Константиновский сборник

(специальный выпуск)

Теория Галуа и смежные вопросы теории полей для школьников

Коллектив авторов-составителей

Приложение к журналу «Математическое образование». Серия «Образование: учебно-методические материалы, история, персоналии, проблемы»

Выпуск 2 (11), декабрь 2025 г.

(исправленная и дополненная версия, июнь 2026 г.)

Москва, 2025–2026

Константиновский сборник

(специальный выпуск)

179

Теория Галуа и смежные вопросы теории полей для школьников

Коллектив авторов-составителей

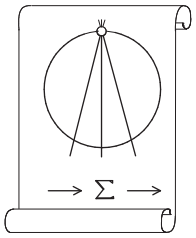
Приложение к журналу «Математическое образование». Серия «Образование: учебно-методические материалы, история, персоналии, проблемы»

Выпуск 2 (11), декабрь 2025 г.
(исправленная и дополненная версия, июнь 2026 г.)

Москва, 2025–2026

Приложение к журналу “Математическое образование”

ISSN 1992-6138



Издатель и учредитель: Фонд
математического образования и просвещения
117419 Москва, ул. Донская, д. 37

Редактор серии Комаров С.И.

Ответственный за выпуск Имайкин В.М.

Выпуск 2 (11), 2025 г. (исправленная и дополненная версия 2026 г.)

©“Математическое образование”, составление, 2025–2026 г.

Предлагаем вниманию читателей курс в листках для профильных старшеклассников по введению в теорию Галуа и смежные вопросы теории полей.

Адрес электронной почты для материалов: matob@yandex.ru

Подписано в печать 05.06.2026. Объем 5 п.л. Тираж 100 экз. Цена свободная.

Теория Галуа и смежные вопросы теории полей для школьников

Коллектив авторов-составителей

Содержание

Предисловие

Данный курс появился в ходе уникального педагогического эксперимента, проводимого командой преподавателей математики в ГБОУ Школа 179 г. Москвы в классе 8Б – 11Б, 2022 – 2026 гг.

На предмете “спецматематика” учащимся предлагается традиционный для данной школы курс математического анализы в листках. Листки по анализу перемежались немногочисленными листками алгебраического содержания с целью ознакомить детей с основными алгебраическими структурами, такими как группы, кольца, поля.

Состав класса оказался достаточно сильным, и дети хорошо справлялись с начальными алгебраическими листками. Постепенно у педагогов возникла мысль расширить алгебраическую часть курса вплоть до освоения основ теории Галуа — в этом суть данного эксперимента. Запас времени для данного класса достаточный, так как стандартный курс анализа рассчитан на два года, а в этом классе у педагогов 4 года — с 8 по 11 класс.

В результате сложился курс в листках для профильных старшеклассников по введению в теорию Галуа и смежные вопросы теории полей, который предлагается вниманию читателей.

Авторы-составители курса: Дубовицкий Александр Викторович, Дубовицкая Мария Александровна, Дубовицкая Наталья Викторовна, Комаров Станислав Игоревич.

Авторы выражают благодарность Д.А. Тимашеву и С.О. Горчинскому за то, что они любезно предоставили свои лекции, прочитанные на механико-математическом факультете МГУ имени М.В. Ломоносова, а также Е.В. Щепину, Л.Д. Беклемишеву, А.И. Бондалу и К.А. Шрамову за очень полезные консультации.

Сводка определений

Поскольку для успешного освоения курса необходимо интенсивно работать с определениями, мы выносим в начало курса сводку определений. В дальнейшем каждое из определений приведено в соответствующем листке. Дробные номера некоторых листков объяснены в предисловии к полным текстам листков, стр. 7.

Листок 0.

Определение 0.1. Пусть $n \in \mathbb{N}$. *Перестановкой* n элементов называется взаимно однозначное отображение множества $\{1, 2, \dots, n\}$ в себя (т.е. в это же множество). Перестановку σ записывают в виде таблицы $\begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$: в верхней строке перечислены элементы области определения, в нижней — их образы. Множество всевозможных перестановок n элементов называется *симметрической группой* S_n.

Определение 0.2. *Произведением* двух перестановок $\sigma, \tau \in S_n$ называется перестановка $\sigma\tau$, являющаяся композицией этих перестановок: $(\sigma\tau)(i) = \sigma(\tau(i))$.

Определение 0.3. *Тождественной перестановкой* называется такая перестановка e, что для всех $\sigma \in S_n$ верно $\sigma e = e\sigma = \sigma$.

Определение 0.4. *Циклической перестановкой* попарно различных элементов $a_1, a_2, \ldots, a_k$ называется перестановка $\begin{pmatrix} a_1 & a_2 & \ldots & a_{k-1} & a_k \\ a_2 & a_3 & \ldots & a_k & a_1 \end{pmatrix}$ — все не упомянутые здесь элементы, как обычно и считается в теории перестановок, переходят сами в себя. Коротко такую перестановку называют *циклом*, множество $\{a_1, a_2, \ldots, a_k\}$ — *орбитой* цикла, число k — *длиной* цикла. У цикла есть более компактная запись $(a_1\ a_2\ \ldots\ a_k)$.

Определение 0.5. Два цикла называются *независимыми*, если их орбиты не пересекаются.

Цикл $(i\ j)$ длины 2 называется *транспозицией*. Транспозиция вида $(i\ i{+}1)$ называется *элементарной*.

Определение 0.6. Говорят, что перестановки σ и τ *коммутируют*, если $\sigma\tau = \tau\sigma$.

Определение 0.7. Пусть дана перестановка $\begin{pmatrix} 1 & \ldots & \ldots & \ldots & n \\ \ldots & i & \ldots & j & \ldots \end{pmatrix}$. Говорят, что пара чисел i и j образуют *инверсию*, если $i > j$, но i встречается в нижней строке раньше, чем j. Число инверсий характеризует беспорядок в перестановке по отношению к обычному порядку. Перестановка называется *чётной*, если в ней количество инверсий чётно, или *нечётной*, если это количество нечётно.

Определение 0.8. Пусть $\sigma \in S_n$. Минимальное (если таковое существует) натуральное число k, для которого $\sigma^k = e$, называется *порядком* перестановки и обозначается $\operatorname{ord}\sigma$.

Листок 1.

Определение 1.1. *Операцией (бинарной операцией)* на множестве G называется отображение $\circ : G \times G \to G$.

Определение 1.2. У операции на множестве G выделяют следующие свойства:
– *коммутативность*: $a \circ b = b \circ a$;
– *ассоциативность*: $(a \circ b) \circ c = a \circ (b \circ c)$;
– *существование нейтрального элемента*: $\exists\, e \in G\ \forall\, a \in G$: $a \circ e = e \circ a = a$;
– *существование обратного элемента для* a: $\exists\, b \in G$: $a \circ b = b \circ a = e$, пишут $b = a^{-1}$.

Определение 1.3. Множество G с заданной операцией $\circ$ называется *группой*, если операция определена на всех упорядоченных парах элементов G, то есть $\circ : G \times G \to G$, при этом она ассоциативна на всех тройках элементов G, существует нейтральный элемент и любой элемент обратим. Если, кроме того, для любых двух элементов операция коммутативна, группа называется *коммутативной* или *абелевой*.

Определение 1.4. Пусть G — группа, $a \in G$. *Натуральная степень элемента* a определяется как $a^n = a \cdot \ldots \cdot a$, где количество множителей равно натуральному n. *Отрицательные степени* элемента a можно определить по формуле $a^{-n} = (a^n)^{-1}$, где n — натуральное. Считаем, что $a^0 = e$

Определение 1.5. Группа G с операцией $\circ$ *изоморфна* группе H с операцией $*$, если существует такая биекция $f : G \to H$, что для любых $a, b \in G$ $f(a \circ b) = f(a) * f(b)$. Обозначение: $G \cong H$.

Листок 2.

Определение 2.1. Пусть G — группа с операцией $\circ$. Если $A \subset G$ с той же операцией является группой, то A называется *подгруппой* группы G.

Определение 2.2. Пусть G — группа, $M = \{g_i \in G : i \in I\}$. Тогда $H = \langle M \rangle$ — обозначается *минимальная подгруппа*, содержащая M. Множество элементов M называется *системой образующих* для $\langle M \rangle$. (Проверяется, что такая подгруппа существует и единственна.)

Определение 2.3. Пусть G — группа и $\exists g \in G : G = \langle g \rangle$. Тогда G называется *циклической группой, порожденной элементом* g.

Определение 2.4. Пусть H — подгруппа группы G. Множество элементов вида $\{gh \ : g \in G, h \in H\}$ называется *левым смежным классом* gH (g фиксировано, h пробегает всю подгруппу H). Аналогично определяется *правый смежный класс* Hg.

Определение 2.5. Пусть G — группа, $a \in G$. Тогда $|\langle a \rangle|$ называется **порядком** элемента a.

Определение 2.6. Пусть G — группа, H — ее подгруппа, G/H — разбиение на левые и правые смежные классы. Тогда $|G/H|$ называется *индексом* H в группе G. (Проверяется, что это число не зависит от того, какие классы берутся — левые или правые.)

Листок 3.

Определение 3.1. Множество K с операциями сложения и умножения называется *кольцом*, если выполняются следующие свойства:

– K — абелева группа по сложению (называется *аддитивной группой* кольца K);

– $a(b + c) = ab + ac$; $(a + b)c = ac + bc$ (дистрибутивность умножения относительно сложения).

Кольцо называется *коммутативным кольцом с единицей*, если операция умножения коммутативна и существует единичный элемент по умножению. Допустимо иметь в кольце всего один элемент.

Определение 3.2. *Полем* называется коммутативное кольцо с единицей, в котором больше одного элемента и каждый ненулевой элемент обратим по умножению.

Определение 3.3. Пусть K — кольцо с единицей и $a \in K$. Элемент a называется *обратимым*, если существует $a^{-1} \in K$ такой, что $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Определение 3.4. Пусть K — кольцо, $a, b \in K$. Если $a \neq 0$ и $b \neq 0$, но $ab = 0$, то a называется *левым делителем нуля*, а b — *правым*. В коммутативном кольце левые и правые делители нуля не различаются.

Определение 3.5. Пусть P — поле и существует такое n, что $n \cdot 1 = 0$. Тогда минимальное натуральное число с этим свойством называют *характеристикой поля*. Если такого n не существует, то говорят, что поле P имеет *нулевую характеристику*. Обозначение: $char\, P$.

Листок 4.

Определение 4.1. Пусть G — группа с операцией $*$, G' — группа с операцией $\circ$. Отображение $\varphi : G \to G'$ называется *гомоморфизмом*, если $\varphi(a * b) = \varphi(a) \circ \varphi(b)$ для любых $a, b \in G$.

Определение 4.2. Пусть $\varphi : G \to G'$ — гомоморфизм. Определим множества:

$Ker\, \varphi = \{g \in G \,|\, \varphi(g) = e'\}$ (e' — единица группы G') — *ядро* гомоморфизма φ.

$\mathrm{Im}\, \varphi = \{g' \in G' \,|\, \exists\, g \in G : g' = \varphi(g)\}$ — *образ* гомоморфизма φ.

Определение 4.3. Пусть H — подгруппа группы G. Если для любого $h \in H$ и для любого $g \in G$ $ghg^{-1} \in H$, то подгруппа H называется *нормальной*. Обозначение: $H \triangleleft G$.

Можно проверить, что для любого гомоморфизма φ $Ker\, \varphi$ является нормальной подгруппой.

Определение 4.4. Пусть G — группа, $H \triangleleft G$. На множестве смежных классов (обозначение: G/H) введём операцию *произведения классов*: $g_1H \circ g_2H = g_1g_2H$.

Определение 4.5. Группа G/H с операцией из предыдущего определения называется *факторгруппой* группы G по подгруппе H.

Листок 5.

Определение 5.1. Пусть X — множество. Обозначим через $\mathrm{Aut}\, X$ группу всех взаимно однозначных отображений из X в себя. Любая подгруппа G группы $\mathrm{Aut}\, X$ называется *группой преобразований* множества X.

Определение 5.2. Пусть G — группа преобразований множества X (не обязательно всех). Будем говорить, что точки $x, y \in X$ *эквивалентны* относительно G, и писать $x \underset{G}{\sim} y$, если существует такое преобразование $g \in G$, что $gx = y$.

Определение 5.3. Подмножество элементов группы G, оставляющих точку x на месте, называется *стабилизатором* точки x и обозначается $St(x)$. Иначе, $St(x) = \{g \in G : gx = x\}$.

Определение 5.4. Гомоморфизм $G \xrightarrow{\varphi} \operatorname{Aut} X$ называется *действием* группы G на множестве X или *представлением* группы G автоморфизмами множества X. Если понятно, о каком действии идёт речь, то результат применения отображения $\varphi(g) : X \to X$ к точке $x \in X$ обозначается просто через gx.

Листок 6.

Определение 6.1. Пусть I — подгруппа по сложению коммутативного кольца K, т.ч. $\forall\, h \in I$ и $\forall\, x \in K$ $xh \in I$. Тогда I называется *идеалом* кольца K. В любом ненулевом кольце K есть, по крайней мере, два идеала: $\{0\}$ и K, которые называются *тривиальными*. Пусть I — идеал кольца $\mathcal{R}$. Элементы $a, b \in \mathcal{R}$ называются *сравнимыми по идеалу* I, если $a - b \in I$. Пишут: $a \equiv b \pmod{I}$.

Определение 6.2. *Идеал в K, порождённый множеством элементов A* — это множество всех элементов $x \in K$, т.ч. $x = u_1 a_1 + \ldots + u_t a_t$, где $u_1, \ldots, u_t \in K$, $a_1, \ldots, a_t \in A$. Обозначение $<A>$.

Если идеал порождён одним элементом $a \in K$, то он называется *главным*. Ясно, что $<a> = a \cdot K$.

Определение 6.3. Кольцо, в котором все идеалы — главные, называется *кольцом главных идеалов*.

Определение 6.4. Идеал I кольца K называется *максимальным*, если для любого идеала H из $I \subset H$ следует $H = I$ или $H = K$.

Определение 6.5. Идеал I в кольце K называется *простым*, если $\forall a, b \in K$ из $ab \in I$ и $a \notin I$ следует $b \in I$.

Листок 7.

Определение 7.1. Коммутативное ассоциативное кольцо с единицей без делителей нуля называется *областью целостности*.

Определение 7.2. Пусть R — область целостности, $N : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ — функция со следующими свойствами:

1) $\forall\, a, b \in R, a \neq 0, b \neq 0$ $N(ab) \geqslant N(a)$;

2) $\forall\, a, b \in R, a \neq 0$ существует представление, не обязательно единственное, вида $b = aq + r$, где $r = 0$ или $N(r) < N(a)$.

Тогда R называется *евклидовым кольцом*, а N — *евклидовой нормой*.

Определение 7.3. Пусть $c \in R$ — обратим (т.е. $\exists\, d \in R$ $cd = 1$). Тогда если $a = bc$, то элементы a и b называют *ассоциированными*.

Определение 7.4. Будем говорить, что элемент $d \in R$ *делит* $a \in R$, и писать $d|a$, если $\exists\, b \in R$ такой, что $a = db$.

Определение 7.5. Для любых $a, b \in R$ *наибольшим общим делителем* (обозначается НОД(a, b), иногда (a, b)) называется $d \in R$, удовлетворяющий условиям: 1) $d|a$, $d|b$; 2) $c|a$, $c|b \Rightarrow c|d$.

Определение 7.6. Кольцом *целых гауссовых чисел* $\mathbb{Z}[i]$ называется подмножество комплексных чисел вида $a + bi$, $a, b \in \mathbb{Z}$, с естественными операциями сложения и умножения.

Определение 7.7. Пусть $p \in R, p \neq 0$, причём p необратим. Если из равенства $p = ab$ следует, что a или b обратим, то элемент p называется *простым* (или *неразложимым*).

Простые элементы кольца многочленов $P[x]$ над полем P называются *неприводимыми* многочленами.

Определение 7.8. Область целостности R называется *факториальным кольцом*, если любой ненулевой элемент $a \in R$ можно представить в виде $a = up_1 \dots p_r$, где u — обратимый, $p_1, \dots, p_r$ — простые, причём любые два таких разложения совпадают с точностью до ассоциированных элементов.

Листок 7,25.

Определение 7,25.1. Пусть G — группа, x, $y \in G$. *Коммутатором элементов* x и y называется элемент $[x,\ y] = xyx^{-1}y^{-1}$.

Определение 7,25.2. Пусть G — группа. Тогда подгруппа, порожденная всеми коммутаторами из G, называется *коммутантом* и обозначается G'.

Определение 7,25.3. Пусть G — группа, $G^{(1)} = G'$, $G^{(2)} = G^{(1)'}$, $\dots$, $G^{k+1} = G^{k'}$. Тогда G^k называется *k-кратным коммутантом*.

Определение 7,25.4. Группа G называется *разрешимой*, если для некоторого $m \in \mathbb{N}$ $G^{(m)} = e$.

Листок 7,5.

Определение 7,5.1. Образующие в группе корней n-й степени из единицы называются *первообразными корнями* n-й степени из единицы.

Определение 7,5.2. *Круговым многочленом* называется многочлен

$$\Phi_n(x) = \prod_{\xi i}(x - \xi_i),$$

где ξi — первообразные корни из единицы n-й степени.

Листок 8.

Определение 8.1. *Внешней прямой суммой* абелевых групп $A_1, A_2, \dots, A_k$ называется множество $A_1 \times A_2 \times \dots \times A_k$ с покомпонентной операцией сложения. Обозначение: $A_1 \oplus A_2 \oplus \dots \oplus A_k$.

Определение 8.2. Говорят, что абелева группа A *разлагается в прямую сумму* подгрупп $A_1, A_2, \dots, A_k$, если для любого $a \in A$ существует и притом единственное представление $a = a_1 + a_2 + \dots + a_k$, где $a_i \in A_i$. Иначе это называют *внутренней прямой суммой*. Обозначение такое же, как и для внешней прямой суммы: $A = A_1 \oplus A_2 \oplus \dots \oplus A_k$.

Определение 8.3. Конечная абелева группа, порядок которой есть степень простого числа p, называется *примарной* или *p-группой*.

Листок 8,5.

Определение 8,5.1. Пусть R_1 и R_2 — кольца с единицей. Отображение $\varphi : R_1 \to R_2$ называется *гомоморфизмом*, если для любых x, $y \in R_1$ выполнены условия:
1) $\varphi(x + y) = \varphi(x) + \varphi(y)$
2) $\varphi(xy) = \varphi(x)\varphi(y)$
3) $\varphi(1_1) = 1_2$.

Определение 8,5.2. Пусть E, L — поля, $E \subset L$, операции, ноль и единица в E и L одни и те же. Тогда E называется *подполем* L, а L — *расширением* поля E.

Определение 8,5.3. Пусть $\varphi : E \to P$ — гомоморфизм полей. Тогда отображение $h^\varphi : E[x] \to P[x]$, сопоставляющее многочлену $f(x) = a_0x^n + \dots + a_{n-1}x + a_n \in E[x]$ многочлен $f_\varphi(x) = \varphi(a_0)x^n + \dots + \varphi(a_{n-1})x + \varphi(a_n) \in P[x]$, называется *индуцированным гомоморфизмом*.

Определение 8,5.4. Пусть P — поле. *Минимальным подполем поля* P называется пересечение всех подполей поля P.

Определение 8,5.5. *Автоморфизмом поля* P называется изоморфизм $P \to P$.

Определение 8,5.6. Пусть $P \subset L$ — расширение поля P, $a_1, \ldots, a_s \in L$. Говорят, что *поле L порождено элементами $a_1, \ldots, a_s$*, и пишут $L = P(a_1, \ldots, a_s)$, если в L нет меньшего подполя, содержащего P и $a_1, \ldots, a_s$. Поле L называют *конечно порожденным над P*. Если $L = P(a)$, то расширение называют *простым*, а элемент a — *примитивным элементом*.

Определение 8,5.7. Пусть $P \subset L$ — расширение полей. Элемент $a \in L$ называется *алгебраическим над P*, если существует ненулевой многочлен $f \in P[x]$, такой, что $f(a) = 0$.

Определение 8,5.8. Многочлен со старшим коэффициентом 1, образующий идеал I_a, называется *минимальным многочленом элемента a* и обозначается μ_a.

Листок 9.

Определение 9.1. См. определение 8,5.2.

Определение 9.2. См. определение 8,5.6.

Определение 9.3. Если $F \subset E$ — расширение поля F, то символом $[E : F]$ мы обозначаем размерность векторного пространства $\dim_F E$, которая называется *степенью расширения*. Если степень расширения конечна, т.е. $[E : F] < \infty$, то такое расширение называют *конечным*.

Определение 9.4. Пусть $F \subset E$ — расширение поля F и $a \in E$. Если $\exists\, f(x) \in F[x]$ такой, что $f(a) = 0$ и $f \not\equiv 0$, то элемент a называется *алгебраическим* над F.

Определение 9.5. Пусть $F \subset E$ — расширение поля F и $a \in E$ — алгебраический над F. Единственный многочлен $f(x) \in F[x]$, неприводимый и нормализованный (старший коэффициент равен 1), т.ч. $f(a) = 0$, мы будем называть *минимальным многочленом* элемента a и обозначать $\mu_a(x)$.

