многочлена $x^N - 1$ с таким N, чтобы в $\mathbb{L}'_0$ содержались первообразные корни из единицы всех степеней k_i, являющихся показателями радикалов в формуле для α. Далее действуем по индукции: если $\mathbb{L}'_i$ уже построено, то в качестве $\mathbb{L}'_{i+1}$ возьмём поле разложения многочлена $\prod_{\sigma\in\operatorname{Gal}\mathbb{L}'_i/\Bbbk}(x^{k_i} - \sigma(a_i))$. Так как коэффициенты этого многочлена инвариантны относительно группы $\operatorname{Gal}\mathbb{L}'_i/\Bbbk$, они лежат в $\Bbbk$, и $\mathbb{L}'_{i+1} \supset \Bbbk$ является расширением Галуа, содержащим поле $\mathbb{L}_{i+1} = \mathbb{L}_i[x]/(x^{k_i} - a_i)$. Поле $\mathbb{L}'_{i+1}$ получается из поля $\mathbb{L}'_i$ цепочкой последовательных переходов к полям разложения двучленов вида $x^n - a$ с $a \in \mathbb{L}'_i$. По теор. 4.1 все такие переходы являются

[1] См. раздел 11.2 на с. 190 лекций [Алг 1].
[2] См. задачу 9⋄4 из листка № 9 прошлогоднего курса алгебры.
[3] См. раздел 10.6 на с. 186 лекций [Алг 1].
[4] Требование $\operatorname{char}(\Bbbk) = 0$ можно ослабить до требования, чтобы $\operatorname{char}(\Bbbk)$ не делила ни один из показателей радикалов, участвующих в формуле для вычисления корня. Приводимое здесь доказательство работает и в этом случае.

расширениями Галуа с циклическими группами Галуа. Согласно предл. 4.1 и предл. 2.4 первый шаг нашего построения — переход от $\Bbbk$ к $\mathbb{L}_0'$ — также является расширением Галуа с абелевой группой Галуа. Таким образом, поле $\mathbb{L}'$ можно получить из $\Bbbk$ последовательными абелевым расширениями Галуа, и его группа $\operatorname{Gal}\mathbb{L}'/\Bbbk$ разрешима. □

Пример 4.6 (общее уравнение степени n и теорема Абеля)
Зафиксируем произвольное поле $\mathbb{F}$ характеристики нуль. Многочлен

$$x^n + a_1 x^{n-1} + \ldots + a_n \in \mathbb{F}(a_1, \ldots, a_n)[x], \tag{4-12}$$

рассматриваемый над полем $\Bbbk = \mathbb{F}(a_1, \ldots, a_n)$ рациональных функций от n алгебраически независимых переменных $a_1, \ldots, a_n$ с коэффициентами в $\mathbb{F}$, называется *общим*, поскольку придавая его коэффициентам конкретные значения из поля $\mathbb{F}$, можно получить любой «конкретный» многочлен $f \in \mathbb{F}[x]$. Наличие формулы, выражающей корни общего многочлена (4-12) через элементы поля $\Bbbk = \mathbb{F}(a_1, \ldots, a_n)$ в радикалах[1], позволяло бы единообразно решить в радикалах все «конкретные» уравнения n-той степени с коэффициентами из $\mathbb{F}$. Из прим. 3.8 на стр. 34 следует, что над полем $\mathbb{F} = \mathbb{Q}$ такой формулы нет. Чтобы проанализировать наличие такой формулы над произвольным полем $\mathbb{F}$, вычислим группу $\operatorname{Gal} f/\Bbbk$. Обозначим через $t_1, \ldots, t_n$ корни f в его поле разложения $\mathbb{K} \supset \Bbbk$. По теореме Виета элементы $a_i \in \Bbbk$ являются полиномами от t_i, и так как поле $\mathbb{K}$ алгебраично над $\Bbbk$, элементы $t_1, \ldots, t_n$ трансцендентно порождают[2] $\mathbb{K}$ как алгебру над $\mathbb{F}$. По сл. 1.3 на стр. 11 среди этих элементов можно выбрать базис трансцендентности поля $\mathbb{K}$ над $\mathbb{F}$. Так как $\operatorname{tr deg}_{\mathbb{F}} \mathbb{K} \geqslant n$, базисом трансцендентности поля $\mathbb{K}$ над $\mathbb{F}$ является весь набор $t_1, \ldots, t_n$. В частности, $t_1, \ldots, t_n$ алгебраически независимы над $\mathbb{F}$ и различны. Поэтому многочлен f сепарабелен, а его поле разложения $\mathbb{K} = \mathbb{F}(t_1, \ldots, t_n)$ является расширением Галуа поля $\Bbbk = \mathbb{F}(a_1, \ldots, a_n)$. Так как любая перестановка независимых переменных продолжается до автоморфизма поля рациональных функций, группа Галуа $\operatorname{Gal}\mathbb{K}/\Bbbk$ изоморфна S_n, и $[\mathbb{K} : \Bbbk] = n!$, а поле инвариантов $\mathbb{F}(t_1, \ldots, t_n)^{S_n} = \mathbb{F}(a_1, \ldots, a_n)$. Так как при $n \geqslant 5$ подгруппа $A_n \lhd S_n$ проста[3], группа S_n не разрешима, а значит, общее уравнение степени $n \geqslant 5$ не разрешимо в радикалах ни над каким полем $\mathbb{F}$ характеристики нуль. Этот результат известен как *теорема Абеля*[4].