Определение 9.6. Расширение полей $F \subset E$ называется *алгебраическим*, если $\forall\, a \in E$ a — алгебраический над F.

Определение 9.7. Поле F называется *алгебраически замкнутым*, если степень любого неприводимого многочлена из $F[x]$ не больше 1.

Определение 9.8. Конечное расширение поля рациональных чисел называется *полем алгебраических чисел*.

Листок 10.

Определение 10.1. Пусть K — поле, $f \in K[x]$, $\deg f > 0$. *Поле разложения многочлена* — это такое расширение $F \supset K$, для которого f разлагается на линейные множители и не существует промежуточных полей $F \supset M \supset K$ с тем же свойством.

Определение 10.2. Пусть P — поле, $f \in P[x]$ — неприводимый, $P \subset F$ — расширение полей, в котором $f(x)$ разлагается на линейные множители, α и β — корни $f(x)$. Тогда поля $P(\alpha)$ и $P(\beta)$ называются *сопряжёнными*, а множество корней $f(x)$ — *классом сопряжённых элементов*.

Определение 10.3. Расширение $E \subset F$ называется *нормальным*, если $\forall\, a \in F$ $\mu_a(x)$ разлагается на линейные множители.

Определение 10.4. Гомоморфизм алгебраической структуры (группы, кольца, поля и т.д.) в себя называется

– *мономорфизмом*, если он инъективен;

– *эндоморфизмом*, если он сюръективен;

– *автоморфизмом*, если он инъективен и сюръективен.

Определение 10.5. Автоморфизм $\Phi : x \to x^p$ в конечных полях характеристики p называется *автоморфизмом Фробениуса*.

Определение 10.6. Поле из p^n элементов обозначается $GF(p^n)$ — *Galois Field* — и называется *полем Галуа*.

Определение 10.7. Пусть $F \subset K$ — расширение полей. Тогда $Aut\,(K/F) = \{\varphi : K \to K$ — автоморфизм, т.ч. $\varphi|_F = id.\}$

Листок 11.

Определение 11.1. Расширение $L \supset K$ называется *расширением Галуа́*, если $|\mathrm{Aut}(L/K)| = [L : K]$.

В случае расширения Галуа группа автоморфизмов $\mathrm{Aut}(L/K)$ называется *группой расширения Галуа* и обозначается $\mathrm{Gal}(L/K)$.

Определение 11.2. Пусть $L \supset K$ — конечное расширение, $H \subseteq G = \mathrm{Aut}(L/K)$ — подгруппа. Тогда *полем инвариантов* H называется $L^H = \{a \in L \,|\, \varphi(a) = a, \forall\, \varphi \in H\}$.

Определение 11.3. Пусть K — поле. $f \in K[x]$ называется *сепарабельным*, если f не имеет кратных корней ни на каком расширении поля K.

Определение 11.4. Пусть $K \subset L$ — расширение полей. $a \in L$ *сепарабелен* над K, если a — корень сепарабельного многочлена $f \in K[x]$.

Определение 11.5. $K \subset L$ — расширение полей — называется *сепарабельным*, если $\forall\, a \in L$ a сепарабельно.

Определение 11.6. Поле K называется *совершенным*, если $char\, K = 0 \vee char\, K = p$ и $\forall\, a \in K$ $\exists\, b \in K$: $b^p = a$.

Листок 12.

Определение 12.1. Пусть K — поле, $f \in K[x]$. Тогда $L = K(f)$ — *поле разложения* $f(x)$.

Определение 12.2. Пусть G — группа, S — множество всех подгрупп G, I_g — действие G на S сопряжением, т.е. $\forall\, g \in G$ $I_g(H) = gHg^{-1}$ $\forall\, H \subset G$. Назовём *нормализатором* подгруппы H стабилизатор при действии сопряжением, т.е. $N_G(H) = N(H) = \{g \in G : gHg^{-1} = H\}$.

Листок 13.

Определение 13.1. Расширение полей $K \subset F$ называется *радикальным*, если существует башня расширений $K = K_0 \subset K_1 \subset \ldots \subset K_{i-1} \subset K_i = K_{i-1}(b_i) \subset \ldots \subset K_s = F$, где $b_i^{n_i} \in K_{i-1}$ для некоторого $n_i \in \mathbb{N}$.

Определение 13.2. Уравнение $f(x) = 0$ *разрешимо в радикалах*, если $K(f) \subseteq F$, $F \supseteq K$ — радикальное расширение поля K.

Определение 13.3. Пусть G — группа. Назовём *центром* группы G

$$Z(G) = \{x \in G : xy = yx\ \forall\, y \in G\}.$$

Листок 14.

Определение 14.1. *Алгоритмом построения циркулем и линейкой* назовём описание конечной последовательности элементарных построений, в которых разрешается:

• провести прямую через две уже отмеченные точки;

• отметить точку пересечения двух уже проведённых прямых;

• провести окружность с центром в отмеченной точке и радиусом, равным расстоянию между двумя отмеченными точками;

• отметить точку пересечения уже проведённой прямой и уже построенной окружности;

• отметить точку пересечения двух уже построенных окружностей.

Листок 16.

Определение 16.1. Пусть p — простое число. Последовательность

$$\{x_n\} = \{x_0, x_1, x_2, \ldots, x_n, \ldots | x_i \in \mathbb{Z}\ \forall i \bigwedge x_n \equiv x_{n-1} (\mathrm{mod}\ p^n)\ \forall n \geq 1\}$$

называется *целым p-адическим числом*. Две последовательности $\{x_n\}$ и $\{x'_n\}$ определяют одно и то же p-адическое число тогда и только тогда, когда $x_n \equiv x'_n (\mathrm{mod}\ p^{n+1})\ \forall n \geq 0$.

Определение 16.2. Пусть $\alpha \in \mathbb{Z}_p$ и $\alpha = \{x_0, x_1, \ldots | x_i \in \mathbb{Z}\}$. Назовём *канонической записью* такую последовательность $\{x'_0, x'_1, \ldots\}$: $x_n \equiv x'_n (\mathrm{mod}\ p^{n+1})\ \forall n \geq 0$ и $\forall x'_n\ 0 \leq x'_n < p^{n+1}$.

Определение 16.3. Пусть $\alpha,\ \beta \in \mathbb{Z}_p\ \alpha = \{x_0, x_1, \ldots\}\ \beta = \{y_0, y_1, \ldots\}$. Тогда *сумма* $\alpha + \beta = \{x_0 + y_0, x_1 + y_1, \ldots\}$, а *произведение* $\alpha \cdot \beta = \{x_0 y_0, x_1 y_1, \ldots\}$.

Определение 16.4. Пусть $\alpha, \beta \in \mathbb{Z}_p$. Будем говорить, что α *делит* β $(\alpha|\beta)$, если $\exists \gamma \in \mathbb{Z}_p : \beta = \alpha\gamma$.

Определение 16.5. Пусть $\alpha \in \mathbb{Z}_p$. α называется *обратимым* или *делителем единицы*, если $\exists \beta \in \mathbb{Z}_p : \alpha\beta = 1$.

Определение 16.6. Пусть $\alpha \in \mathbb{Z}_p$, $\alpha = p^m \cdot \varepsilon$, где ε – делитель единицы. Тогда m называется *p-показателем* α и обозначается $\nu_p(\alpha)$.

Определение 16.7. Поле отношений $\mathbb{Z}_p$ называется *полем p-адических чисел* и обозначается $\mathbb{Q}_p$, а его элементы называются *p-адическими числами*.

Определение 16.8. Пусть F – поле, $||\ || : F \to \mathbb{R}^+$, т.ч.

1) $||x|| = 0 \Leftrightarrow x = 0$;

2) $||xy|| = ||x|| \cdot ||y||$;

3) $||x + y|| \leqslant ||x|| + ||y||$.

Тогда функция $||\ ||$ называется *нормой* на поле F.

Если выполняется 3'), то норма называется *неархимедовой*, иначе она называется *архимедовой*:

3') $||x + y|| \leqslant \max(||x||, ||y||)$.

Определение 16.8. Пусть $\xi \in \mathbb{Q}_p$, $||\ ||_p$: $\mathbb{Q}_p \to \mathbb{R}^+$: $||\xi||_p \stackrel{\text{def}}{=} p^{-\nu(\xi)}$. Тогда $||\ ||_p$ называется *p-адической нормой*.

Определение 16.9. Пара (X, ρ) называется *метрическим пространством*, где X — множество, если функция $\rho : (X \times X) \to \mathbb{R}^+$ (называемая *метрикой*) удовлетворяет следующим условиям 1)-3):

1) $\rho(x, y) = 0 \Leftrightarrow x = y$;

2) $\rho(x, y) = \rho(y, x)$;

3) $\rho(x, z) \leq \rho(x, y) + \rho(y, z)$.

Если выполняется 3'), то метрика ρ называется *неархимедовой*:

3') $\rho(x, z) \leqslant \max(\rho(x, z), \rho(y, z))$.

Определение 16.10. *p-адической метрикой* на $\mathbb{Q}_p$ называется функция $\rho(x, y) \stackrel{\text{def}}{=} ||x - y||_p$, где $x, y \in \mathbb{Q}_p$.

Листок 17.

Определение 17.1. $\exists \gamma = \lim\limits_{n\to\infty} c^{p^n}$ в $\mathbb{Q}_p$; $\quad \gamma = c\,(\mathrm{mod}\, p)$; $\quad \gamma^{p-1} = 1$ в $\mathbb{Q}_p$, т.е. $\gamma_1, \ldots, \gamma_{p-1}$ — корни уравнения $x^{p-1} - 1 = 0$.

Числа $\gamma_1, \ldots, \gamma_{p-1}$ называются *представителями Тейхмю́ллера* в $\mathbb{Q}_p$.

Определение 17.2. Метрики в поле F называются *эквивалентными*, если множества бесконечно малых последовательностей совпадают.

Определение 17.3. Норма $||\ ||$ на поле F называется *тривиальной*, если $\forall\, x \neq 0\ ||x|| = 1$.

Листок 18.

Определение 18.1. Множество называется *бесконечным по Дедеки́нду*, если оно равномощно некоторому своему собственному подмножеству.

Определение 18.2. Бинарное отношение $\leq$ на множестве X называется *отношением частичного порядка*, если выполняются следующие свойства:

– *рефлексивность*: $x \leq x\ \forall\ x \in X$;

– *антисимметричность*: $(x \leq y$ и $y \leq x) \Rightarrow x = y$;
– *транзитивность*: $(x \leq y$ и $y \leq z) \Rightarrow x \leq z$.

Множество с заданным на нём отношением частичного порядка называют *частично упорядоченным множеством* (ЧУМ).

Определение 18.3. Два элемента ЧУМ называются *сравнимыми*, если $x \leq y$ или $y \leq x$. ЧУМ, в котором любые два элемента сравнимы, называется *линейно упорядоченным множеством*.

Определение 18.4. Линейно упорядоченное подмножество ЧУМ называется *цепью*.

Определение 18.5. Пусть $A \subset X$, X — ЧУМ. Тогда элемент $x \in X$: $a \leqslant x \ \forall\, a \in A$ называется *верхней гранью* A.

Определение 18.6. Пусть X — ЧУМ. Элемент $a \in X$ называется *максимальным*, если не существует большего элемента.

Определение 18.7. Пусть L — бесконечномерное линейное пространство.

Множество векторов называется *линейно независимым*, если никакая линейная комбинация конечного числа векторов из этого множества не равна нулю.

Линейно независимое множество векторов называется *базисом Га́меля* пространства L, если любой вектор представим в виде конечной линейной комбинации элементов базиса.

Листки, как они есть

Здесь мы приводим листки в том виде, в каком они раздавались учащимся 8 (22/23 г.) – 11 (25/26 г.) классов на предмете "Математический анализ". Даем их сквозную нумерацию с указанием фактического номера листка в процессе обучения. На предмете "Алгебра" также было роздано несколько листков по этой тематике. Если листок по анализу опирается на результаты некоторого листка по алгебре, этот алгебраический листок включен в данную подборку с дробным номером.

Большинство эпиграфов добавлено при составлении данной подборки.

0. Перестановки (листок 21, 8 класс)

Определение 0.1. Пусть $n \in \mathbb{N}$. *Перестановкой* n элементов называется взаимно однозначное отображение множества $\{1, 2, \ldots, n\}$ в себя (т.е. в это же множество). Перестановку σ записывают в виде таблицы $\begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}$: в верхней строке перечислены элементы области определения, в нижней — их образы. Множество всевозможных перестановок n элементов называется *симметрической группой* S_n.

Определение 0.2. *Произведением* двух перестановок $\sigma, \tau \in S_n$ называется перестановка $\sigma\tau$, являющаяся композицией этих перестановок: $(\sigma\tau)(i) = \sigma(\tau(i))$.

Обратите внимание, что к аргументу применяется сначала второй множитель, а к его результату — первый.

Для $k \in \mathbb{N}$ и $\sigma \in S_n$ запись $\sigma\sigma \ldots \sigma\sigma$ (k множителей) записывают как σ^k и называют *k-й степенью* перестановки σ.

Покажем, как устроено произведение перестановок.

Для примера возьмём $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ и $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 4 & 1 & 2 & 3 \end{pmatrix}$.

Проверьте, что две последних записи означают одну и ту же перестановку!

Тогда $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$.

Задача 0.1. а) Пусть $\xi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$, $\zeta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$. Вычислите $\xi\zeta$ и $\zeta\xi$.

б) При каком наименьшем n в группе S_n найдутся две такие перестановки α, β, что $\alpha\beta \neq \beta\alpha$?

в) Докажите, что операция произведения перестановок ассоциативна.

Определение 0.3. *Тождественной перестановкой* называется такая перестановка e, что для всех $\sigma \in S_n$ верно $\sigma e = e\sigma = \sigma$.

Если $\sigma \in S_n$, то *обратной* к ней называется такая перестановка σ^{-1}, что $\sigma\sigma^{-1} = \sigma^{-1}\sigma = e$.

Задача 0.2. а) Докажите, что в группе S_n существует тождественная перестановка, причём единственная. Выпишите её явный вид.

б) Докажите, что если $\alpha\sigma = e$, то $\sigma\alpha = e$.

в) Докажите, что у всякой перестановки $\sigma \in S_n$ есть обратная, причём единственная. Покажите, как восстановить явный вид σ^{-1} по виду σ.

Определение 0.4. *Циклической перестановкой* попарно различных элементов $a_1, a_2, \ldots, a_k$ называется перестановка $\begin{pmatrix} a_1 & a_2 & \ldots & a_{k-1} & a_k \\ a_2 & a_3 & \ldots & a_k & a_1 \end{pmatrix}$ — все не упомянутые здесь элементы, как обычно и считается в теории перестановок, переходят сами в себя. Коротко такую перестановку называют *циклом*, множество $\{a_1, a_2, \ldots, a_k\}$ — *орбитой* цикла, число k — *длиной* цикла. У цикла есть более компактная запись $(a_1\ a_2\ \ldots\ a_k)$.

Определение 0.5. Два цикла называются *независимыми*, если их орбиты не пересекаются.

Цикл $(i\ j)$ длины 2 называется *транспозицией*. Транспозиция вида $(i\ i{+}1)$ называется *элементарной*.

Определение 0.6. Говорят, что перестановки σ и τ *коммутируют*, если $\sigma\tau = \tau\sigma$.

Задача 0.3. Верно ли, что:

а) если два цикла независимы, то они коммутируют;

б) если два цикла коммутируют и имеют одинаковую длину, то они независимы;

в) если два цикла коммутируют и имеют разную длину, то они независимы?

Задача 0.4. Докажите, что:

а) всякую перестановку можно разложить в произведение независимых циклов;

б) всякая перестановка может быть разложена в произведение транспозиций;

в) всякая перестановка может быть разложена в произведение элементарных транспозиций;

г) всякую перестановку можно разложить в произведение транспозиций вида $(1\ k)$;

д) всякая перестановка разложима в произведение множителей двух видов: $(1\ 2)$ и $(1\ 2\ \ldots\ n)$.

В пунктах б), в), г), д) один и тот же сомножитель может появиться в разложении несколько раз.

Задача 0.5. а) Разложите перестановки $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 7 & 2 & 4 & 3 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 8 & 9 & 5 & 1 & 4 & 3 & 2 & 7 \end{pmatrix}$ в произведение независимых циклов.

б) Разложите перестановки $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$ и $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ в произведение транспозиций.

в) Разложите циклы $(2\ 3\ 4)$ и $(1\ 2\ 3\ 4)$ в произведение транспозиций вида $(1\ k)$.

Задача 0.6. Несколько жителей города N хотят обменяться квартирами. У каждого есть по квартире, но каждый хочет переехать в другую (разные люди хотят переехать в разные квартиры). По законам города разрешены только парные обмены: если два человека обмениваются квартирами, то в тот же день они не участвуют в других обменах. Докажите, что можно устроить парные обмены так, что уже через два дня каждый будет жить в той квартире, куда он хотел переехать.

Задача 0.7. Набор перестановок $A \subset S_n$ называется набором *образующих* для S_n, если всякая перестановка $\sigma \in S_n$ раскладывается в произведение элементов этого набора.

а) Какое наименьшее количество элементов может иметь набор образующих для S_n при $n > 2$?

б) Отберём из наборов образующих те, которые состоят исключительно из транспозиций. Какое наименьшее количество элементов может иметь отобранный набор образующих для S_n при $n > 2$?

Определение 0.7. Пусть дана перестановка $\begin{pmatrix} 1 & \dots & \dots & \dots & n \\ \dots & i & \dots & j & \dots \end{pmatrix}$. Говорят, что пара чисел i и j образуют *инверсию*, если $i > j$, но i встречается в нижней строке раньше, чем j. Число инверсий характеризует беспорядок в перестановке по отношению к обычному порядку. Перестановка называется *чётной*, если в ней количество инверсий чётно, или *нечётной*, если это количество нечётно.

Задача 0.8. а) Найдите число инверсий в перестановке $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$.

б) Докажите, что если в перестановке поменять местами два произвольных элемента, то чётность перестановки изменится.

в) Докажите, что чётная перестановка может быть разложена в произведение только чётного числа транспозиций, а нечётная — в произведение только нечётного числа транспозиций.

г) Докажите, что перестановки σ и σ^{-1} имеют одинаковую чётность.

д) Каких перестановок в S_n больше: чётных или нечётных?

Задача 0.9. Определите чётность перестановки:

а) $\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ n & n-1 & n-2 & \dots & 2 & 1 \end{pmatrix}$; **б)** $\begin{pmatrix} 1 & 2 & 3 & \dots & \dots & \dots & \dots & n \\ 1 & 3 & 5 & \dots & 2 & 4 & 6 & \dots \end{pmatrix}$; **в)** $(i_1\ i_2\ i_3\ \dots\ i_k)$.

Определение 0.8. Пусть $\sigma \in S_n$. Минимальное (если таковое существует) натуральное число k, для которого $\sigma^k = e$, называется *порядком* перестановки и обозначается $\operatorname{ord}\sigma$.

Задача 0.10. а) Докажите, что для всякой перестановки $\sigma \in S_n$ существует хотя бы одно (а значит, существует и минимальное) натуральное k, для которого $\sigma^k = e$.

б) Пусть перестановка $\sigma \in S_n$ разложена в произведение независимых циклов, длины которых известны. Покажите, как по этим данных вычислить порядок перестановки.

в) Докажите, что для любой перестановки $\sigma \in S_n$ верно, что $n!$ делится на $\operatorname{ord}\sigma$.

Задача 0.11. Рассмотрим четыре группы перестановок: чётные перестановки чётного порядка, чётные нечётного порядка, нечётные чётного и нечётные нечётного. Выясните, какие из этих групп пусты, а какие — нет, если:

а) $n = 1, 2, 3$; б) $n = 4, 5, 6$; в) $n \geqslant 7$.

Задача 0.12. Можно ли в группе а) S_3; б) S_4 взять по одному разу все перестановки и перемножить их в таком порядке, что результат окажется тождественной перестановкой?

1. Операции на множестве. Группы. Изоморфизм групп (листок 23, 8 класс)

Замечание 1.1. В школе (и не только) вы постоянно встречаетесь с операциями над парами объектов (парами элементов множества): сложение, вычитание, умножение, деление двух чисел; сложение и вычитание пары масс, сил или скоростей; сложение и умножение двух матриц; сложение и умножение двух многочленов; сложение и умножение двух остатков по фиксированному модулю; умножение перестановок. В этом листке формализуется понятие операции и вводится понятие группы, как множества с операцией, удовлетворяющей некоторым выделенным свойствам.

Определение 1.1. *Операцией (бинарной операцией)* на множестве G называется отображение $\circ : G \times G \to G$.

Менее формально: операция на множестве — это сопоставление упорядоченным парам элементов этого множества некоторого элемента (однозначно определенного) этого же множества. Пишут так: $a \circ b = c$, то есть упорядоченной паре $(a; b)$ поставлен в соответствие элемент c. На одном и том же множестве можно вводить разные операции. Например, “Деление” $a : b$ определяется для каждого “умножения” $\circ$ привычным образом: $a : b = c$, если $a = c \circ b$. Другое важное определение “деления”, эквивалентное данному, будет дано ниже.

Задача 1.1. Какие из операций сложения, вычитания, умножения и деления определены для всех упорядоченных пар множества

а) натуральных чисел;

б) целых чисел;

в) "привычных" рациональных чисел;

г) многочленов с целыми коэффициентами?

Замечание 1.2. Операцию на конечных множествах можно задавать таблицей "умножения": строки и столбцы "нумеруются" элементами множества, на пересечении строки элемента a и столбца элемента b записывается элемент c, равный $a \circ b$. Для операции, определенной на всем множестве, должны быть заполнены все клетки таблицы.

Задача 1.2. Составьте, если это возможно, таблицы для данных операций на данных множествах:

а) умножение и деление на множестве чисел $\{-1; 1\}$, множестве перестановок S_2 и множестве ненулевых остатков по модулю 3;

б) умножение и деление на множестве чисел $\{-1; 0; 1\}$, сложение и вычитание на множестве остатков по модулю 3;

в) сложение и умножение на множестве остатков (вычетов) по модулю 4 и по модулю 5;

г) умножение на подмножестве $\{\sigma_0; \sigma_1; \sigma_2; \sigma_3\}$ перестановок S_4: $\sigma_0 = e$, $\sigma_1 = (1, 2)$, $\sigma_2 = (3, 4)$, $\sigma_3 = (1, 2)(3, 4)$.

Определение 1.2. У операции на множестве G выделяют следующие свойства:

– *коммутативность*: $a \circ b = b \circ a$;

– *ассоциативность*: $(a \circ b) \circ c = a \circ (b \circ c)$;

– *существование нейтрального элемента*: $\exists\, e \in G\ \forall\, a \in G$: $a \circ e = e \circ a = a$;

– *существование обратного элемента для* a: $\exists\, b \in G$: $a \circ b = b \circ a = e$, пишут $b = a^{-1}$.

Замечание 1.3. В широком смысле операция на множестве может быть определена не на всех парах, а свойства ассоциативности и коммутативности операции могут относиться не ко всем парам (тройкам) элементов. Например, говорят, что два элемента a и b *коммутируют*, если $a \circ b = b \circ a$, или два элемента a и b *не коммутируют*, если $a \circ b \neq b \circ a$. В этом широком смысле в таблице умножения могут быть заполнены не все клетки. Но при определении *алгебраических структур* (множеств с операциями), например, групп в этом листке, операции должны быть определены для любых упорядоченных пар.

Задача 1.3. а) В каких примерах из задачи 1 для любых элементов имеет место коммутативность? ассоциативность?

б) В каких примерах из задачи 1 существует нейтральный элемент для операций сложения и умножения?

в) Элементы, для которых существует обратный, называются *обратимыми*. Укажите множества обратимых элементов в примерах из задачи 1 для операций сложения и умножения.

г) Сколько обратимых элементов в множестве вычетов по модулю 57 с операцией умножения? Как связано число обратимых элементов в множестве вычетов по модулю n с функцией Эйлера $\phi(n)$?

Задача 1.4. Докажите, что если для некоторой операции существует нейтральный элемент, то он единственный.

Задача 1.5. Докажите, что если ассоциативность выполнена для любых трёх элементов G, то:

а) если существует обратный для $a \in G$, то он единственный;

б) значение произведения $a_1 \circ a_2 \circ \ldots \circ a_k$ не зависит от расстановки скобок;

в) $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ для любых $m, n \in \mathbb{N}$ (определите натуральную степень элемента по индукции).

Определение 1.3. Множество G с заданной операцией $\circ$ называется *группой*, если операция определена на всех упорядоченных парах элементов G, то есть $\circ : G \times G \to G$, при этом она ассоциативна на всех тройках элементов G, существует нейтральный элемент и любой элемент обратим.

Если, кроме того, для любых двух элементов операция коммутативна, группа называется *коммутативной* или *абелевой*.

Замечание 1.4. В понятных случаях вместо $a \circ b$ пишут ab. В большинстве случаев операцию в группе, не имеющую содержательного названия, называют *умножением* и так же обозначают, а её нейтральный элемент называют *единицей* (но пишут e). Иногда (особенно в коммутативных группах) её называют *сложением* и обозначают $+$, а её нейтральный элемент называют *нулём* и пишут 0.

Задача 1.6. а) Какие из привычных числовых множеств с привычными операциями являются группами?

б) Какие из множеств задачи 2 с операциями умножения/сложения являются группами?

в) Какие из групп пунктов а) и б) этой задачи абелевы?

г) Пусть G — множество всех биекций некоторого непустого множества X на себя, $h \circ f$ — это композиция биекций, т.е. $(h \circ f)(x) = h(f(x))$. Докажите, что G — это группа с операцией $\circ$.

д*) Является ли группой множество рациональных чисел без -1 с операцией $a \circ b = a + b + ab$ и множество из 2г?

Определение 1.4. Пусть G — группа, $a \in G$. *Натуральная степень элемента* a определяется как $a^n = a \cdot \ldots \cdot a$, где количество множителей равно натуральному n. *Отрицательные степени* элемента a можно определить по формуле $a^{-n} = (a^n)^{-1}$, где n — натуральное. Считаем, что $a^0 = e$.

Задача 1.7. Докажите, что в любой группе:

а) единица и обратный элемент единственны;

б) $ac = bc \Leftrightarrow a = b \Leftrightarrow ca = cb$ (говорят, что в группах можно *сокращать* и справа, и слева);

в) $(ab)^{-1} = b^{-1}a^{-1}$;

г) $a^{-n} = (a^{-1})^n$;

д) $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ для любых целых m и n.

е) Определим деление в группе так: $a : b = a \cdot b^{-1}$. Докажите, что такое деление совпадает с делением из определения 1.

Задача 1.8. Верно ли, что в таблице умножения группы в каждой строке и в каждом столбце присутствуют все элементы группы? Каково свойство таблицы умножения абелевой группы?

Задача 1.9. а) На множестве из трёх элементов $\{e, a, b\}$ операция задана таблицей:

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	a	e

Есть ли в этом множестве единичный элемент? Является ли это множество с операцией $\circ$ группой?

б) Как изменить таблицу умножения в п. а), чтобы получившаяся операция превратила множество $\{e, a, b\}$ в группу? Верно ли, что это можно сделать единственным способом? Такая таблица умножения называется *групповой*.

в) Как переименовать вычеты 0, 1, 2 по модулю 3 буквами e, a, b так, чтобы таблица сложения вычетов по модулю 3 превратилась в таблицу умножения из п. б)?

Задача 1.10. а) Сколько различных групповых таблиц умножения можно составить на множестве из 2 элементов $\{e, a\}$?

б) Сколько различных групповых таблиц умножения можно составить на множестве из 4 элементов $\{e, a, b, c\}$? Какая из них соответствует группе вычетов по модулю 4 с операцией сложения, а какая — группе из задачи 2 г)?

Определение 1.5. Группа G с операцией $\circ$ *изоморфна* группе H с операцией $*$, если существует такая биекция $f : G \to H$, что для любых $a, b \in G$ $f(a \circ b) = f(a) * f(b)$. Обозначение: $G \cong H$.

Задача 1.11. Докажите, что:

а) группе вычетов по модулю 2 изоморфны группа S_2 и группа из двух чисел $\{-1; 1\}$ с операцией умножения;

б) изоморфизм групп обладает всеми свойствами отношения эквивалентности.

Задача 1.12. а) Докажите, что группы изоморфны тогда и только тогда, когда в них так можно одинаковым образом переименовать элементы, что таблицы умножения операций в этих группах окажутся одинаковыми.

б) Используя утверждение п. а), докажите, что любые две группы из двух элементов изоморфны и любые две группы из трёх элементов изоморфны;

в) Сколько имеется неизоморфных друг другу групп из четырёх элементов? Приведите примеры таких групп из этого листка.

Задача 1.13. Опишите все не изоморфные группы (задайте их таблицы умножения и приведите конкретные примеры)

а) порядка 5; б) порядка 6; в*) порядка 8.

2. Группы. Теорема Лагранжа (листок 26, 8 класс)

Задача 2.1. Пусть G — группа. Докажите, что:

а) если $\forall a \in G\ a^2 = e$, то группа G абелева;

б) если $\forall a, b \in G\ a^2b^2 = (ab)^2$, то группа G абелева.

Определение 2.1. Пусть G — группа с операцией $\circ$. Если $A \subset G$ с той же операцией является группой, то A называется *подгруппой* группы G.

Задача 2.2. Докажите, что пересечение любого набора подгрупп группы является подгруппой.

Задача 2.3. Найдите все подгруппы группы целых чисел.

Определение 2.2. Пусть G— группа, $M = \{g_i \in G : i \in I\}$. Тогда $H = \langle M \rangle$ — обозначается *минимальная подгруппа*, содержащая M. Множество элементов M называется *системой образующих* для $\langle M \rangle$.

Определение 2.3. Пусть G — группа и $\exists g \in G : G = \langle g \rangle$. Тогда G называется *циклической группой, порожденной элементом* g.

Задача 2.4. Пусть $G = S_n$. Докажите, что: $\forall k \leqslant n$ найдется циклическая подгруппа порядка k.

Определение 2.4. Пусть H — подгруппа группы G. Множество элементов вида $\{gh\ : g \in G, k \in H\}$ называется *левым смежным классом* gH (g фиксировано, h пробегает всю подгруппу H). Аналогично определяется *правый смежный класс* Hg.

Задача 2.5. Установите биекцию между правыми и левыми смежными классами из определения 2.4.

Задача 2.6. Пусть H — подгруппа группы G и R — отношение: $g_1Rg_2 \Leftrightarrow \exists g \in G : g_1, g_2 \in gH$. Докажите, что:

а) R — отношение эквивалентности;

б) $g_1Rg_2 \Leftrightarrow g^{-1}g_2 \in H$;

в) все классы смежности равномощны.

г) Определите и докажите соответствующие утверждения для правых смежных классов.

Определение 2.5. Пусть G — группа, $a \in G$. Тогда $|\langle a \rangle|$ называется *порядком* элемента a.

Задача 2.7. Возьмем множество $SL_2(2, \mathbb{Z})$ матриц 2×2 с элементами из $\mathbb{Z}$ и определителем, равным 1.

а) Докажите, что $SL_2(2, \mathbb{Z})$ — группа.

б) В группе $SL_2(2,\mathbb{Z})$ рассмотрим матрицы $A=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ и $B=\begin{pmatrix}0&1\\-1&1\end{pmatrix}$. Найдите порядки матриц A и B.

в) Докажите, что $\langle AB\rangle \cong \mathbb{Z}(+)$.

Вывод: произведение двух элементов конечного порядка не всегда является элементом конечного порядка.

Задача 2.8. а) Определите порядки всех элементов группы S_3 и группы $\mathbb{Z}/6\mathbb{Z}$.

б) Укажите все элементы подгруппы в S_4, порожденной элементами (12) и (23).

Теорема Лангранжа. *Порядок конечной группы делится на порядок её подгруппы.* Докажите.

Следствие. *Порядок любого элемента конечной группы делит порядок группы.*

Определение 2.6. Пусть G — группа, H — ее подгруппа, G/H — разбиение на левые и правые смежные классы. Тогда $|G/H|$ называется *индексом* H в группе G.

Задача 2.9. Пусть $G=S_n$, H — подгруппа, оставляющая на месте число n. Найдите разбиение G/H по левым и правым смежным классам.

Задача 2.10. Пусть $G=S_3$.

а) Постройте таблицу умножения.

б) Найдите все подгруппы.

в) Найдите разбиение по этим подгруппам на левые и правые смежные классы.

г) Выделите подгруппы, где эти разбиения совпадают.

Задача 2.11. Рассмотрим группу $G=SL_2(\mathbb{Z})$, $n\in\mathbb{N}$, и в ней $M=\left\langle\begin{pmatrix}0&1\\-1&0\end{pmatrix}\right\rangle$,

$H=\left\{\begin{pmatrix}1&k\\0&1\end{pmatrix} : n|k\in\mathbb{N}\right\}$.

а) Докажите, что H— подгруппы группы $G=SL_2(\mathbb{Z})$ и что $H\subset M$.

б) Найдите разбиение M/H на левые и правые смежные классы.

Задача 2.12. Пусть $G=U(\mathbb{Z}/n\mathbb{Z})$ — множество обратимых элементов. Докажите, что:

а) G – группа; б) $a^{\varphi(n)}\equiv 1 \pmod n$ (**Теорема Эйлера**).

в*) Найдите все n, при которых $U(\mathbb{Z}/n\mathbb{Z})$ — циклическая группа.

Задача 2.13. а) Найдите все неизоморфные группы четного порядка $\leqslant 7$.

б) Найдите все неизоморфные группы нечетного порядка $\leqslant 7$.

в*) Найдите все неизоморфные группы порядка 8 и 9.

Задача 2.14. Пусть G — группа; $a,b\in G$: $ab=ba$, $(|\langle a\rangle|,\ |\langle b\rangle|)=1$. Докажите, что: $\langle a,b\rangle=\langle ab\rangle$.

Задача 2.15. Пусть G — группа; $a,b\in G$, $ab=ba$, $|\langle a\rangle|=m$, $|\langle b\rangle|=n$. Докажите, что $\exists c$: $|\langle c\rangle|=HOK(m,\ n)$

Задача 2.16. Пусть A_n — множество четных перестановок порядка $n\geqslant 3$. Докажите, что:

а) A_n — группа; б) $A_n=\langle(123),(124),\dots(12n)\rangle$.

Задача 2.17. Найдите в A_4 подгруппу порядка 6.

Задача 2.18. Докажите, что группа четного порядка всегда содержит элемент порядка 2.

Подсказка: разбейте G на пары g и g^{-1}.

3. Свойства операций. Кольца и поля – I (листок 29, 8 класс)

... А у кольца
Начала нет
И нет конца!

Музыка: Ян Френкель,
стихи: Михаил Танич.

Поле, русское поле...

Музыка: Ян Френкель,
стихи: Ирина Гофф.

Задача 3.1. *Формулы сокращённого умножения и уравнение Пелля.* Пусть a, b — целые числа, n — натуральное число, $(a + b\sqrt{2})^n = A_n + B_n\sqrt{2}$. Докажите, что:

0) A_n и B_n – целые;

а) $(a - b\sqrt{2})^n = A_n - B_n\sqrt{2}$;

б) если $a^2 - 2b^2 = 1$, то $A_n^2 - 2B_n^2 = 1$;

в) $H = \{a + b\sqrt{2} : a^2 - 2b^2 = 1\}$ — бесконечная группа с «привычной» операцией умножения.

г) Докажите, что последовательность $\{a_n\}$, где $a_n = (7 - 5\sqrt{2})^{2n+1}$, является бесконечно малой.

д) Решите в целых числах, если возможно, уравнение $(2 + 3\sqrt{47})^m = (3 + 2\sqrt{47})^n$.

Задача 3.2. *Арифметика остатков + комбинаторика.* Для множества вычетов (остатков) по модулю 57 Руслан заполнил таблицы сложения и умножения и в клетках с результатами операций посчитал количество нулей и количество единиц в каждой из таблиц. Какие числа он получил?

Задача 3.3. На множестве $K = \{(a, b) : a \in \mathbb{Z}_2, b \in \mathbb{Z}_3\}$ определите покомпонентные операции сложения и умножения. Пишут $K = \mathbb{Z}_2 \oplus \mathbb{Z}_3$ и говорят, что K является *прямой суммой* $\mathbb{Z}_2$ и $\mathbb{Z}_3$.

а) Укажите нулевой элемент для сложения и единичный для умножения, если такие существуют.

б) В скольких клетках таблиц сложения и умножения $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ стоит нулевой элемент?

в) В скольких клетках таблиц сложения и умножения $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ стоит единичный элемент?

г) Сколько обратимых элементов в таблице умножения $\mathbb{Z}_2 \oplus \mathbb{Z}_3$?

д) Существует ли биекция $\mathbb{Z}_6$ на $\mathbb{Z}_2 \oplus \mathbb{Z}_3$, при которой таблицы сложения и умножения $\mathbb{Z}_6$ и $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ совпадут?

При необходимости уточните понимание условия у преподавателя.

Определение 3.1. Множество K с операциями сложения и умножения называется *кольцом*, если выполняются следующие свойства:

- K — абелева группа по сложению (называется *аддитивной группой* кольца K);
- $a(b + c) = ab + ac$; $(a + b)c = ac + bc$ (дистрибутивность умножения относительно сложения).

Кольцо называется *коммутативным кольцом с единицей*, если операция умножения коммутативна и существует единичный элемент по умножению. Допустимо иметь в кольце всего один элемент.

Определение 3.2. *Полем* называется коммутативное кольцо с единицей, в котором больше одного элемента и каждый ненулевой элемент обратим по умножению.

Задача 3.4. Какие из множеств $\mathbb{Z}$, $\mathbb{Q}$, $n\mathbb{Z}$ (целые числа, кратные $n > 1$), $\mathbb{Z}_n$ (вычеты по модулю $n > 1$), $\mathbb{Z}[x]$ (многочлены с целыми коэффициентами), $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$, $M_2(\mathbb{Q})$ (матрицы 2×2 с коэффициентами из $\mathbb{Q}$) с двумя операциями являются:

а) кольцами, кольцами с единицей, коммутативными кольцами с единицей (укажите «наилучший» вариант);

б) полями.

Задача 3.5. Верно ли, что:

а) в произвольном кольце $a \cdot 0 = 0 \cdot a = 0$; $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$;

б) в произвольном кольце с единицей $a \cdot (-1) = (-1) \cdot a = -a$?

Определение 3.3. Пусть K — кольцо с единицей и $a \in K$. Элемент a называется *обратимым*, если существует $a^{-1} \in K$ такой, что $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Задача 3.6. Пусть K — кольцо с единицей, $U(K)$ — множество всех его обратимых элементов.

а) Докажите, что $U(K)$ — мультипликативная группа.

б) Найдите все обратимые элементы в $M_2(\mathbb{Q})$.

Определение 3.4. Пусть K — кольцо, $a, b \in K$. Если $a \neq 0$ и $b \neq 0$, но $ab = 0$, то a называется *левым делителем нуля*, а b — *правым*. В коммутативном кольце левые и правые делители нуля не различаются.

Определение 3.5. Пусть P — поле и существует такое n, что $n \cdot 1 = 0$. Тогда минимальное натуральное число с этим свойством называют *характеристикой поля*. Если такого n не существует, то говорят, что поле P имеет *нулевую характеристику*. Обозначение: $char\, P$.

Задача 3.7. а) Пусть P — поле. Докажите, что $char\, P = 0$ или $char\, P = p$, где p — простое число.

б) Докажите, что в поле характеристики p $\forall\, a, b \in P$ $(a + b)^p = a^p + b^p$.

в) Найдите корни уравнения $x^2 + x - 1 = 0$ в $\mathbb{Z}_{11}$.

Задача 3.8. Докажите, что в абелевой группе G:

а) все элементы, порядок которых является степенью фиксированного простого числа p, образуют подгруппу G_p;

б) все элементы конечного порядка образуют подгруппу, причем каждый элемент a конечного порядка n однозначно представим в виде суммы $a = a_{p_1} + a_{p_2} + ... + a_{p_k}$, где $p_1, p_2, ..., p_k$ — все простые делители числа n и $a_{p_i} \in G_{p_i}$, $i = 1, 2, ..., k$;

Указание: если несколько целых чисел $b_1, b_2, ..., b_n$ попарно взаимно просты, то существует их линейная комбинация с целыми коэффициентами k_i, $i = 1, 2, ..., n$, равная 1:

$$k_1 b_1 + k_2 b_2 + ... + k_n b_n = 1.$$

в) если существуют элементы порядков m и n, то в G существует также элемент, порядок которого равен $HOK(m, n)$.

Задача 3.9. Докажите, что конечная подгруппа мультипликативной группы произвольного поля всегда циклична.

Подсказка: Воспользуйтесь тем фактом, что многочлен степени k с коэффициентами из данного поля имеет в этом поле не более k корней.

4. Теорема о гомоморфизме. Строение циклических групп (листок 34, 9 класс)

Гомоморфный образ группы,
Будь во имя коммунизма
Изоморфен фактор-группе
По ядру гомоморфизма!

Из фольклора матклассов
1970-1980х годов

Определение 4.1. Пусть G — группа с операцией $*$, G' — группа с операцией $\circ$. Отображение $\varphi : G \to G'$ называется *гомоморфизмом*, если $\varphi(a * b) = \varphi(a) \circ \varphi(b)$ для любых $a, b \in G$.
В дальнейшем значки $*, \circ$ и т.п. мы будем опускать.

Определение 4.2. Пусть $\varphi : G \to G'$ — гомоморфизм. Определим множества:
$Ker\varphi = \{g \in G \,|\, \varphi(g) = e'\}$ (e' — единица группы G') — *ядро* гомоморфизма φ.
$\mathrm{Im}\, \varphi = \{g' \in G' \,|\, \exists\, g \in G : g' = \varphi(g)\}$ — *образ* гомоморфизма φ.

Задача 4.1. Укажите гомоморфизм из группы целых чисел $\mathbb{Z}$ в группы вычетов $\mathbb{Z}/n\mathbb{Z}$. Что является ядром и образом этого гомоморфизма?