Упражнение 4.13. Покажите, что поле инвариантов $\mathbb{K}^{A_n}$ подгруппы $A_n \lhd S_n$ является квадратичным расширением поля $\Bbbk$ элементом $\sqrt{D(f)} = \prod_{1 \leqslant i < j \leqslant n}(t_i - t_j)$.

Замечание 4.1. Отсутствие «общей» формулы для решения в радикалах полиномиального уравнения n-той степени не запрещает существования «конкетных» уравнений, корни которых выражаются через коэффициенты уравнения в радикалах.

Теорема 4.4
Пусть[5] $\operatorname{char}(\Bbbk) = 0$ и $f \in \Bbbk[x]$ приведён и неприводим. Если группа $\operatorname{Gal} f/\Bbbk$ разрешима, то все

[1] Как это делает, например, школьная формула $x_\pm = (p \pm \sqrt{p^2 - 4q})/2$ для решения «общего» квадратного уравнения $x^2 + px + q = 0$.

[2] См. n° 1.4 на стр. 10.

[3] См. раздел 11.1.1 на с. 188 лекций [Алг 1].

[4] Сам Абель доказал эту теорему для $\mathbb{F} = \mathbb{C}$ с привлечением комплексного анализа.

[5] Требование $\operatorname{char}(\Bbbk) = 0$ можно ослабить до требования, чтобы $\operatorname{char}(\Bbbk)$ не совпадала с порядком никакого композиционного фактора Жордана – Гёльдера группы Галуа многочлена f. Приводимое доказательство в этом случае тоже работает.

корни многочлена f выражаются через элементы поля $\Bbbk$ посредством четырёх арифметических действий и извлечения корней.

Доказательство. Обозначим через $\mathbb{K} \supset \Bbbk$ поле разложения многочлена f, а через $\mathbb{L} \supset \Bbbk$ результат присоединения к $\Bbbk$ первообразного корня степени $n = |\operatorname{Gal} \mathbb{K}/\Bbbk|$ из единицы. Все элементы поля $\mathbb{L}$ выражаются в радикалах через элементы поля $\Bbbk$. По предл. 3.2 на стр. 29 расширение $\mathbb{LK} \supset \mathbb{L}$ является расширением Галуа, и его группа Галуа G является подгруппой разрешимой группы $\operatorname{Gal} \mathbb{K}/\Bbbk$. Поэтому G тоже разрешима и имеет фильтрацию $G = G_0 \supset G_1 \supset \ldots \supset G_m = \{e\}$ с простыми циклическими факторами $G_i / G_{i+1} \simeq \mathbb{Z}/(p_i)$. Тем самым, поле $\mathbb{LK}$ получается из $\mathbb{L}$ последовательными циклическими расширениями Галуа. По теор. 4.2 на стр. 40 каждое такое расширение заключается в присоединении радикала. Поэтому все элементы поля $\mathbb{LK}$ выражаются в радикалах через элементы поля $\Bbbk$. □

Ответы и указания к некоторым упражнениям

Упр. 4.2. В силу мультипликативности символа Лежандра

$$\left[\frac{(-1)^{\frac{q-1}{2}}q}{p}\right] = \left[\frac{(-1)^{\frac{q-1}{2}}}{p}\right]\cdot\left[\frac{q}{p}\right] = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left[\frac{q}{p}\right].$$

Упр. 4.3. Воспользуйтесь тем, что

$$\operatorname{sp}(\zeta^m,\zeta^n) = \begin{cases} p-1, \text{ при } m+n\equiv 0\,(\mathrm{mod}\ p)\,,\\ -1, \text{ в остальных случаях}\,. \end{cases}$$

Упр. 4.4. Так как n обратимо по модулю p, существует такое k, что $\zeta^m = \zeta^{kn}$. Поэтому

$$\frac{1-\zeta^m}{1-\zeta^n} = \frac{1-\zeta^{kn}}{1-\zeta^n} = 1+\zeta^n+\ldots+\zeta^{(k-1)n}\in\mathcal{O}\,.$$

Меняя m и n ролями, заключаем, что $(1-\zeta^n)/(1-z^m)$ тоже лежит в $\mathcal{O}$.

Упр. 4.5. Многочлен $\mu_\vartheta\in\Bbbk[t]$, будучи минимальным многочленом числа ϑ, неприводим, и группа Галуа G транзитивно действует на его корнях $\vartheta_1,\ldots,\vartheta_d$, а стабилизатор каждого корня имеет порядок $|G|/d = n/d$. Поскольку χ_ϑ имеет те же самые корни и переводится в себя группой Галуа, транзитивно переставляющей эти корни друг с другом, $\chi_\vartheta = \prod(t-\vartheta_i)^{n/d} = \mu_\vartheta(t)^{n/d}$.

Упр. 4.7. Пусть $k = \min(\nu\in\mathbb{N}\mid \zeta^\nu\in G)$. Если $\zeta^\ell\in G$, где $\ell = kq+r$ и $0\leqslant r\leqslant k-1$, то $\zeta^r = \zeta^\ell(\zeta^k)^{-q}\in G$, откуда $r=0$, и $G = \{\zeta^{ki}\mid 0\leqslant i\leqslant n-1\}$, где $n = m/k = |G|$.

Упр. 4.9. Рассмотрим линейное соотношение $x_1\psi_1+\ldots+x_n\psi_n = 0$ между различными гомоморфизмами $\psi_\nu : G\to\Bbbk^\times$ с ненулевыми коэффициентами $x_i\in\Bbbk$ и минимально возможным числом слагаемых n, и пусть $\psi_1(h)\neq\psi_2(h)$ для некоторого $h\in G$. Так как для каждого $g\in G$ выполняется равенство $\sum_i x_i\psi_i(h)\psi_i(g) = \sum_i x_i\psi_i(hg) = 0$, мы получаем ещё одно линейное соотношение между функциями ψ_i с коэффициентами $x_i\,\psi_i(h)$. Деля все его коэффициенты на $\psi_1(h)$ и вычитая из исходного соотношения, получаем более короткую линейную зависимость между ψ_i с нулевым коэффициентом при ψ_1 и ненулевым коэффициентом при ψ_2. Противоречие.

Упр. 4.11. Воспользуйтесь равенствами

$$\begin{aligned} 0 &= (\alpha+\beta+\gamma)^3 = \alpha^3+\beta^3+\gamma^3+3(\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha+\alpha\beta^2+\beta\gamma^2+\gamma\alpha^2)+6\alpha\beta\gamma\\ 0 &= (\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\gamma\alpha) = \alpha^2\beta+\beta^2\gamma+\gamma^2\alpha+\alpha\beta^2+\beta\gamma^2+\gamma\alpha^2+3\alpha\beta\gamma\\ \delta &= (\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha)-(\alpha\beta^2+\beta\gamma^2+\gamma\alpha^2) \end{aligned}$$

и тем, что $\delta(\omega-\omega^2) = \delta\sqrt{-3} = \sqrt{-3D}$.

Упр. 4.12. Если все факторы ряда Жордана–Гёльдера $G = G_0\rhd G_1\rhd\ldots\rhd G_m = \{e\}$ абелевы, то $[G_i,G_i]\subset G_{i+1}$ при всех i, и ряд последовательных коммутантов заведомо тривиализуется через m шагов. Тривиализующийся на конечном шаге ряд из последовательных коммутантов представляет собой убывающую цепочку подгрупп с абелевыми факторами, как в форм. (4-10) на стр. 42. Наконец, если есть такая цепочка, то каждый её абелев фактор в свою очередь обладает композиционным рядом с простыми циклическими факторами. При помощи предложения 11.2 на с. 192 учебника [Алг 1] композиционные ряды для факторов соединяются в композиционный ряд группы G. Это доказывает равносильность трёх определений разрешимости. Второе и третье утверждения упражнения тоже вытекают из предложений 11.1 – 11.2 на с. 191 – 192 учебника [Алг 1].