Задача 4.2. Докажите, что для любого гомоморфизма $\varphi : G \to G'$:

а) $\varphi(e) = e'$, где e и e' — единицы групп G и G' соответственно;

б) $\forall g \in G$ $\varphi(g^{-1})$ является обратным для $\varphi(g)$ в группе G';

в) $Ker\varphi$ и $\operatorname{Im}\varphi$ являются подгруппами в G и G' соответственно;

г) для любого $h \in Ker\varphi$ и для любого $g \in G$ $ghg^{-1} \in Ker\varphi$;

д) $\forall\, g \in G$ $Hg = gH$, где $H = Ker\varphi$.

Задача 4.3. Пусть G — конечная группа. Тогда для любого гомоморфизма $\varphi : G \to G'$ $|G| = |\ker\varphi| \cdot |\operatorname{Im}\varphi|$.

Определение 4.3. Пусть H — подгруппа группы G. Если для любого $h \in H$ и для любого $g \in G$ $ghg^{-1} \in H$, то подгруппа H называется *нормальной*. Обозначение: $H \triangleleft G$.

Таким образом, для любого гомоморфизма φ пдгруппа $Ker\varphi$ является нормальной подгруппой.

Задача 4.4. Докажите, что:

а) в любой группе нормальны единичная подгруппа и сама группа;

б) подгруппа индекса 2 всегда нормальна:

в) в коммутативной группе все подгруппы нормальны.

Определение 4.4. Пусть G — группа, $H \triangleleft G$. На множестве смежных классов введём операцию *произведения классов*: $g_1H \circ g_2H = g_1g_2H$.

Задача 4.5. Докажите, что:

а) произведение смежных классов определено корректно (т.е. не зависит от выбора представителя смежных классов);

б) множество смежных классов G/H с указанной в определении операцией является группой.

Определение 4.5. Группа G/H называется *фактор-группой* группы G по подгруппе H.

Задача 4.6. Пусть $H \triangleleft G$. Докажите, что тогда существует группа G' и гомоморфизм $\varphi : G \to G'$ такие, что $Ker\varphi = H$.

(*Указание*: в качестве G' рассмотрите G/H.)

Задача 4.7. Докажите, что если $\varphi : G \to G'$ — гомоморфизм, то $\operatorname{Im}\varphi \cong G/Ker\varphi$.

В итоге мы доказали следующую теорему:

Теорема о гомоморфизме групп. *Гомоморфный образ группы изоморфен фактор-группе по ядру гомоморфизма.*

Задача 4.8. Докажите, что $A_n \triangleleft S_n$ и $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$, где A_n — *знакопеременная* группа чётных перестановок порядка n.

Задача 4.9. Докажите, что:

а) $V_4 = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \subset S_4$ — нормальная подгруппа в S_4;

б) $S_4/V_4 \cong S_3$.

Задача 4.10. Пусть G — циклическая группа. Докажите, что:

а) всякая подгруппа G — циклическая;

б) гомоморфный образ G цикличен;

в) если G бесконечна, то $G \cong \mathbb{Z}$;

г) если G конечна, то $G \cong \mathbb{Z}/n\mathbb{Z}$ для некоторого $n \in \mathbb{N}$.

д) если $|G| = n$, $k|n$, то существует и причём единственная подгруппа порядка k.

Задача 4.11. Докажите, что группа простого порядка всегда циклическая.

Задача 4.12. Сколько различных образующих может иметь циклическая группа?

Задача 4.13. а) Докажите, что циклы $(1\,2\,3), (1\,2\,4), \ldots, (1\,2\,n)$ порождают A_n.

б**) Докажите, что в A_5 нет собственных нормальных подгрупп, отличных от e и A_5.

5. Действия групп (листок 36, 9 класс)

То, что аксиоматизаторы называют «абстрактными группами»
— это просто группы преобразований различных множеств,
рассматриваемые с точностью до изоморфизма
(взаимно-однозначного отображения, сохраняющего операции).
Никаких «более абстрактных» групп
в природе не существует, как это доказал Кэли.

В.И. Арнольд. О преподавании математики

Определение 5.1. Пусть X — множество. Обозначим через $\mathrm{Aut}\, X$ группу всех взаимно однозначных отображений из X в себя. Любая подгруппа G группы $\mathrm{Aut}\, X$ называется *группой преобразований* множества X.

Знакомыми вам группами преобразованиями являются: группа S_n и её подгруппы, группы движений плоскости, группы симметрий многоугольника.

Задача 5.1. Сколько элементов в группе движений ромба, не являющегося квадратом, и в группе поворотов квадрата? Изоморфны ли эти группы?

Определение 5.2. Пусть G — группа преобразований множества X (не обязательно всех). Будем говорить, что точки $x, y \in X$ *эквивалентны* относительно G, и писать $x \underset{G}{\sim} y$, если существует такое преобразование $g \in G$, что $gx = y$.

Задача 5.2. Докажите, что отношение $x \underset{G}{\sim} y$ является отношением эквивалентности.

Определение 5.2. Класс эквивалентности точки $x \in X$ называется её *орбитой* и обозначается Gx. Иначе, $Gx = \{gx : g \in G\}$.

Задача 5.3. Опишите орбиты элементов множества X относительно действия группы G, если:
а) X — плоскость, O — фиксированная точка, G — группа поворотов вокруг точки O;
б) $X = \{1, 2, \ldots, n\}$, $G = S_n$;
в) X — прямоугольник, не являющийся квадратом, G — его группа симметрий.

Определение 5.3. Подмножество элементов группы G, оставляющих точку x на месте, называется *стабилизатором* точки x и обозначается $St(x)$. Иначе, $St(x) = \{g \in G : gx = x\}$.

Понятие орбиты и стабилизатора может относиться не только к точке, но и к любому подмножеству множества X.

Задача 5.4. Докажите, что $St(x)$ — подгруппа в G.

Задача 5.5. Найдите стабилизаторы всех точек из задачи 2.

Теорема 5.1. *Имеется взаимно однозначное соответствие между орбитой Gx и множеством смежных классов $G/St(x)$, при котором точке $y = gx \in Gx$ соответствует смежный класс $gSt(x)$.*

Следствие 5.1. *Если G — конечная группа, то $|G| = |Gx||St(x)|$.*

Задача 5.6. Докажите теорему и следствие из неё.

Задача 5.7. Докажите, что $St(gx) = gSt(x)g^{-1}$ и что $|St(x)| = |St(y)|$, если x и y из одной орбиты.

Задача 5.8. Пусть G — группа преобразований конечного множества X. Тогда $X = X_1 \cup X_2 \cup \ldots \cup X_r$ — разбиение на орбиты с представителями $x_1, x_2, \ldots, x_r$. Докажите, что $|X| = \sum_{i=1}^{r} |G/St(x_r)|$.

Определение 5.4. Гомоморфизм $G \xrightarrow{\varphi} \mathrm{Aut}\, X$ называется *действием* группы G на множестве X или *представлением* группы G автоморфизмами множества X. Если понятно, о каком действии

идёт речь, то результат применения отображения $\varphi(g) : X \to X$ к точке $x \in X$ обозначается просто через gx.

Поскольку образ $\varphi(G) \subset \operatorname{Aut} X$ является группой преобразований, множество X распадается в дизъюнктное объединение орбит $Gx = \{gx | g \in G\}$. Порядки стабилизаторов всех точек одной орбиты одинаковы.

Для любой группы G можно определить три её важных действия на самой себе:

1) *Левое* действие L_g: $L_g(x) = gx$.

2) *Правое* действие R_g: $R_g(x) = xg$.

3) *Присоединённое* действие T_g: $T_g(x) = gxg^{-1}$.

Определение 5.5. Действие называется *транзитивным*, если любую точку множества X можно перевести в любую другую точек каким-нибудь преобразованием из группы G.

Задача 5.9. Докажите, что для любого элемента $g \in G$ отображения L_g, R_g и T_g являются биекциями группы G на себя.

Задача 5.10. Теорема Кэли. Докажите, что *любая группа порядка n изоморфна некоторой подгруппе группы S_n.*

Задача 5.11. Пусть H — подгруппа группы G.

а) Опишите орбиты подгруппы H относительно левых и правых сдвигов.

б) Что является стабилизатором подгруппы H при этих действиях?

Задача 5.12. Конечная группа транзитивно действует на множестве, содержащем более одного элемента. Верно ли, что всегда найдётся элемент группы, действующий без неподвижных точек?

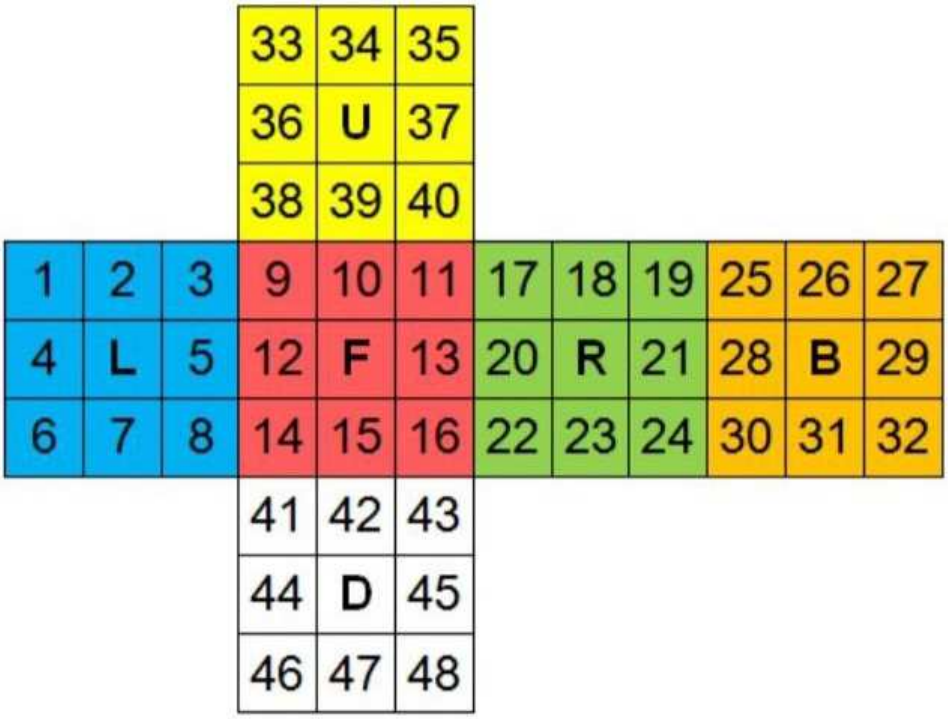
Задача 5.13*. Формула Бернсайда. Пусть конечная группа G действует на конечном множестве X. Для каждого $g \in G$ обозначим через $X^g = \{x \in X \mid gx = x\} = \{x \in X \mid g \in St(x)\}$ множество неподвижных точек преобразования g. Докажите, что тогда $|X/G| = |G|^{-1} \sum\limits_{g \in G} |X^g|$.

Задача 5.14. Пользуясь формулой Бернсайда, найдите число существенно различных раскрасок граней куба в 3 цвета. (Две раскраски считаются *существенно различными*, если они не могут быть совмещены путём вращения куба.)

Задача 5.15. Предположим, что у нас имеются одинаковые по форме бусины n различных цветов (количество бусин каждого цвета неограничено). Сколько различных ожерелий одинаковой формы можно сделать из 6 бусин?

Кубик Рубика и его группа

Рассмотрим развертку кубика Рубика:



Теперь поворотам соответствующих граней на 90° по часовой стрелке можно сопоставить элементы симметрической группы S_{48}:

$L = (1,3,8,6)(2,5,7,4)(33,9,41,32)(36,12,44,29)(38,14,46,27)$
$F = (9,11,16,14)(10,13,15,12)(38,17,43,8)(39,20,42,5)(40,22,41,3)$
$R = (17,19,24,22)(18,21,23,20)(48,16,40,25)(45,13,37,28)(43,11,35,30)$
$B = (25,27,32,30)(26,29,31,28)(19,33,6,48)(21,34,4,47)(24,35,1,46)$
$U = (33,35,40,38)(34,37,39,36)(25,17,9,1)(26,18,10,2)(27,19,11,3)$
$D = (41,43,48,46)(42,45,47,44)(6,14,22,30)(7,15,23,31)(8,16,24,32)$

Тогда группа кубика Рубика G определяется как подгруппа S_{48}, порождаемая поворотами шести граней на 90°:

$G = \langle L, F, R, B, U, D \rangle$
$|G| = \dfrac{8! \cdot 12! \cdot 3^8 \cdot 2^{12}}{3 \cdot 2 \cdot 2} = 43\,252\,003\,274\,489\,856\,000 = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11$

Задача 5.16. Найдите, если возможно, действие на кубике Рубика следующих групп:
а) $\mathbb{Z}/2\mathbb{Z}$ и $\mathbb{Z}/13\mathbb{Z}$; б) S_3; в*) $\mathbb{Z}/68\mathbb{Z}$.

Задача 5.17. Сколько элементов в стабилизаторе клетки 34? клетки 35?

6. Кольца. Идеалы. Поле действительных чисел. Поле частных (листок 38, 9 класс)

Бог создал целые числа, всё остальное — дело рук человека.
Леопольд Кронекер

Пусть $\mathcal{R}$ — множество всех фундаментальных последовательностей рациональных чисел, а $\mathcal{R}_0$ — множество всех бесконечно малых последовательностей в $\mathcal{R}$.

Задача 6.1. Покажите, что $\mathcal{R}$ — ассоциативное коммутативное кольцо с 1. Что есть 0, 1 и противоположный элемент в $\mathcal{R}$? Есть ли в $\mathcal{R}$ делители 0?

Замечание 6.1. $\mathcal{R}_0$ — подгруппа по сложению в $\mathcal{R}$, причём $\forall\,\alpha \in \mathcal{R}_0$ и $\forall\,\beta \in \mathcal{R}$ $\alpha \cdot \beta \in \mathcal{R}_0$. *Эквивалентность* двух последовательностей $\alpha, \beta \in \mathcal{R}$ означает, что $\alpha - \beta \in \mathcal{R}_0$.

В этом листке, если не сказано иное, все кольца считаются ассоциативными и коммутативными.

Определение 6.1. Пусть I — подгруппа по сложению коммутативного кольца K, т.ч. $\forall\, h \in I$ и $\forall\, x \in K$ $xh \in I$. Тогда I называется *идеалом* кольца K. В любом ненулевом кольце K есть, по крайней мере, два идеала: $\{0\}$ и K, которые называются *тривиальными*. Пусть I — идеал кольца $\mathcal{R}$. Элементы $a, b \in \mathcal{R}$ называются *сравнимыми по идеалу* I, если $a - b \in I$. Пишут: $a \equiv b \,(\mathrm{mod}\ I)$.

Задача 6.2. Найдите все идеалы I в кольце целых чисел. Что означает сравнимость по mod I?

Задача 6.3. Докажите, что:

а) если K — поле, то в нём нет нетривиальных идеалов;

обратно: если K ненулевое кольцо с 1, в котором нет нетривиальных идеалов, то это кольцо — поле;

б) если I — идеал в коммутативном кольце K, то $x \equiv y (\mathrm{mod}\ I)$ — отношение эквивалентности;

в) на классах эквивалентности по mod I можно ввести две операции: $[x] + [y] = [x + y]$ и $[x] \cdot [y] = [x \cdot y]$, которые корректно определены, т.е. если $[x'] = [x]$, а $[y'] = [y]$, то $[x'] + [y'] = [x] + [y]$ и $[x'] \cdot [y'] = [x] \cdot [y]$, и превращают множество классов эквивалентности K/I в коммутативное кольцо; причём, если в K есть 1, то и в K/I есть 1;

г) $\mathcal{R}/\mathcal{R}_0$ — поле.

Множество $\mathcal{R}/\mathcal{R}_0$ классов эквивалентности фундаментальных последовательностей является моделью **поля действительных чисел**. В нём ещё нужно ввести отношение порядка (т.е. научиться сравнивать действительные числа) и доказать, что любое ограниченное множество имеет ТВГ. Тогда мы получим модель тех действительных чисел, о которых у вас имеется (?) интуитивное представление.

А пока вернемся к алгебре, точнее, к теории колец и идеалов в них. Идеалы в теории колец играют ту же роль, что и нормальные подгруппы в теории групп. И точно так же мы можем построить естественный гомоморфизм в кольцо классов вычетов по модулю I (см. задачу 6.11).

Определение 6.2. *Идеал в K, порождённый множеством элементов A* — это множество всех элементов $x \in K$, т.ч. $x = u_1 a_1 + \ldots + u_t a_t$, где $u_1, \ldots, u_t \in K$, $a_1, \ldots, a_t \in A$. Обозначение $<A>$.

Если идеал порождён одним элементом $a \in K$, то он называется *главным*. Ясно, что $<a> = a \cdot K$.

Определение 6.3. Кольцо, в котором все идеалы — главные, называется *кольцом главных идеалов*.

Задача 6.4. Проверьте, что

а) множество $<A>$ из определения 2 действительно является идеалом в кольце K;

б) кольцо целых чисел $\mathbb{Z}$ и кольцо многочленов $P[x]$, где P — поле, являются кольцами главных идеалов.

Выясним, при каких условиях на I *фактор-кольцо* K/I — поле, а при каких K/I — кольцо без делителей 0.

Определение 6.4. Идеал I кольца K называется *максимальным*, если для любого идеала H из $I \subset H$ следует $H = I$ или $H = K$.

Определение 6.5. Идеал I в кольце K называется *простым*, если $\forall a, b \in K$ из $ab \in I$ и $a \notin I$ следует $b \in I$.

Замечание 6.2. Это определение очень похоже на свойство простых чисел. Какое?

Задача 6.5. Докажите, что:

а) если K — коммутативное ассоциативное кольцо с 1, то K/I — поле титтк I — максимальный идеал;

б) если K — коммутативное ассоциативное кольцо, то K/I — кольцо без делителей 0 титтк I — простой идеал;

в) любой максимальный идеал является простым.

Задача 6.6. Пусть p — простое и $\mathbb{Q}_{[p]} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$. Докажите, что $p \cdot \mathbb{Q}_{[p]}$ — единственный максимальный идеал в $\mathbb{Q}_{[p]}$.

Задача 6.7. Найдите все максимальные и простые идеалы в $\mathbb{Z}$ и в $P[x]$, где P — поле.

Задача 6.8. Докажите, что в кольце многочленов $\mathbb{Z}[x]$ идеал $x \cdot \mathbb{Z}[x]$ является простым, но не максимальным.

Задача 6.9. Пусть K — коммутативное ассоциативное кольцо с единицей и без делителей нуля. Определим отношение эквивалентности на множестве выражений $\{\frac{a}{b}, b \neq 0\}$: $\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad = bc$. Пусть $\mathbb{Q}(K)$ — множество классов эквивалентности по этому отношению. Определим операции сложения и умножения в $\mathbb{Q}(K)$: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ (нетрудно проверить, что операции определены корректно, т.е. не зависят от выбора представителя в классе эквивалентности). Докажите, что:

а) $\mathbb{Q}(K)$ с введёнными операциями сложения и умножения — коммутативное ассоциативое кольцо с единицей;

б) $\mathbb{Q}(K)_0 = \{\frac{0}{b}, \text{ где } b \neq 0\}$ — максимальный идеал в кольце $\mathbb{Q}(K)$.

Замечание 6.3. $\mathbb{Q}(K)/\mathbb{Q}(K)_0$ — поле по задаче 6.4а. Это поле называется *полем частных* кольца K.

Задача 6.10. Пусть K — коммутативное ассоциативное кольцо с единицей и без делителей нуля, Q_K — его поле частных.

а) Покажите, что $\varphi : K \to Q_K$, т.ч. $\varphi(a) = [\frac{a}{1}]$ является инъективным, $\varphi(a + b) = \varphi(a) + \varphi(b)$ и $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. Таким образом, φ — инъективный гомоморфизм — «естественное вложение» K в поле Q_K.

б*) Пусть кольцо K содержится в поле P. Докажите, что тогда существует вложение $\psi : Q_K \to P$ (инъективный гомоморфизм), т.ч. $K \subset \psi(Q_K) \subset P$, причём если $K \subset P' \subset P$, где P' — поле, то $\psi(Q_K) \subset P'$.

в) Постройте поле частных кольца $K[x]$.

Задача 6.11. Пусть $\varphi : K \to K'$ — сюръективный гомоморфизм колец. Тогда $I = \{a \in K : \varphi(a) = 0\}$ — идеал в кольце K и $K' \cong K/I$. Т.е. гомоморфный образ кольца изоморфен факторкольцу по ядру гомоморфизма.

7. Евклидовость и факториальность (листок 40, 9 класс)

Три дня в деканате студент пролежал,
Одетый в евклидовы кольца,
А горем убитый декан прочитал,
Рыдая над ним, Фихтенгольца.

Из фольклора студентов
математических факультетов

Определение 7.1. Коммутативное ассоциативное кольцо с единицей без делителей нуля называется *областью целостности*.

Определение 7.2. Пусть R — область целостности, $N : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ — функция со следующими свойствами:

1) $\forall\, a, b \in R, a \neq 0, b \neq 0\ N(ab) \geqslant N(a)$;

2) $\forall\, a, b \in R, a \neq 0$ существует представление, не обязательно единственное, вида $b = aq + r$, где $r = 0$ или $N(r) < N(a)$.

Тогда R называется ***евклидовым кольцом***, а N — *евклидовой нормой*.

Задача 7.1. а) Покажите, что функция $N(a) = |a|$ является евклидовой нормой в кольце $\mathbb{Z}$, по отношению к которой кольцо $\mathbb{Z}$ евклидово.

б) Деление с остатком определено в кольце многочленов над полем (например, в $\mathbb{R}[x]$). По отношению к какой евклидовой норме в $\mathbb{R}[x]$ определено это деление с остатком?

в*) Покажите, что евклидовым является кольцо конечных десятичных дробей.

Задача 7.2. Докажите, что любое евклидово кольцо является кольцом главных идеалов.

Далее везде подразумевается, что R — область целостности.

Определение 7.3. Пусть $c \in R$ — обратим (т.е. $\exists\, d \in R\ cd = 1$). Тогда если $a = bc$, то элементы a и b называют *ассоциированными*.

Задача 7.3. Пусть R — евклидово кольцо. Докажите, что если $a = bc$ и a и b неассоциированы, то $N(b) < N(a)$.

Определение 7.4. Будем говорить, что элемент $d \in R$ *делит* $a \in R$, и писать $d|a$, если $\exists\, b \in R$ такой, что $a = db$.

Задача 7.4. Докажите, что если a и b — элементы области целостности R, то равносильны следующие утверждения:

1) $aR = bR$; 2) a и b ассоциированы; 3) a и b делят одни и те же элементы.

Определение 7.5. Для любых $a, b \in R$ *наибольшим общим делителем* (обозначается НОД(a, b), иногда (a, b)) называется $d \in R$, удовлетворяющий условиям: 1) $d|a$, $d|b$; 2) $c|a$, $c|b \Rightarrow c|d$.

Задача 7.5. Докажите, что в евклидовом кольце R для любых элементов a и b существует НОД(a, b). Укажите алгоритм построения и докажите, что $\exists\, u, v \in R$: $ua + vb =$ НОД(a, b).

Определение 7.6. Кольцом *целых гауссовых чисел* $\mathbb{Z}[i]$ называется подмножество комплексных чисел вида $a + bi$, $a, b \in \mathbb{Z}$, с естественными операциями сложения и умножения.

Задача 7.6. а) Докажите, что $\mathbb{Z}[i]$ — область целостности.

б) Найдите множество обратимых элементов в $\mathbb{Z}[i]$.

в) Докажите, что кольцо $\mathbb{Z}[i]$ евклидово с нормой $N(z) = z \cdot \overline{z}$.

г) Постройте поле частных кольца $\mathbb{Z}[i]$.

Задача 7.7. Покажите, что в $\mathbb{Z}$ $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$, где $d =$ НОД(n, m), и $n\mathbb{Z} \cap m\mathbb{Z} = k\mathbb{Z}$, где $k =$ НОК(n, m).

Задача 7.8. Рассмотрим множество $D_3 = \{a + b\xi\}, a, b \in \mathbb{Z}$, где $\xi = \frac{-1+i\sqrt{3}}{2}$.

а) Найдите все обратимые элементы в D_3.

б) Докажите, что D_3 является евклидовым кольцом с нормой, равной квадрату модуля.

Определение 7.7. Пусть $p \in R, p \neq 0$, причём p необратим. Если из равенства $p = ab$ следует, что a или b обратим, то элемент p называется *простым* (или *неразложимым*).

Простые элементы кольца многочленов $P[x]$ над полем P называются *неприводимыми* многочленами.

Задача 7.9. а) Разложите 2, 3, 5 на простые множители в кольце гауссовых чисел.

б*) Найдите все простые элементы в кольце гауссовых чисел.

Задача 7.10. Докажите, что $R[X]$ — кольцо главных идеалов тогда и только тогда, когда R — поле.

Задача 7.10. Пусть R — кольцо главных идеалов. Докажите, что тогда:

а) равносильны свойства: 1) $p \in R$ простой; 2) pR — максимальный идеал; 3) если $p|ab$, то $p|a$ или $p|b$;

б) нет бесконечно возрастающей цепочки различных идеалов $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$;

в) любой ненулевой элемент раскладывается на простые, причём однозначно с точностью до ассоциированных элементов;

г) у любых двух ненулевых элементов есть НОД и НОК и $\forall a, b, c \in R$ если $c|ab$ и $(a, c) = 1$, то $c|b$ (*Указание.* Воспользуйтесь пунктом в).

Определение 7.7. Область целостности R называется *факториальным кольцом*, если любой ненулевой элемент $a \in R$ можно представить в виде $a = up_1 \dots p_r$, где u — обратимый, $p_1, \dots, p_r$ — простые, причём любые два таких разложения совпадают с точностью до ассоциированных элементов.

Замечание 7.1. Из задач 7.11в и 7.2 следует, что факториальным является всякое кольцо главных идеалов, а значит, и всякое евклидовое кольцо.

Задача 7.11. Факториально ли кольцо: а) $\mathbb{Z}_8[X]$; б) $\mathbb{Z}[\sqrt{-5}]$; в) $\mathbb{Z}[\sqrt{-3}]$?

Указание к п. б): представьте 6 двумя разными способами и докажите неассоциированность этих представлений.

Задача 7.12. Приведите пример факториального кольца, которое не является кольцом главных идеалов.

Указание. Воспользуйтесь тем, что кольцо многочленов над факториальным кольцом факториально.

Замечание 7.2. Существуют кольца, в которых выполнена основная теорема арифметики, но которые не допускают алгоритма деления с остатком (ни по отношению ни к какой норме). Таким кольцом является, например, кольцо всех чисел вида $\frac{a+b\sqrt{-19}}{2}$, где a и b — целые числа одинаковой чётности.

Задача 7.13*.** Докажите утверждение из замечания выше.

7,25. Коммутант. Разрешимые группы. Простота знакопеременной группы (март 2024 г.)

Определение 7,25.1. Пусть G — группа, x, $y \in G$. *Коммутатором элементов* x и y называется $[x,\ y] = xyx^{-1}y^{-1}$.

Задача 7,25.1. Докажите, что: а) $[x,\ y] = e \Leftrightarrow xy = yx$; б) $[x,\ y]^{-1} = [y,\ x]$;

Определение 7,25.2. Пусть G — группа. Тогда подгруппа, порожденная всеми коммутаторами из G, называется *коммутантом* и обозначается G'.

Задача 7,25.2. Докажите, что $G' \triangleleft G$.

Задача 7,25.3. Пусть $\varphi : G \to H$ — эпиморфизм. Докажите, что тогда $\varphi(G') = H'$.

Задача 7,25.4. Пусть G — группа, $H \triangleleft G$. Докажите, что если G/H абелева, то $G' \subset H$. Иными словами, коммутант является наименьшей нормальной подгруппой, факторгруппа по которой абелева.

Задача 7,25.5. Пусть $H \subset G$ — подгруппа группы G, такая, что $G' \subset H$. Докажите, что тогда $H \triangleleft G$ и G/H — абелева группа.

Задача 7,25.6. Докажите, что знакопеременная группа A_n порождается тройными циклами, а при $n \geq 5$ — произведениями пар независимых транспозиций.

Задача 7,25.7. Докажите, что $S_n' = A_n$.

Задача 7,25.8. Докажите, что $A_4' = V_4$ ($V_4 = \{e,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\} \subset S_4$ — нормальная подгруппа в S_4, так называемая группа Клейна, также ее можно определить как $V_4 = \{(a,\ b) : a,\ b \in \mathbb{Z}/2\mathbb{Z}\}$ с покомпонентной операцией сложения).

Задача 7,25.9. Докажите, что $S_n' = A_n$ при $n \geq 5$.

Определение 7,25.3. Пусть G — группа, $G^{(1)} = G'$, $G^{(2)} = G^{(1)'}$, $\dots$, $G^{k+1} = G^{k'}$. Тогда G^k называется *k-кратным коммутантом*.

Определение 7,25.4. Группа G называется *разрешимой*, если для некоторого $m \in \mathbb{N}$ $G^{(m)} = \{e\}$.

Задача 7,25.10. Докажите, что если G — разрешимая группа, $H \subset G$ — подгруппа, то H — разрешимая.

Задача 7,25.11. Докажите, что если G — разрешимая группа, $H \lhd G$, то G/H — разрешимая.

Задача 7,25.12. Пусть G — группа, $H \lhd G$. Если H и G/H — разрешимые, то группа G — разрешимая.

Задача 7,25.13. Докажите, что для любого $k \in \mathbb{N}$ $G^{(k)} \lhd G$.

Задача 7,25.14. Докажите, что если $H \lhd G$, то $H' \lhd G$.

Задача 7,25.15. Найдите G', G/G' и докажите разрешимость группы G, если G — это: а) группа кватернионов; б) группа диэдра.

Задача 7,25.16. Докажите, что любая конечная p-группа разрешима.

7,5. Лемма Гаусса. Круговые многочлены, (алгебра, март 2024 г.)

Задача 7,5.1. Пусть $f = a_0x^n + a_1x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$ имеет рациональный корень $\frac{u}{v}$, $(u,\ v) = 1$. Докажите, что $u|a_n$, $v|a_0$.

Следствие. *Если $f \in \mathbb{Z}[x]$ — приведенный ($a_0 = 1$), то все рациональные корни f — целые.*

Лемма Гаусса. *Пусть $f \in \mathbb{Z}[x]$ такой, что $f = gh$, где g, $h \in \mathbb{Q}[x]$. Тогда существует $\lambda \in \mathbb{Q}[x]$, такой, что λg, $\lambda^{-1}h \in \mathbb{Z}[x]$. Иными словами: если многочлен с целыми коэффициентами разлагается в произведение двух многочленов с рациональными коэффициентами, то он разлагается в произведение двух пропорциональных им многочленов с целыми коэффициентами.*

Задача 7,5.2. Докажите лемму Гаусса.

Следствие. Если многочлен из $\mathbb{Z}[x]$ разложим в произведение двух многочленов положительной степени из $\mathbb{Q}[x]$, то он разложим и в $\mathbb{Z}[x]$.

Задача 7,5.3. Пусть $p \in \mathbb{N}$ — простое. Докажите, что многочлен $x^p + x^{p-1} + \ldots + 1$ неприводим над $\mathbb{Q}[x]$.

Задача 7,5.4. Докажите, что кольцо $\mathbb{Z}[x]$ факториально.

Задача 7,5.5. Сформулируйте и докажите лемму Гаусса для кольца многочленов над факториальным кольцом.

Задача 7,5.6. Докажите, что: а) кольцо многочленов над факториальным кольцом факториально; б) кольцо многочленов от n переменных над факториальным кольцом факториально.

Признак (“критерий”) Эйзенштейна. Пусть $p \in \mathbb{N}$ — простое число. Пусть многочлен $f = a_0x^n + a_1x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$ удовлетворяет условиям: a_0 не делится на p, a_i делится на p для всех $i = 1, ..., n$, a_n не делится на p^2. Тогда многочлен f неприводим над $\mathbb{Q}$.

Задача 7,5.6,5. Докажите признак Эйзенштейна.

Рассмотрим корни уравнения $x^n - 1$ в $\mathbb{C}$.

Задача 7,5.7. Докажите, что корни уравнения $x^n - 1$ в $\mathbb{C}$ образуют циклическую группу по умножению, изоморфную группе $\mathbb{Z}/n\mathbb{Z}$ по сложению.

Определение 7,5.1. Образующие в группе корней n-й степени из единицы называются *первообразными корнями* n-й степени из единицы.

Определение 7,5.2. *Круговым многочленом* называется многочлен

$$\Phi_n(x) = \prod_{\xi i}(x - \xi_i),$$

где ξi — первообразные корни из единицы n-й степени.

Очевидно, что $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$.

Задача 7,5.8. Докажите, что $\deg \Phi_n(x) = \varphi(n)$.

Задача 7,5.9. Докажите, что: а) $\Phi_n(x) \in \mathbb{Z}[x]$. б) $\Phi_n(0) = 1$ при $n > 1$.

Задача 7,5.10. Докажите формулу $x^n - 1 = \prod\limits_{d|n} \Phi_d(x)$.

Задача 7,5.11. Пусть p — простое. Докажите, что $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + 1$.

Задача 7,5.12. Докажите, что при любом $d|n$ имеет место равенство $x^n - 1 = (x^d - 1)\Phi_n(x)h_d(x)$, где $h_d(x) \in \mathbb{Z}[x]$.

Задача 7,5.13. Найдите $\Phi_n(x)$ для $n \leq 12$.

Задача 7,5.14. Докажите, что круговой многочлен неприводим над $\mathbb{Q}$.

8. Конечные абелевы группы (листок 42, 9 класс)

Он известный специалист
по конечным абелевым группам.

Шутка про одного из
наших учителей.

В этом листке все группы абелевы. Групповую операцию в абелевых группах принято обозначать знаком $+$, а нейтральный элемент — нулём 0.

Определение 8.1. *Внешней прямой суммой* абелевых групп $A_1, A_2, \ldots, A_k$ называется множество $A_1 \times A_2 \times \ldots \times A_k$ с покомпонентной операцией сложения. Обозначение: $A_1 \oplus A_2 \oplus \ldots \oplus A_k$.

Задача 8.1. Дана группа $\mathbb{Z}_4 \oplus \mathbb{Z}_6$.

а) Найдите в этой группе все элементы порядка 3 и все элементы порядка 6.

б) Есть ли в этой группе элемент порядка 24?

Задача 8.2. Изоморфны ли группы $\mathbb{Z}_{12} \oplus \mathbb{Z}_{72}$ и $\mathbb{Z}_{18} \oplus \mathbb{Z}_{48}$?

Задача 8.3. Будет ли циклической группа $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{179}$? Изменится ли ответ, если в этой прямой сумме $\mathbb{Z}_{179}$ заменить на $\mathbb{Z}_{57}$?

Задача 8.4. Пусть A_1 и A_2 — подгруппы абелевой группы A такие, что $A_1 \cap A_2 = \{0\}$ и $\forall\, a \in A$ $\exists\, a_1 \in A_1, a_2 \in A_2$ $a = a_1 + a_2$. Докажите, что $A \cong A_1 \oplus A_2$.

Определение 8.2. Говорят, что абелева группа A *разлагается в прямую сумму* подгрупп $A_1, A_2, \ldots, A_k$, если для любого $a \in A$ существует и притом единственное представление $a = a_1 + a_2 + \ldots + a_k$, где $a_i \in A_i$. Иначе это называют *внутренней прямой суммой*. Обозначение такое же, как и для внешней прямой суммы: $A = A_1 \oplus A_2 \oplus \ldots \oplus A_k$.

Задача 8.5. Дана группа $\mathbb{Z}_{12}$. Пусть A_1 — множество всех элементов порядка 3, включая 0, и A_2 — множество всех элементов порядка 2 или 4, включая 0. Верно ли, что A_1 и A_2 — подгруппы $\mathbb{Z}_{12}$ и $\mathbb{Z}_{12} = A_1 \oplus A_2$?

Задача 8.6. Установите изоморфную связь между внутренней и внешней прямыми суммами.

Замечание 8.1. Поскольку обозначение для внешней и внутренней прямых сумм совпадают, то о какой конкретно сумме идёт речь, следует из контекста конкретной задачи.

Задача 8.7. Пусть G — конечная абелева группа, $|G| = n$, $n = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$, p_i — различные простые числа. Тогда $G = G_{p_1} \oplus G_{p_2} \oplus \ldots \oplus G_{p_k}$, где G_{p_i} — подгруппа группы G, состоящая из элементов, имеющих порядок, равный степени простого числа p_i. (См. также задачу 3.8).

Определение 8.3. Конечная абелева группа, порядок которой есть степень простого числа p, называется *примарной* или *p-группой*.

Задача 8.8. Пусть A — примарная группа, $a \in A$ — элемент максимального порядка. Тогда существует подгруппа $B \subset A$ такая, что $A = <a> \oplus B$.

Теорема Фробениуса-Штикельбергера. *Каждая конечная абелева группа однозначно (с точностью до порядка слагаемых) разлагается в прямую сумму конечного числа примарных циклических групп.*

Задача 8.9. Докажите теорему Фробениуса-Штикельбергера.

Задача 8.10. Найдите все неизоморфные абелевы группы: а) порядка 16; б) порядка 36.

Задача 8.11. а) В группе $\mathbb{Z}_2 \oplus \mathbb{Z}_{57} \oplus \mathbb{Z}_{179}$ найдите подгруппу порядка 537.

б) Докажите, что для конечных абелевых групп верна теорема, обратная **теореме Лагранжа**: если G — конечная абелева группа, $|G| = n$, $d|n$, то существует подгруппа $B \subset G$, $|B| = d$.

Задача 8.12. Докажите, что если G — конечная абелева группа, $|G| = n$ и n не делится на квадраты, то G — циклическая.

Задача 8.13. Докажите, что конечная абелева группа является циклической тогда и только тогда, когда её порядок равен наименьшему общему кратному порядков всех её ненулевых элементов.

Задача 8.14. Конечная подгруппа мультипликативной группы любого поля всегда циклична. (См. также задачу 3.9).

Указание. Воспользуйтесь теоремой Безу, которая верна для любых многочленов над любым полем.

8,5. Простые, но очень важные факты о полях и кольцах многочленов (10 класс, алгебра, июль 2024 г.)

Задача 8,5.1. Докажите, что если в кольце есть единица, то она единственна.

Задача 8,5.2. Докажите, что если конечное кольцо не содержит делителей нуля, то оно содержит единицу и все его ненулевые элементы обратимы.

Напомним, что *гомоморфизмом колец* R_1 *и* R_2 называется отображение $\varphi : R_1 \to R_2$, сохраняющее операции.

Задача 8,5.3. Пусть $\varphi : R_1 \to R_2$ — гомоморфизм колец. а) Докажите, что $\varphi(0_1) = 0_2$. б) Покажите, что если кольцо R_1 с единицей, то необязательно $\varphi(1_1) = 1_2$.

Задача 8,5.4. Докажите, что если $\varphi : R_1 \to R_2$ — эпиморфизм колец, то $\varphi(1_1) = 1_2$.

Для колец с единицей определение гомоморфизма включает дополнительное требование.

Определение 8,5.1. Пусть R_1 и R_2 — кольца с единицей. Отображение $\varphi : R_1 \to R_2$ называется *гомоморфизмом*, если для любых x, $y \in R_1$ выполнены условия:
1) $\varphi(x + y) = \varphi(x) + \varphi(y)$
2) $\varphi(xy) = \varphi(x)\varphi(y)$
3) $\varphi(1_1) = 1_2$.

Определение 8,5.2. Пусть E, L — поля, $E \subset L$, операции, единица, ноль в E и L одни и те же. Тогда E называется *подполем* L, а L — расширением поля E.

Задача 8,5.5. Пусть $\varphi : E \to P$ — гомоморфизм полей. Докажите, что φ инъективен и $E \cong \varphi(E)$.

Определение 8,5.3. Пусть $\varphi : E \to P$ — гомоморфизм полей. Тогда отображение $h^\varphi : E[x] \to P[x]$, сопоставляющее многочлену $f(x) = a_0x^n + \ldots + a_{n-1}x + a_n \in E[x]$ многочлен $f^\varphi(x) = \varphi(a_0)x^n + \ldots + \varphi(a_{n-1})x + \varphi(a_n) \in P[x]$, называется *индуцированным гомоморфизмом.*

Задача 8,5.6. Пусть $\varphi : E \to P$ — гомоморфизм полей, $\widetilde{\varphi} : E[x] \to P[x]$ — индуцированный гомоморфизм. Докажите, что: а) индуцированный гомоморфизм $\widetilde{\varphi} : E[x] \to P[x]$ является гомоморфизмом колец многочленов; б) индуцированный гомоморфизм $\widetilde{\varphi} : E[x] \to P[x]$ инъективен. Если $\varphi : E \to P$ — изоморфизм, то докажите, что: в) если $f(x) \in E[x]$ — неприводим, то $f^\varphi(x) \in P[x]$ тоже неприводим; г) $a \in E$ — корень $f(x) \in E[x] \Leftrightarrow \varphi(a) \in P$ — корень $f^\varphi(x) \in P[x]$; д) $f(x) \in E[x]$ раскладывается на линейные множители $\Leftrightarrow f^\varphi(x) \in P[x]$ раскладывается на линейные множители; е) $f(x) \in E[x]$ имеет кратные корни $\Leftrightarrow f^\varphi(x) \in P[x]$ имеет кратные корни.

Задача 8,5.7. Пусть $R_1 \subset R_2$ — евклидовы кольца, a, $b \in R_1$. Докажите, что $(a, b)_{R_1} = (a, b)_{R_2}$, т.е. НОД не изменяется при расширении евклидовых колец.

Задача 8,5.8. Пусть P — поле, $f \in P[x]$. Докажите, что у f есть кратный корень в каком-нибудь расширении поля P тогда и только тогда, когда $(f, f') \neq 1$.

Задача 8,5.9. Пусть P — поле, $f \in P[x]$ — неприводимый. Докажите, что $(f, f') \neq 1$ тогда и только тогда, когда $\mathrm{char}\ P = p > 0$ и $f(x) = g(x^p)$, где $g \in P[x]$.

Задача 8,5.10. Пусть P — поле, f, $g \in P[x]$, причем $(f, g) = 1$, и пусть для некоторого расширения L поля P эти многочлены раскладываются в произведение линейных множителей в кольце $L[x]$. Докажите, что они не имеют общих корней в этом расширении.

Задача 8,5.11. Пусть P — поле, f, $g \in P[x]$, причем f — неприводимый многочлен. Пусть в расширении $L \supset P$ f и g имеют общий корень. Докажите, что тогда $f|g$.

Определение 8,5.4. Пусть P — поле. *Минимальным подполем поля* P называется пересечение всех подполей поля P.

Задача 8,5.12. Докажите, что минимальное подполе изоморфно: а) Z_p, если $\mathrm{char}\ P = p$; б) $\mathbb{Q}$, если $\mathrm{char}\ P = 0$.

Определение 8,5.5. *Автоморфизмом поля* P называется изоморфизм $P \to P$.

Задача 8,5.13. Докажите, что: а) автоморфизмы поля образуют группу; б) минимальное подполе инвариантно при всех автоморфизмах поля; в) найдите группу автоморфизмов поля $\mathbb{R}$.

Определение 8,5.6. Пусть $P \subset L$ — расширение поля P, $a_1, \ldots, a_s \in L$. Говорят, что *поле* L *порождено элементами* $a_1, \ldots, a_s$, и пишут $L = P(a_1, \ldots, a_s)$, если в L нет меньшего подполя, содержащего P и $a_1, \ldots, a_s$. Поле L называют *конечно порожденным над* P. Если $L = P(a)$, то расширение называют *простым*, а элемент a — *примитивным элементом*.

Задача 8,5.14. Пусть $L = P(a_1, \ldots, a_s)$ — конечно порожденное расширение поля P. Докажите, что:

а) любой элемент $a \in L$ можно представить в виде $a = \frac{f(a_1, \ldots, a_s)}{g(a_1, \ldots, a_s)}$, f, $g \in P[a_1, \ldots, a_s]$;

б) любое конечно порожденное расширение является конечной цепочкой простых расширений: $P(a_1 \ldots, a_s) = (\ldots(P(a_1))(a_2))\ldots)(a_s)$.

Определение 8,5.7. Пусть $P \subset L$ — расширение полей. Элемент $a \in L$ называется *алгебраическим над* P, если существует ненулевой многочлен $f \in P[x]$, такой, что $f(a) = 0$.

Задача 8,5.15.Пусть $P \subset L$ — расширение полей, $a \in L$ — алгебраический. Докажите, что множество $I_a = \{f \in P[x] | f(a) = 0\}$ образует идеал в $P[x]$.

Определение 8,5.8. Многочлен со старшим коэффициентом 1, образующий идеал I_a, называется *минимальным многочленом элемента* a и обозначается μ_a.

Задача 8,5.16. Докажите, что любая конечная p-группа разрешима.

Задача 8,5.17. Пусть $P \subset L$ — расширение полей, $a \in L$. Докажите, что $P(a) \cong P[x]/(\mu_a \cdot P[x])$.

Задача 8,5.18. Постройте таблицы сложения и умножения для поля $P[x]/(\mu_a \cdot P[x])$, где:

а) $P = \mathbb{Z}_2$, $\mu_a = x^2 + x + 1$; б) $P = \mathbb{Z}_2$, $\mu_a = x^3 + x + 1$; в) $P = \mathbb{Z}_3$, $\mu_a = x^2 + 1$;

9. Конечные алгебраические расширения (листок 43, 10 класс)

Полюшко, поле!
Полюшко, широко поле!

Из симфонии «Поэма о бойце-комсомольце», 1934 г.
композитор Лев Книппер, слова Виктор Гусев.

Задача 9.1. Пусть α – корень $f(x) = x^3 - 3x + 1$ (у $f(x)$ 3 различных действительных корня).
а) Найдите $\frac{\alpha}{\alpha+1}$ в $\mathbb{Q}[\alpha]$.

б) Рассмотрим множество P всех многочленов в $\mathbb{Q}[x]$ степени меньше 3. Операция сложения в P — это обычное сложение многочленов. Операция умножения в P — это умножение по модулю $x^3 - 3x + 1$. Докажите, что P — поле (содержащее $\mathbb{Q}$).

Указание. Докажите, что $f(x)$ неприводим, и воспользуйтесь тем, что по алгоритму Евклида для взаимно простых многочленов f и g можно найти такие u, v, что $vg + uf = 1$, $\deg v < \deg g$, $\deg u < \deg f$.

в*) Докажите, что P изоморфно $\mathbb{Q}[\alpha]$.

Определение 9.1. Пусть $F \subset E$ — поля, F — подполе E. Тогда E называется *расширением* поля F.

Определение 9.2. (Совпадает с определением 8,5.6). Пусть $P \subset L$ — расширение поля P, a_1, …, $a_s \in L$. Говорят, что *поле L порождено элементами* a_1, …, a_s, и пишут $L = P(a_1, \ldots, a_s)$, если в L нет меньшего подполя, содержащего P и a_1, …,a_s. Поле L называют *конечно порожденным над* P. Если $L = P(a)$, то расширение называют *простым*, а элемент a — *примитивным элементом*.

Задача 9.2. Пусть дано расширение $F \subset L$, $a_1, \ldots, a_n \in L$. Докажите, что $F(a_1, \ldots, a_n)$ является пересечением всех подполей в L, содержащих F и $a_1, \ldots, a_n$.

Задача 9.3. Пусть $F \subset E$ — расширение поля F. Докажите, что тогда E — линейное пространство над F (и даже алгебра над F для тех, кто знает, что такое алгебра).

Определение 9.3. Если $F \subset E$ — расширение поля F, то символом $[E : F]$ мы обозначаем размерность векторного пространства $\dim_F E$, которая называется *степенью расширения*. Если степень расширения конечна, т.е. $[E : F] < \infty$, то такое расширение называют *конечным*.

Задача 9.4. Найдите степень расширения:
а) $[\mathbb{C} : \mathbb{R}]$; б) $[\mathbb{R} : \mathbb{Q}]$; в) $[P : \mathbb{Q}]$, где поле P — из задачи 1;

Задача 9.5. Докажите, что всякое конечное расширение конечно порождено.

Задача 9.6. Пусть K — поле, $f \in K[x]$, $\deg f = n$. Рассмотрим множество $K_f[x]$ всех многочленов из $K[x]$ степени меньше n с операцией сложения многочленов.

а) Определите на множестве $K_f[x]$ операцию умножения (см. задачу 9.1б) и докажите, что $K_f[x]$ становится коммутативным кольцом с единицей и линейным пространством над K.

б) Докажите, что $K[x]/(f) \cong K_f[x]$

в) Найдите размерность $K[x]/(f)$.

г) Докажите, что $K[x]/(f)$ — поле $\Leftrightarrow$ f неприводим в $K[x]$.

Задача 9.7. Пусть F — поле, $f \in F[x]$ — неприводимый многочлен. Докажите, что существует поле $L \supset F$, в котором f имеет корень, т.е. $\exists\, \alpha \in L : f(\alpha) = 0$.

Задача 9.8. (**Теорема Кронекера** — Следствие 1 из задачи 9.7) Для любого многочлена над полем существует расширение этого поля, в котором этот многочлен имеет корень.

Задача 9.9. (Следствие 2 из задачи 9.7) Для любого многочлена над полем существует расширение этого поля, в котором он раскладывается на линейные множители.

Определение 9.4. Пусть $F \subset E$ — расширение поля F и $a \in E$. Если $\exists\, f(x) \in F[x]$ такой, что $f(a) = 0$ и $f \not\equiv 0$, то элемент a называется *алгебраическим* над F.

Задача 9.10. Пусть $F \subset E$ — расширение поля F и $a \in L$ — алгебраический над F. Докажите, что тогда $\exists!\, f(x) \in F[x]$ – неприводимый и нормализованный (старший коэффициент равен 1), т.ч. $f(a) = 0$.

Определение 9.5. Такой многочлен мы будем называть *минимальным многочленом* элемента a и обозначать $\mu_a(x)$.

Задача 9.11. Найдите минимальный многочлен для:
а) $\sqrt{2}$ над $\mathbb{Q}$; б) $\sqrt[7]{5}$ над $\mathbb{Q}$; в) $\sqrt[105]{9}$ над $\mathbb{Q}$; г) $2 - 3i$ над $\mathbb{R}$; д) $2 - 3i$ над $\mathbb{C}$.

Определение 9.6. Расширение полей $F \subset E$ называется *алгебраическим*, если $\forall\, a \in E$ a — алгебраический над F.

Задача 9.12. Докажите, что всякое конечное расширение является алгебраическим.

Задача 9.13 (Теорема о башне полей). Пусть $K \subset F \subset E$ – конечные расширения вложенных полей. Докажите, что тогда $[F : K] \cdot [E : F] = [E : K]$.

Задача 9.14. Пусть дана последовательность расширений полей $F_1 \subset F_2 \subset F_3 \subset \ldots \subset F_n$. Докажите, что $F_1 \subset F_n$ — конечное расширение титтк расширения $F_i \subset F_{i+1}$, $i = 1, \ldots, n-1$ конечны.

Задача 9.15. Пусть $F \subset E$ — расширение поля F, $a \in E$ — алгебраический над F. Докажите, что тогда $F(a) \cong F[x]/(\mu_a(x))$ и $[F(a) : F] = \deg \mu_a(x)$.

Задача 9.16. Пусть $E = K(a_1, \ldots, a_n)$ — конечно порождённое расширение поля K, т.ч. $\forall\, i$ a_i — алгебраический над k. Докажите, что тогда $K \subset E$ — конечное алгебраическое расширение.

Задача 9.17. Пусть $K \subset F \subset E$ — башня полей, где каждый этаж алгебраический. Докажите, что тогда $K \subset E$ — алгебраическое расширение.

Определение 9.7. Поле F называется *алгебраически замкнутым*, если степень любого неприводимого многочлена из $F[x]$ не больше 1.

Теорема 9.1. (**Теорема Штейница.**) *Пусть F — поле. Тогда существует $F \subset E$ — расширение поля F, т.ч. E алгебраически замкнуто.*

Теорему можно принять и использовать без доказательства.

Определение 9.8. Конечное расширение поля рациональных чисел называется *полем алгебраических чисел.*

Замечание 9.1. Это не то же самое, что *поле всех алгебраических чисел*, которое получается присоединением к $\mathbb{Q}$ всех корней всех многочленов с рациональными коэффициентами.

Задача 9.18. Пусть F — поле. Докажите, что тогда существует поле $\overline{F}$: $\overline{F} \supset F$ алгебраично и $\overline{F}$ — алгебраически замкнуто.

Задача 9.19. Докажите, что $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Указание. Воспользуйтесь тем, что многочлен $(x^p - 2)$ по критерию Эйзенштейна неприводим для любого p.

10. Поле разложения многочлена. Нормальные расширения полей. Конечные поля (листок 45, 10 класс)

О поле, поле, кто тебя ... ?

А.С. Пушкин, «Руслан и людмила».

Задача 10.1. Пусть $\varphi : P \to F$ — гомоморфизм полей, α — корень $h \in P[x]$ — неприводимого многочлена, и $P(\alpha)$ — простое расширение P. Докажите, что тогда гомоморфизм φ продолжается до гомоморфизма $\psi : P(\alpha) \to F$ ровно столькими способами, сколько различных корней имеет многочлен h^φ в F.

Определение 10.1. Пусть K — поле, $f \in K[x]$, $\deg f > 0$. *Поле разложения многочлена* — это такое расширение $F \supset K$, для которого f разлагается на линейные множители и не существует промежуточных полей $F \supset M \supset K$ с тем же свойством.

Задача 10.2. Пусть K — поле, $f \in K[x]$, $\deg f > 0$. Докажите, что тогда $\exists!$ с точностью до изоморфизма поле разложения f.

Указание. Постройте цепочку простых расширений, примените индукцию, задачу 10.1 и минимальность поля разложения.

Определение 10.2. Пусть P — поле, $f \in P[x]$ — неприводимый, $P \subset F$ — расширение полей, в котором $f(x)$ разлагается на линейные множители, α и β — корни $f(x)$. Тогда поля $P(\alpha)$ и $P(\beta)$ называются *сопряжёнными*, а множество корней $f(x)$ — *классом сопряжённых элементов*.

Задача 10.3. Докажите, что сопряжённые поля изоморфны.

Задача 10.4. Пусть $F = \mathbb{Q}$. Найдите степень поля разложения для следующих многочленов:
а) $ax + b$ $(a \neq 0)$; б) $x^2 - 2$; в) $x^3 - 1$; г) $x^3 - 2$; д) $x^4 - 2$;
е) $x^p - 1$ (p — простое); ж) $x^n - 1$; з) $x^p - a$ (p — простое, $\sqrt[p]{a} \notin \mathbb{Q}$).

Задача 10.5. Пусть $f = x^4 - 2$. Найдите классы сопряжённых элементов, если:
а) $P = \mathbb{Q}$; б) $P = \mathbb{Q}(\sqrt{2})$; в) $P = \mathbb{Q}(\sqrt[4]{2})$; г) $P = \mathbb{Q}(i, \sqrt[4]{2})$.

Задача 10.6. Пусть $P = \mathbb{Q}$, $f = x^4 + 1$, $g = x^4 + 2$. Докажите, что поля разложения f и g не изоморфны.

Определение 10.3. Расширение называется *нормальным*, если $\forall\, a \in F$ $\mu_a(x)$ разлагается на линейные множители.

Задача 10.7. Пусть $P \subset F$ — конечное расширение. Докажите, что тогда $P \subset F$ нормально $\Leftrightarrow$ $\exists\, f \in P[x] : F$ — поле разложения $f(x)$.

Указание. Продолжите тождественный изоморфизм до изоморфизма сопряжённых полей.

Задача 10.8*. Придумайте и докажите критерий нормальности для любых расширений полей.

Задача 10.9. Докажите, что если $P \subset F \subset L$ — расширение полей, и $P \subset L$ нормально, то $F \subset L$ нормально. (То есть нормальность сохраняется при подъёме.)

Задача 10.10. Докажите, что:
а) расширения 2-й степени всегда нормальны;
б) нормальность не транзитивна, т.е. если $P \subset F$ — нормальное $\wedge$ $F \subset L$ — нормальное $\not\Rightarrow$ $P \subset L$ — нормальное.

Указание. Воспользуйтесь примером из задачи 4.

Задача 10.11. Пусть P — поле, $|P| < \infty$, $charP = p$. Докажите, что тогда $|P| = p^n$.

Определение 10.4. Гомоморфизм алгебраической структуры (группы, кольца, поля и т.д.) в себя называется
– *мономорфизмом*, если он инъективен;
– *эндоморфизмом*, если он сюръективен;
– *автоморфизмом*, если он инъективен и сюръективен.

Задача 10.12. (Определение 10.5.) Докажите, что $\Phi : x \to x^p$ в конечных полях характеристики p является автоморфизмом. Он называется *автоморфизмом Фробениуса*.

Задача 10.13. Докажите, что для любого простого p и натурального n $\exists!\, P$ — поле, т.ч. $|P| = p^n$.

Указание. Воспользуйтесь цикличностью мультипликативной группы поля, $\exists!$ поля разложения многочлена, критерием кратности корня и эндоморфизмом Фробениуса в полях конечной характеристики.

Задача 10.14. (Следствие) Докажите, что $\forall\, n \in \mathbb{N}$ $\exists\, f \in \mathbb{Z}_p[x]$ т.ч. f неприводим и $\deg f = n$.

Обозначение. (Определение 10.6.) Поле из p^n элементов обозначается $GF(p^n)$ — *Galois Field* — и называется *полем Галуа*.

Задача 10.15. а) Постройте $GF(16)$ и найдите порождающие элементы $GF^*(16)$. Звездочка обозначает множество всех ненулевых элементов.

б) Постройте $GF(27)$ и найдите порождающие элементы $GF^*(27)$.

Указание. Найдите неприводимый многочлен нужной степени над минимальным подполем и используйте его корень. Вспомните теорему о строении конечных абелевых групп.

в) Верно ли, что $GF(16) \subset GF(64)$?

г) Найдите все подполя $GF(1024)$.

Определение 10.7. Пусть $F \subset K$ — расширение полей. Тогда $\mathrm{Aut}(K/F) = \{\varphi : K \to K$ — автоморфизм, т.ч. $\varphi|_F = id.\}$

Задача 10.16. Пусть $G = \mathrm{Aut}\, GF(p^n)$ — группа автоморфизмов $GF(p^n)$. Докажите, что тогда $G = <\Phi>$, $|G| = n$. Здесь Φ — автоморфизм Фробениуса.

Задача 10.17. Пусть $GF^*(p^n) = <\theta>$ и $h(x)$ — минимальный многочлен θ над $\mathbb{Z}_p$. Докажите, что тогда $GF(p^n)$ — поле разложения $h(x)$ и $h(x) = \prod\limits_{i=1}^{n}(x - \theta^{p^i})$.

Задача 10.18. Докажите, что:
а) $GF(p^d) \subset GF(p^n) \Leftrightarrow d \,|\, n$;
б) $\mathrm{Aut}(GF(p^n)/GF(p^d)) = <\Phi^d>$, где Φ — автоморфизм Фробениуса.

Замечание 10.1. Вспомним, что подгруппы конечной циклической группы подрядка n находятся во взаимно однозначном соответствии с делителями n. То есть мы получили взаимно однозначное соответствие между подполями конечного поля и группой автоморфизмов поля, оставляющих подполе на месте. Это и есть *соответствие Галуа*.

Задача 10.19. Пусть P — поле. Докажите, что $P^* = <a> \Leftrightarrow |P| < \infty$.

Задача 10.20*. Докажите, что $\overline{\mathbb{Z}_p} = \bigcup\limits_{n=1}^{\infty} GF(p^{n!})$.

11. Группы автоморфизмов поля. Расширения Галуа. Сепарабельность (листок 47, 10 класс)

И вот нашли большое поле,
Есть разгуляться где на воле!
М.Ю. Лермонтов, «Бородино».

Задача 11.1. (*Лемма 1*) Пусть $[L : K] = n$, $G = \mathrm{Aut}(L/K)$. Докажите, что тогда $|G| \leqslant n$.

Указание. Возьмите тождественный на K изоморфизм и продолжайте его до автоморфизма на L путём построения башни простых расширений.

Задача 11.2. Найдите группы автоморфизмов:
а) $\mathbb{C}/\mathbb{R}$; б) $\mathbb{R}/\mathbb{Q}$; в) $GF(p^n)/GF(p^k)$; г) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$; д) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$; е) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$; ж) $\mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}$; з) $\mathbb{Q}(\sqrt[3]{2})$.

Задача 11.3. Найдите группу автоморфизмов поля разложения над $\mathbb{Q}$:
а) $x^3 - 1$; б) $x^3 - 2$; в) $x^4 + 4$; г) $x^n - 1$.

В дальнейшем мы будем рассматривать только конечные расширения полей.

Определение 11.1. Расширение $L \supset K$ называется *расширением Галуа́*, если $|\mathrm{Aut}(L/K)| = [L : K]$.

В случае расширения Галуа группа автоморфизмов $\mathrm{Aut}(L/K)$ называется *группой расширения Галуа* и обозначается $\mathrm{Gal}(L/K)$.

Замечание 11.1. Расширение Галуа — это максимально *подвижное* расширение, т.е. оно имеет максимально возможное число автоморфизмов.

Задача 11.4. Какие расширения из задач 2 и 3 являются расширениями Галуа?

Определение 11.2. Пусть $L \supset K$ — конечное расширение, $H \subseteq G = \mathrm{Aut}(L/K)$ — подгруппа. Тогда *полем инвариантов* H называется $L^H = \{a \in L \,|\, \varphi(a) = a, \forall\, \varphi \in H\}$.

Задача 11.5. $L \supset K$ — конечное расширение, $H \subseteq G = \mathrm{Aut}(L/K)$. Докажите, что L^H — подполе, т.ч. $K \subset L^H \subset L$.

Задача 11.6. $P \subset F$ — конечное расширение, $G = \mathrm{Aut}(F/P)$. Докажите, что тогда:
а) $G \supset G_1 \supset G_2 \Rightarrow F^{G_1} \subset F^{G_2}$;
б) $F \supset P_1 \supset P_2 \supset P \Rightarrow \mathrm{Aut}(F/P_1) \subset \mathrm{Aut}(F/P_2)$;
в) $F^{\mathrm{Aut}(F/P)} \supset P$;
г) $\forall$ подгруппы $H \subset G$ $\mathrm{Aut}(F/F^H) \supset H$.

Задача 11.7. (*Лемма 2*) Пусть $L \supset K$ — конечное расширение, $[L : K] = n$, $G = \mathrm{Aut}(L/K)$. Докажите, что если $|G| = n$, то $L^G = K$.

Указание. Воспользуйтесь теоремой о башне расширений.

Задача 11.8. (*Лемма 3*) Пусть $L \supset K$ — конечное расширение, $[L : K] = n$, $G = \mathrm{Aut}(L/K)$, $H \subset G$ — подгруппа, т.ч. $L^H = K$. $\forall\, a \in L$ рассмотрим орбиту $Ha = \{a_1 \dots a_m\}$. Докажите, что тогда многочлен $\mu(x) = (x - a_1) \dots (x - a_m) \in K[x]$ — минимальный многочлен a над K.

Указание. Воспользуйтесь теоремой Виета и однозначностью разложения на множители.

Следствие. В условиях леммы 3 $\forall\, a \in L$ $\mu_a(x)$ не имеет кратных корней и разлагается на линейные множители над L.

Задача 11.9. (*Лемма 4*) Докажите, что векторное пространство над бесконечным полем нельзя представить в виде конечного объединения собственных подпространств.

Задача 11.10. (*Лемма 5*) Пусть $L \supset K$ — конечное расширение, $[L : K] = n$, $\mathrm{Aut}(L/K) = G$, $H \subset G$ — подгруппа, т.ч. $L^H = K$. Докажите, что тогда $H = G$ и $|G| = n$.

Указание. Постройте продолжение тождественного автоморфизма через простые расширения и воспользуйтесь теоремой о башне расширений. Представьте L как объединение собственных линейных подпространств.

В итоге доказана **теорема**:

Теорема 11.1 *$L \supset K$ — конечное расширение, $[L : K] = n$, $G = Aut(L/K)$. Тогда $|G| = n \Leftrightarrow L^G = K$.*

Определение 11.3. Пусть K — поле. $f \in K[x]$ называется *сепарабельным*, если f не имеет кратных корней ни на каком расширении поля K.

Замечание 11.2. Из задач 8, 9 листка 8,5 “Простые факты” сепарабельность равносильна условию $(f, f') \neq 1$.

Определение 11.4. Пусть $K \subset L$ — расширение полей. $a \in L$ *сепарабелен* над K, если a — корень сепарабельного многочлена $f \in K[x]$.

Задача 11.11. Пусть $K \subset L$ — расширение полей. Докажите, что $a \in L$ сепарабелен $\Leftrightarrow \mu_a$ сепарабелен.

Определение 11.5. $K \subset L$ — расширение полей называется *сепарабельным*, если $\forall\, a \in L$ a сепарабельно.

Задача 11.12. Пусть P — поле. Докажите, что если $char\, P = 0$, то все алгебраические расширения сепарабельны.

Указание. Воспользуйтесь задачей 9 листка 8,5 “Простые факты”.

Определение 11.6. Поле K называется *совершенным*, если $char\, K = 0 \vee char\, K = p$ и $\forall\, a \in K$ $\exists\, b \in K$: $b^p = a$.

Задача 11.13. Пусть $K \subset E \subset F$ — башня полей. Докажите, что если $K \subset F$ сепарабельно, то $K \subset E$ и $E \subset F$ — сепарабельные расширения.

Задача 11.14. а) Докажите, что конечные поля совершенны.

б) Докажите, что алгебраические расширения совершенных полей сепарабельны.

Задача 11.15. а) Пусть P — поле, $char\, P = p > 0$. Докажите, что многочлен $x^p - a$, где $a \in P$ либо неприводим, либо равен $(x - \theta)^p$, $\theta \in P$.

б) Докажите, что алгебраическое расширение совершенного поля совершенно.

Задача 11.16. $K = \mathbb{Z}_p(t)$ — поле рациональных дробей над $\mathbb{Z}_p$, $f(x) = x^p - t \in K[x]$. Докажите, что f неприводим и несепарабелен.

Указание. Воспользуйтесь критерием Эйзенштейна, леммой Гаусса в $\mathbb{Z}_p[t]$ и критерием сепарабельности.

12. Критерий расширения Галуа. Основная теорема теории Галуа. Теорема о примитивном элементе (листок 48, 10 класс)

Самым лучшим было бы, если бы мы занимались чисто научными исследованиями, не имеющими никакой иной цели, кроме как расширение...

Нильс Хенрик Давид Бор (1885-1962) датский физик-теоретик и общественный деятель, один из создателей современной физики

Задача 12.1. Докажите, что конечное расширение $K \subset L$ — расширение Галуа тогда оно нормально и сепарабельно.

Указание. Воспользуйтесь следствием из 11.8 и доказательством 11.10.

Определение 12.1. Пусть K — поле, $f \in K[x]$. Тогда $L = K(f)$ — *поле разложения* $f(x)$.

Задача 12.2. Докажите, что расширение $L \supset K$ — расширение Галуа тогда $L = K(f)$, $f \in K[x]$ – сепарабельный.

Указание. Воспользуйтесь доказательством 11.10.

Задача 12.3. (**Следствие**.) Пусть $K \subset M$ — конечное сепарабельное расширение. Докажите, что тогда существует расширение Галуа $K \subseteq L$, т.ч. $L \supset M$.

Задача 12.4. Постройте расширение Галуа над $\mathbb{Q}$, содержащее поле: а) $\mathbb{Q}(\sqrt[3]{2})$; б) $\mathbb{Q}(\sqrt[4]{2})$.

Определение 12.2. Пусть G — группа, S — множество всех подгрупп G, I_g — действие G на S сопряжением, т.е. $\forall g \in G\ I_g(H) = gHg^{-1}\ \forall H \subset G$. Назовём *нормализатором* подгруппы H стабилизатор при действии сопряжением, т.е. $N_G(H) = N(H) = \{g \in G : gHg^{-1} = H\}$.

Задача 12.5. Пусть G — группа, S — множество её подгрупп, I_g — действие сопряжением. Докажите, что:

а) I_g — действие G на S;

б) $H \subset N(H) \subset G$ и $H \lhd N(H)$;

в) $N(H) = G \Leftrightarrow H \lhd G$.

Замечание 12.1. Очевидно, что нормализатор — максимальная подгруппа в G, где H нормальна в ней.

Задача 12.6. Основная теорема теории Галуа.

Пусть $K \subset L$ — расширение Галуа, $G = \mathrm{Gal}(L/K)$ — группа Галуа. Докажите, что:

а) имеется биекция (*соответствие Галуа*) между множеством подгрупп $H \subseteq G$ и множеством подполей $M \subset L$, $M \supseteq K$, определённая следующим образом: каждой подгруппе сопоставим поле её инвариантов, а каждому подполю сопоставим подгруппу, состоящую из автоморфизмов расширения, оставляющих на месте все элементы подполя:

$H \mapsto M = L^H$, $M \to H = \{g \in G : g(a) = a\ \forall a \in M\} = \mathrm{Gal}(L/M)$.

Указание. Воспользуйтесь задачей 11.10.

б) если $K \subset M \subset L$, M — подполе, то $L \supset M$ — расширение Галуа и соответствующая подгруппа $H \subset G$ — его группа Галуа.

Указание. Воспользуйтесь критерием расширения Галуа, задачей 11.10 и теоремой 1 листка 11.

в) если $K \subset M \subset L$, M — подполе, то $M \supseteq K$ — расширение Галуа тогда $H \lhd G$, причём $\mathrm{Gal}(M/K) \cong G/H$.

Указание. Разложите $L \supset M$ в цепочку простых расширений и продолжите $\varphi = \mathrm{Aut}(M/K)$ до автоморфизма $g \in G$. Из а) выведите критерий нормальности подгруппы H. Воспользуйтесь задачей 5 и теоремой о башне расширений.

Задача 12.7. Найдите группы Галуа следующих расширений:
а) $GF(p^n)/GF(p^k)$; б) $\mathbb{Q}(x^n-1)/\mathbb{Q}$; в) $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$; г) $\mathbb{Q}(\sqrt{2+\sqrt{3}})/\mathbb{Q}$.

Задача 12.8. Докажите, что любое конечное сепарабельное расширение является простым.
Указание. Воспользуйтесь конечностью множества промежуточных полей и задачей 11.9.

Задача 12.9. а) Пусть K — поле, $f \in K[x]$, $L = K(f)$, $G = \mathrm{Gal}(L/K)$, f — сепарабельный (т.е. не имеет кратных корней). Докажите, что тогда f неприводим титтк G действует на корнях транзитивно (т.е. $\forall\, i,j\ \exists\, g \in G$: $g(a_i) = a_j$, где $a_1, \ldots, a_n$ — корни $f(x)$).
Указание. Воспользуйтесь задачей 11.8.
б) Докажите, что если L — расширение Галуа поля K, то элемент a — примитивный титтк длина орбиты этого элемента под действием группы Галуа равна степени расширения.

Задача 12.10. Найдите примитивные элементы и их минимальный многочлен:
а) $\mathbb{Q}(x^3-2)/\mathbb{Q}$; б) $\mathbb{Q}(\sqrt{p},\sqrt{q})/\mathbb{Q}$, p, q — простые; в) $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$.
г) Будет ли $-\frac{1}{2} + \frac{i\sqrt{2}}{2}$ порождать $\mathbb{Q}(\sqrt{2}, i)$?

Задача 12.11. Найдите группу Галуа $\mathrm{Gal}(\mathbb{Q}(x^4-2)/\mathbb{Q})$.
Указание. Воспользуйтесь тем фактом, что существует только две неабелевы группы 8-го порядка: Q_8 (группа кватернионов) и D_4 (группа диэдра).

13. Критерий Галуа разрешимости уравнения в радикалах (листок 51, 10 класс)

В этом листке везде $\mathrm{char}\, K = 0$

Определение 13.1. Расширение полей $K \subset F$ называется *радикальным*, если существует башня расширений $K = K_0 \subset K_1 \subset \ldots \subset K_{i-1} \subset K_i = K_{i-1}(b_i) \subset \ldots \subset K_s = F$, где $b_i^{n_i} \in K_{i-1}$ для некоторого $n_i \in \mathbb{N}$.

Определение 13.2. Уравнение $f(x) = 0$ *разрешимо в радикалах*, если $K(f) \subseteq F$, $F \supseteq K$ — радикальное расширение поля K.

Задача 13.1. Лемма 1. Докажите, что всякое радикальное расширение $K \subset F$ содержится в некотором радикальном расширении Галуа $K \subset E$, $E \supset F$.
Указание. Примените индукцию к башне расширений и вложите промежуточные поля в поля разложения, пользуясь задачей 10.1.

Задача 13.2. (Лемма 2.) Пусть $f(x) = x^n - 1$, $L = K(f)$. Докажите, что тогда $G = \mathrm{Aut}(L/K)$ — абелева.
Указание. Воспользуйтесь цикличностью конечной подгруппы мультипликативной группы поля.

Задача 13.3. (Лемма 3.) Пусть поле K содержит n различных корней степени n из 1. Пусть также $L = K(b)$: $b^n = c \in K$. Докажите, что тогда $L = K(f)$, где $f(x) = x^n - c$, $G = \mathrm{Aut}(L/K)$ — циклическая и n кратно $|G|$.
Указание. Постройте гомоморфизм $G \to \mathbb{Z}/n\mathbb{Z}$.

Задача 13.4. Пусть L — поле, $G = \mathrm{Aut}(L)$, $\sigma_1, \ldots, \sigma_n$ — различные автоморфизмы. Докажите, что тогда $\sigma_1, \ldots, \sigma_n$ линейно независимы над L, т.е. $\forall\, c_1, \ldots, c_n \in L$: $\sum\limits_{i=1}^{n} c_i\sigma_i = 0 \Rightarrow \forall\, i\ c_i = 0$.
Указание. Проведите индукцию по n.

Задача 13.5. (Лемма 4.) Пусть $L \supset K$ — расширение Галуа, $G = \mathrm{Gal}(L/K) = <g>$ — циклическая группа порядка n, K содержит n различных корней из 1, $r(\alpha) = \alpha + \xi g(\alpha) + \xi^2 g^2(\alpha) + \ldots + \xi^{n-1} g^{n-1}(\alpha)$, где ξ — первообразный корень n-й степени из 1, $\alpha \in L$. Докажите, что $\exists\, \alpha \in L$: $r(\alpha) \neq 0$.
Указание. Воспользуйтесь задачей 13.4.

Задача 13.6. (Лемма 5.) Пусть $L \supset K$ — расширение Галуа, $G = \mathrm{Gal}(L/K) = <g>$ — циклическая группа порядка n, K содержит n различных корней из 1. Докажите, что $\exists\, \beta \in L$: $L = K(\beta)$, $\beta^n \in K$.

Указание. В качестве β возьмите ненулевой $r(\alpha)$ из задачи 13.5, воспользуйтесь задачей 12.9 б) и докажите, что $r^n(\alpha) \in L^G = K$.

Задача 13.7. (Лемма 6.) Пусть G — конечная разрешимая группа. Докажите, что тогда можно построить следующий ряд подгрупп: $G = H_0 \triangleright H_1 \triangleright \ldots \triangleright H_{i-1} \triangleright H_i \triangleright \ldots \triangleright H_s = \{e\}$, т.ч. $H_{i-1}/H_i \cong \mathbb{Z}_{p_i}$, p_i — простое.

Указание. Рассмотрите максимальную собственную нормальную подгруппу, содержащую коммутант, и воспользуйтесь свойствами коммутанта и разрешимых групп. Вспомните задачи 4, 5, 11 и 12 листка 7,25.

Задача 13.8. Теорема Галуа. Пусть $char\ K = 0$, $f \in K[x]$, $L = K(f)$, $G = \mathrm{Aut}(L/K)$. Докажите, что уравнение $f(x) = 0$ разрешимо в радикалах титтк группа G разрешима.

Указание.

$\Rightarrow$ Примените леммы 1, 2, 3, основную теорему теории Галуа (задача 12.6) и критерий разрешимости групп. Добавьте в башню подполей корни из 1 нужной степени.

$\Leftarrow$ Примените лемму 6, основную теорему теории Галуа и присоедините к башне подполей корни из 1 нужной степени. Воспользуйтесь леммой 5 и получите радикальное расширение.

Пусть $f(x) = x^n + c_1 x^{n-1} + \ldots + c_n$ – произвольный многочлен степени n.

Вопрос. Существуют ли общие формулы, выражающие корни f через его коэффициенты $c_1, \ldots, c_n$ с помощью арифметических операций и операций извлечения корня?

Будем рассматривать $c_1, \ldots, c_n$ как независимые переменные и считать, что $f \in K(c_1, \ldots, c_n)[x]$. Если уравнение $f(x) = 0$ над полем $K(c_1, \ldots, c_n)$ разрешимо в радикалах, то решение даст нам общие формулы, выражающие корни f через его коэффициенты. Применим теорему Галуа, для этого нам нужно знать поле разложения многочлена f и вычислить его группу Галуа.

Задача 13.9. а) (Лемма 7.) Докажите, что симметрическую дробно-линейную функцию над полем K можно представить в виде дробно-рациональной функции от элементарных симметрических многочленов.

б) (Лемма 8.) Пусть K — поле, $K(c_1, \ldots, c_n)$ — поле рациональных функций от формальных переменных $c_1, \ldots, c_n$ и $L \supset K(c_1, \ldots, c_n)$ — поле разложения многочлена f. Докажите, что это расширение Галуа, причём $\mathrm{Gal}(L/K(c_1, \ldots, c_n)) \cong S_n$.

Указание. Рассмотрите расширение полей $K(\sigma_1, \ldots, \sigma_n) \subset K(x_1, \ldots, x_n)$, где x_i – формальные переменные, а σ_i – элементарные симметрические многочлены от $x_1, \ldots, x_n$. Докажите, что $L^{S_n} = K(\sigma_1, \ldots, \sigma_n)$ и воспользуйтесь теоремой Виета.

в) (Обратная задача теории Галуа.) Пусть G — конечная группа. Докажите, что $\exists\, K \subset L$ — расширение Галуа некоторых полей, т.ч. $\mathrm{Gal}(L/K) \cong G$.

Указание. Воспользуйтесь леммой 8 (задача 13.9 б)), теоремой Кэли (задача 5.10) и ОТТГ (задача 12.6).

Исходя из задачи 13.9 б) и неразрешимости S_n при $n > 4$ (листок 7,25, задача 9), доказана **теорема Абеля-Руффини**:

Общее алгебраическое уравнение степени n разрешимо в радикалах титтк $n \leqslant 4$.

Определение 13.3. Пусть G — группа. Назовём *центром* группы G $Z(G) = \{x \in G : xy = yx\ \forall\, y \in G\}$.

Замечание. Очевидно, что $Z(G) \triangleleft G$.

Задача 13.10. Первая теорема Силова. Пусть G — группа, т.ч. $|G| = p^n \cdot m$, $(m, p) = 1$. Докажите, что тогда $\exists\, H$ — подгруппа, т.ч. $|H| = p^n$.

Указание. Индукция по порядку группы. Рассмотрите действие G на себе сопряжением (задача 5.8) и исследуйте два случая: $p \mid |Z(G)|$ и $p \nmid |Z(G)|$, где $Z(G)$ – центр группы G. Используйте задачу 5.9 (обратная теорема Лагранжа).

Задача 13.11. (Лемма 9.) Пусть $f(x) \in K[x]$ — неприводимый многочлен степени n. Докажите, что тогда $\mathrm{Gal}(f) \subset S_n$.

Задача 13.12. (Лемма 10.) Пусть $G \subset S_p$: подгруппа, p — простое число. Пусть G содержит транспозицию и действует на $\{1, 2, \ldots, p\}$ транзитивно. Докажите, что:

а) $G = S_p$ при $p = 5$;

Указание. Найдите в G элемент 5-го порядка, пользуясь транзитивностью (следствие 5.1) и теоремой Силова (задача 13.10). С помощью него и транспозиции постройте элементы 4-го и 6-го порядка. Сделайте выводы о порядке подгруппы (теорема Лагранжа, листок 2).

б) $G = S_p$ при простом p.

Указание. Докажите, что $(1, 2)$ и $(1, 2, \ldots, p)$ порождают S_p. Используйте элемент порядка p и транспозицию для сведения к этому случаю.

Задача 13.13. Пусть $f(x) \in \mathbb{Q}[x]$ — неприводимый многочлен степени p, где p — простое, причём ровно 2 его корня невещественны. Докажите, что тогда $G = \mathrm{Gal}(f) \cong S_p$.

Указание. Комплексное сопряжение будет транспозицией в группе Галуа многочлена. В силу задачи 12.9 а) G действует на корнях транзитивно. Далее пользуйтесь леммой 10 (задача 13.12).

Задача 13.14. Докажите, что $\mathbb{Q}(x^5 - 10x + 5) \cong S_5$.

Указание. Воспользуйтесь критерием Эйзенштейна (задача 6.5 листка 7,5). Методами математического анализа установите существование ровно трёх вещественных корней. Воспользуйтесь задачей 13.13.

Задача 13.15. Теорема И. Шура. Пусть $P = \mathbb{Q}$, $f(x) = \sum\limits_{m=0}^{n} \dfrac{x^m}{m!}$. Докажите, что тогда $\mathrm{Gal}(f) \cong A_n$, если $n \mid 4$, и $\mathrm{Gal}(f) \cong S_n$, если $n \nmid 4$.

Задача 13.16.* Теорема И. Шафаревича.** Пусть G — конечная разрешимая группа. Докажите, что тогда $\exists\, F$ — поле, что $\mathrm{Gal}(F/\mathbb{Q}) \cong G$.

14. Построение с помощью циркуля и линейки (листок 53, 11 класс)

Рассмотрим евклидову плоскость как поле комплексных чисел, т.е. отметим точки $0, 1, i$. Тогда многие задачи на построение с помощью циркуля и линейки могут быть сформулированы в следующем виде: на плоскости отмечено несколько комплексных чисел и требуется построить ещё одно комплексное число, определённым образом зависящее от отмеченных чисел. Формализуем понятие построения циркулем и линейкой.

Определение 14.1. *Алгоритмом построения циркулем и линейкой* назовём описание конечной последовательности элементарных построений, в которых разрешается:

- провести прямую через две уже отмеченные точки;
- отметить точку пересечения двух уже проведённых прямых;
- провести окружность с центром в отмеченной точке и радиусом, равным расстоянию между двумя отмеченными точками;
- отметить точку пересечения уже проведённой прямой и уже построенной окружности;
- отметить точку пересечения двух уже построенных окружностей.

Задача 14.1. Покажите, что любое комплексное число, построенное при помощи циркуля и линейки, начиная с конечного множества отмеченных точек на комплексной плоскости, лежит в башне квадратичных расширений поля $\mathbb{Q}(z_1, \ldots, z_k)$, порождённого над $\mathbb{Q}$ исходными отмеченными точками $z_1, \ldots, z_k$.

Указание. Интерпретируйте построение точек циркулем и линейкой как процесс пересечения окружностей и прямых, проходящих через уже отмеченные точки.

Задача 14.2. Покажите, как при помощи циркуля и линейки построить комплексные числа $z_1 \pm z_2$, $z_1 \cdot z_2$, z_1/z_2, $\sqrt{z_1}$, имея отмеченными на плоскости комплексные числа $z_1, z_2 \neq 0$.

Задача 14.3. Докажите, что квадратичное расширение поля нулевой характеристики — радикальное расширение Галуа с группой $\mathbb{Z}_2$.

Задача 14.4. Пусть $char\, P = 0$ и $P = P_0 \subset P_1 \subset P_2 \subset \ldots \subset P_n$ — цепочка квадратичных расширений. Докажите, что тогда $\exists\, L$: $L \supset P$, $P_n \subset L$, $L \supset P$ — радикальное расширение Галуа и $[L : P] = 2^k$ для некоторого k.

Указание. Вспомните доказательство 13.1 и включите в индукционное предположение требование, чтобы степень расширения была степенью двойки.

Задача 14.5. Критерий построимости. Докажите, что при помощи циркуля и линейки можно построить комплексное число z из отмеченных комплексных чисел $z_1, \ldots, z_n$ титтк число z алгебраично над $\mathbb{Q}(z_1, \ldots, z_n)$ и $\mathrm{Gal}(\mu_z)$ над $\mathbb{Q}(z_1, \ldots, z_n)$ является 2-группой.

Указание. $\Rightarrow$ Воспользуйтесь 14.4, 12.6 и теоремой о башне полей (9.13).

$\Leftarrow$ Воспользуйтесь разрешимостью p-группы (задача 16 листка 7,25), 13.7, 12.6 и постройте башню квадратичных расширений. Примените 14.3.

Задача 14.6. (Следствие.) Докажите, что правильный n-угольник можно построить с помощью циркуля и линейки титтк $\varphi(n) = 2^k$ для некоторого $k \in \mathbb{N}$.

Указание. Построение правильного n-угольника эквивалентно построению первообразного корня n-й степени из 1. Вспомните задачу 14 из Листка 7,5.

Задача 14.7. С помощью циркуля и линейки постройте правильный n-угольник. Выразите $\cos\frac{2\pi}{n}$ в квадратных радикалах. а) $n = 5$; б*) $n = 17$.

Указание. а) Рассмотрите $G = \mathrm{Gal}(x^n - 1)$, найдите в ней образующий и постройте ряд $\{e\} \subset G_1 \subset \ldots \subset G_k = G$, т.ч. $G_{i+1}/G_i \cong \mathbb{Z}_2$. Заметьте, что комплексное сопряжение — элемент группы G.

Задача 14.8. Пусть $2^k + 1$ – простое число, $k \in \mathbb{N}$. Докажите, что тогда $\exists\, l \in \mathbb{N} \cup \{0\}$: $k = 2^l$.

Замечание 14.1. Числа вида $2^{2^k} + 1$ называют *числами Ферма́*.

Задача 14.9*.** Приведите первые 6 простых чисел Ферма. *Можно пользоваться компьютером.*

Задача 14.10. (Теорема Гаусса-Ванцеля.) Для построения правильного n-угольника с помощью циркуля и линейки необходимо и достаточно, чтобы $n = 2^k \cdot p_1 \cdot \ldots \cdot p_s$, где p_i – простое число Ферма ($i \in \{1, \ldots, s\}$).

Задача 14.11. Докажите, что многочлен $4x^3 - 3x - \alpha$ неприводим над $\mathbb{Q}(\alpha)$, где α – независимая переменная.

Указание. Вспомните лемму Гаусса для факториальных колец (задача 5 листка 7,5) и посмотрите на многочлен как на линейный многочлен от α.

Задача 14.12. (Задача о трисекции угла.) Докажите, что задача о делении угла φ на 3 равные части с помощью циркуля и линейки неразрешима в общем случае.

Указание. Вспомните формулу косинуса тройного угла и примените 14.11 ($\alpha = \cos\varphi$).

Задача 14.13. Покажите, что угол $\frac{2\pi}{3}$ нельзя разделить на 3 равных части с помощью циркуля и линейки.

Указание. Докажите неприводимость над $\mathbb{Q}$ многочлена $8x^3 - 6x + 1$.

Задача 14.14. (Критерий деления угла на 3 равных.) Докажите, что угол в φ радиан допускает трисекцию титтк $\xi = e^{i\varphi}$ является кубом в поле $\mathbb{Q}(\xi)$.

Указание. Рассмотрите многочлен $x^3 - \xi$ и используйте 14.5.

Задача 14.15. Докажите, что угол в $\frac{2\pi}{n}$ радиан допускает трисекцию титтк $(n, 3) = 1$.

Указание. Используйте 10.4, 14.5 и мультипликативность $\varphi(n)$.

Задача 14.16. С помощью циркуля и линейки постройте угол в 3° и выразите $\cos 3^\circ$ с помощью квадратных радикалов.

Указание. Используйте 14.7 а).

Задача 14.17. (Задача об удвоении куба.) С помощью циркуля и линейки постройте ребро куба объёма 2.

Задача 14.18. (Задача о квадратуре круга.) С помощью циркуля и линейки постройте сторону квадрата, равновеликого окружности единичного радиуса.

Указание. Используйте трансцендентность числа π (1882г., Ф.Линдеман).

15. Основная теорема алгебры. Формула Кардано. Теорема Веддербёрна (листок 54, 11 класс)

Задача 15.1. Докажите, что:

а) $\forall\, f(x) \in \mathbb{R}[x]$, $\deg f$ нечётна $\exists\, x_0 \in \mathbb{R}$: $f(x_0) = 0$;

б) $\forall\, z \in \mathbb{C}\ \exists\, z_0$: $z_0^2 = z$;

в) у поля $\mathbb{C}$ нет расширений 2-й степени;

г) расширение 2-й степени над $\mathbb{R}$ изоморфно $\mathbb{C}$.

Указание. г) Воспользуйтесь существованием и единственностью поля разложения (10.2).

Задача 15.2. Пусть $\mathbb{R} \subset K$ — конечное алгебраическое расширение. Докажите, что если $[K : \mathbb{R}]$ нечётна, то $K = \mathbb{R}$.

Указание. Воспользуйтесь теоремой о башне полей и 15.1 а).

Задача 15.3. Пусть $f(x) \in \mathbb{C}[x]$. Докажите, что тогда $g(x) = f \cdot \overline{f} \in \mathbb{R}[x]$ и если g имеет корень в $\mathbb{C}$, то и f имеет корень в $\mathbb{C}$.

Задача 15.4. (**Основная теорема алгебры.**) Пусть $f(x) \in \mathbb{C}[x]$. Докажите, что тогда $\exists\, x_0 \in \mathbb{C}$: $f(x_0) = 0$.

Указание. Постройте $\mathbb{R}(f\overline{f})$ и воспользуйтесь ОТТГ (12.6), первой теоремой Силова (13.10), 15.1, 15.2, 13.7 и задачей 16 листка 7,25.

Пусть K — поле, $char\, K = 0$ (хотя достаточно, чтобы $char\, K \neq 2, 3$).

Задача 15.5. (Лемма 1.) Пусть $f(x) \in K[x]$, $\deg f = 3$. Докажите, что для решения уравнения $f(x) = 0$ достаточно решить уравнение $g(x) = 0$, где $g(x) = x^3 + px + q$.

В дальнейшем для простоты формул будем использовать только это редуцированное уравнение.

Обозначение. Пусть $g(x) = x^3 + px + q$, x_1, x_2, x_3 – его корни. Тогда $D = \prod\limits_{i<j} (x_i - x_j)^2$.

Задача 15.6. (Лемма 2.) Пусть $L = K(g)$, $g(x) = x^3 + px + q$. Докажите, что $D = -4p^3 - 27q^2$ и что $\sqrt{D}$ инвариантен относительно действия A_3 на корнях $g(x)$.

Будем применять результаты листков 12 и 13. Согласно 13.9 б) $\mathrm{Gal}\, g(x) \cong S_3$ (в общем случае), где $g(x) = x^3 + px + q$. Ряд из коммутантов для S_3 будет $S_3 \triangleright A_3 \triangleright \{e\}$ (задача 7 из листка 7,25), причём $S_3/A_3 \cong \mathbb{Z}_2$. Заметим, что $A_3 = <(123)>$. Рассмотрим башню полей $K \subset K(\sqrt{D}) \subset K(g)$. По 12.6, т.к. $\mathrm{Gal}\,(g) = S_3$, $S_3 \triangleright A_3 \triangleright \{e\}$ — соответствие Галуа. Подгруппе индекса 2, очевидно, соответствует квадратичное расширение (12.6). Чтобы применить 13.5 и 13.6, нужно к $K(\sqrt{D})$ добавить корень третьей степени из 1, т.е. решение уравнения $x^2 + x + 1 = 0$. Очевидно, что достаточно добавить $\sqrt{-3}$. Получим $K(\sqrt{D}, \sqrt{-3})$.

Пусть ρ — первообразный корень 3-й степени из 1. Очевидно, что ρ^2 — тоже первообразный. Согласно 13.5, построим две ***резольве́нты Лагранжа***: $r_1(x_1) = x_1 + \rho x_2 + \rho^2 x_3$ и $r_2(x_1) = x_1 + \rho^2 x_2 + \rho x_3$, т.к. $A_3 = <(123)>$ и A_3 действует на корнях $g(x)$. Также заметим, что $x_1 + x_2 + x_3 = 0$ (формула Виета). По 13.6 $r_1^3(x_1)$ и $r_2^3(x_1)$ должны лежать в основном поле, т.е. выражаться через $\sqrt{D}$ и $\sqrt{-3}$.

Задача 15.7. Докажите, что $r_1^3(x_1) = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3}\sqrt{D}$ и $r_2^3(x_1) = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\sqrt{D}$.

Указание. Примените формулы Виета и основную теорему о симметрических многочленах.

Задача 15.8. Докажите, что $r_1(x_1) \cdot r_2(x_1) = -3p$.

Вывод. Т.к. $r_1(x_1) = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}$, $r_2(x_1) = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}}$, а корень 3-й степени — функция многозначная, то выбирать значение корня нужно так, чтобы выполнялось 15.8.

Задача 15.9. Докажите, что $3x_1 = r_1(x_1) + r_2(x_1)$, $3x_2 = \rho^2 r_1(x_1) + \rho r_2(x_1)$, $3x_3 = \rho r_1(x_1) + \rho^2 r_2(x_1)$.

Полученные формулы называются *формулами Кардáно* (1545), хотя их авторами являются Сципион Дель Ферро и Никола Тарталья (1534). Иногда формулу Кардано записывают так:

$$x_{1,2,3} = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{\rho^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{\rho^3}{27} + \frac{q^2}{4}}}.$$

Задача 15.10. Решите следующие уравнения:

а) $x^3 + 3x - 2 = 0$;

б) $x^3 + 6x - 9 = 0$.

Задача 15.11. Докажите, что если $q \in \mathbb{N}$ и $\Phi_n(q) | q - 1$, то $n = 1$, где Φ_n — круговой многочлен.

Указание. Рассмотрите $|\Phi_n(q)|$ и вспомните определение кругового многочлена. Используйте геометрические соображения.

Задача 15.12. (Теорема Веддербёрна.) Пусть D — тело, $|D| < \infty$. Докажите, что тогда D коммутативно, т.е. является полем.

Указание. Рассмотрите D как линейное пространство над своим центром. Подействуйте на D^* сопряжением и примените формулу классов (5.8) к этому действию. Примените индукцию по размерности D над своим центром, посчитайте элементы в формуле классов. Примените задачи 10, 12 из листка 7,5 и 15.11.

16. p-адические числа (листок 56, 11 класс)

Преамбула. Рассмотрим уравнение $x^2 \equiv 2 (\mathrm{mod}\ 7^n)$. При $n = 1$ мы имеем $x_0 \equiv \pm 3\ (\mathrm{mod}\ 7^1)$.

Пусть $n = 2$: $x^2 \equiv 2 (\mathrm{mod}\ 7^2) \Rightarrow x^2 \equiv 2 (\mathrm{mod}\ 7)$, значит решение имеет вид $x_0 + 7t_1$. Пусть $x_0 = 3$ ($x_0 = -3$ рассматривается аналогично) т.е. $x_1 = 3 + 7t_1$. Значит $(3 + 7t_1)^2 \equiv 9 + 6 \cdot 7 \cdot t_1 + 7^2 t_1^2 \equiv 2 (\mathrm{mod}\ 7^2) \equiv 1 + 6t_1 \equiv 0 (\mathrm{mod}\ 7)$, т.е. $t_1 \equiv 1 (\mathrm{mod}\ 7)$ и $x_1 \equiv 3 + 7 \cdot 1 (\mathrm{mod}\ 7^2)$.

Аналогично, при $n = 3$ получаем $x_2 = x_1 + 7^2 \cdot t_2$ и $t_2 \equiv 2 (\mathrm{mod}\ 7)$, т.е. $x_2 \equiv 3 + 7 \cdot 1 + 7^2 \cdot 2 (\mathrm{mod}\ 7^3)$. Продолжая таким образом, мы получим последовательность $x_0, x_1, \ldots, x_n, \ldots$ с такими свойствами: $x_0 \equiv 3 (\mathrm{mod}\ 7)$, $x_n \equiv x_{n-1} (\mathrm{mod}\ 7^n)$, $x_n^2 \equiv 2 (\mathrm{mod}\ 7^{n+1})$.

Аналогия. Для решения уравнения $x^2 = 2$ мы идём таким путём: мы строим последовательность рациональных чисел: $r_0, r_1, r_2, \ldots, r_n, \ldots$ таких, что $|r_n^2 - 2| < 10^{-n}$.

Эта аналогия будет практически полной, если мы условимся два целых числа называть **p**-*близкими* (в нашем примере $p = 7$), когда их разность делится на достаточно большую степень p, где p – простое число. То есть, мы построили последовательность такую, что квадраты её членов становятся сколь угодно 7-близкими к 2. Почти как в привычной нам десятичной записи.

Определение 16.1. Пусть p — простое число. Последовательность

$$\{x_n\} = \{x_0, x_1, x_2, \ldots, x_n, \ldots | x_i \in \mathbb{Z}\ \forall i \bigwedge x_n \equiv x_{n-1} (\mathrm{mod}\ p^n)\ \forall n \geq 1\}$$

называется *целым p-адическим числом*. Две последовательности $\{x_n\}$ и $\{x'_n\}$ определяют одно и то же p-адическое число тогда и только тогда, когда $x_n \equiv x'_n (\mathrm{mod}\ p^{n+1})\ \forall n \geq 0$.

Обозначение. $\{x_n\}$ определяет целое p-адическое число α, записывается: $\{x_n\} \to \alpha$. Множество всех целых p-адических чисел обозначается $\mathbb{Z}_p$.

Задача 16.1. Сопоставим произвольному $m \in \mathbb{Z}$ p-адическое число: $\{m, m, m, \ldots\}$. Докажите, что $\{m, m, m, \ldots\} = \{n, n, n, \ldots\} \Rightarrow m = n$, т.е. $\mathbb{Z} \subset \mathbb{Z}_p$.

Определение 16.2. Пусть $\alpha \in \mathbb{Z}_p$ и $\alpha = \{x_0, x_1, \ldots | x_i \in \mathbb{Z}\}$. Назовём *канонической записью* такую последовательность $\{x_0', x_1', \ldots\}$: $x_n \equiv x_n' (\mathrm{mod}\ p^{n+1})$ $\forall n \geq 0$ и $\forall x_n'$ $0 \leq x_n' < p^{n+1}$.

Задача 16.2. Докажите, что каноническая запись целого p-адического числа единственна.

Задача 16.3. Докажите, что $\forall \alpha \in \mathbb{Z}_p$ каноническую запись можно представить в виде $\{a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots\}$, где $0 \leq a_i < p$ $\forall i$.

Задача 16.4. Докажите, что $\mathbb{Z}_p$ имеет мощность континуума.

Определение 16.3. Пусть α, $\beta \in \mathbb{Z}_p$ $\alpha = \{x_0, x_1, \ldots\}$ $\beta = \{y_0, y_1, \ldots\}$. Тогда *сумма* $\alpha + \beta = \{x_0 + y_0, x_1 + y_1, \ldots\}$, а *произведение* $\alpha \cdot \beta = \{x_0 y_0, x_1 y_1, \ldots\}$.

Задача 16.5. Покажите, что определение 3 корректно и устанавливает на $\mathbb{Z}_p$ структуру коммутативного кольца с единицей.

Определение 16.4. Пусть α, $\beta \in \mathbb{Z}_p$. Будем говорить, что α *делит* β $(\alpha | \beta)$, если $\exists \gamma \in \mathbb{Z}_p : \beta = \alpha\gamma$.

Определение 16.5. Пусть $\alpha \in \mathbb{Z}_p$. α называется *обратимым* или *делителем единицы*, если $\exists \beta \in \mathbb{Z}_p : \alpha\beta = 1$.

Задача 16.6. Пусть $\alpha \in \mathbb{Z}_p$, $\alpha = \{x_0, x_1, \ldots\}$. Докажите, что тогда α обратим $\Leftrightarrow x_0 \not\equiv 0 (\mathrm{mod}\ p)$.

Задача 16.7. Докажите, что $\forall \alpha \in \mathbb{Z}_p$ $\exists\, \varepsilon \in \mathbb{Z}_p$ – делитель единицы, $\exists\, m \geq 0$, $m \in \mathbb{Z}$ такое, что $\alpha = p^m \cdot \varepsilon$, и такое представление однозначно.

Задача 16.8. а) Докажите, что $\mathbb{Z}_p$ – область целостности, т.е. коммутативное кольцо с единицей и без делителей 0.

б) К какому типу колец относится $\mathbb{Z}_p$: евклидово, кольцо главных идеалов, факториальное?

в) Опишите простые элементы в $\mathbb{Z}_p$.

Определение 16.6. Пусть $\alpha \in \mathbb{Z}_p$, $\alpha = p^m \cdot \varepsilon$, где ε – делитель единицы. Тогда m называется *p-показателем* α и обозначается $\nu_p(\alpha)$.

Задача 16.9. Пусть α, $\beta \in \mathbb{Z}_p$. Докажите, что:

а) $\nu(\alpha\beta) = \nu(\alpha) + \nu(\beta)$;

б) $\nu(\alpha + \beta) \geq \min(\nu(a), \nu(\beta))$;

в) $\nu(\alpha + \beta) = \min(\nu(a), \nu(\beta)$, если $\nu(a) \neq \nu(\beta))$;

г) $\alpha | \beta \Leftrightarrow \nu(\alpha) \leq \nu(\beta)$.

Задача 16.10. Докажите, что $\mathbb{Z}_p/(p^k) \cong \mathbb{Z}/p^k\mathbb{Z}$.

Определение 16.7. Поле отношений $\mathbb{Z}_p$ называется *полем p-адических чисел* и обозначается $\mathbb{Q}_p$, а его элементы называются *p-адическими числами*.

Задача 16.11. а) Сформулируйте критерий Эйзенштейна для $\mathbb{Z}_p[x]$.

б) Докажите, что $\forall\, n \in \mathbb{N}$ над $\mathbb{Q}_p$ существует алгебраическое расширение степени n.

Определение 16.8. Пусть F – поле, $||\ || : F \to \mathbb{R}^+$, т.ч.

1) $||x|| = 0 \Leftrightarrow x = 0$;

2) $||xy|| = ||x|| \cdot ||y||$;

3) $||x + y|| \leqslant ||x|| + ||y||$.

Тогда функция $||\ ||$ называется *нормой* на поле F.

Если выполняется 3'), то норма называется *неархимедовой*, иначе она называется *архимедовой*:

3') $||x + y|| \leqslant \max(||x||, ||y||)$.

Задача 16.12. Докажите, что норма $||\ ||$, заданная на поле F, неархимедова титтк $||n|| \leqslant 1$ $\forall\, n \in \mathbb{N}$.

Задача 16.13. Пусть $\alpha \in \mathbb{Q}_p$. Докажите, что тогда $\exists!\, m \in \mathbb{Z}$, $\varepsilon \in \mathbb{Z}_p$ – делитель единицы, т.ч. $\alpha = p^m \cdot \varepsilon$.

Замечание. Число m по-прежнему называется p-показателем.

Определение 16.8. Пусть $\xi \in \mathbb{Q}_p$, $||\ ||_p$: $\mathbb{Q}_p \to \mathbb{R}^+$: $||\xi||_p \stackrel{\text{def}}{=} p^{-\nu(\xi)}$. Тогда $||\ ||_p$ называется *p-адической нормой.*

Задача 16.14. Докажите, что $||\ ||_p$ – неархимедова норма $\mathbb{Q}_p$.

Определение 16.9. Пара (X, ρ) называется *метрическим пространством*, где X — множество, если функция $\rho : (X \times X) \to \mathbb{R}^+$ (называемая *метрикой*) удовлетворяет следующим условиям 1)-3):
1) $\rho(x, y) = 0 \Leftrightarrow x = y$;
2) $\rho(x, y) = \rho(y, x)$;
3) $\rho(x, z) \leq \rho(x, y) + \rho(y, z)$.
Если выполняется 3'), то метрика ρ называется *неархимедовой*:
3') $\rho(x, z) \leqslant \max(\rho(x, z), \rho(y, z))$.

Определение 16.10. *p-адической метрикой* на $\mathbb{Q}_p$ называется функция $\rho(x, y) \stackrel{\text{def}}{=} ||x - y||_p$, где $x, y \in \mathbb{Q}_p$.

Задача 16.15. Покажите, что функция ρ на $\mathbb{Q}_p$ является неархимедовой метрикой.

Задача 16.16. Вычислите $||x - y||_p$, если:
а) $x = 1$, $y = 26$, $p = 5$;
б) $x = \dfrac{1}{9}$, $y = -\dfrac{1}{16}$, $p = 5$;
в) $x = \dfrac{(9!)^2}{3^9}$, $y = 0$, $p = 3$;
г) $x = \dfrac{2^{2^N}}{(2^N)!}$, $y = 0$, $p = 2$.

Задача 16.17. Пусть $x \in \mathbb{Q}$ и $||x||_\infty \stackrel{\text{def}}{=} |x|$. Докажите, что $\prod\limits_{p=2}^{\infty} ||x||_p = 1$, где p пробегает все простые числа и ∞.

17. Начала p-адического анализа (листок 57, 11 класс)

Задача 17.1. Пусть F – поле с неархимедовой метрикой $||\ ||$. Докажите, что:
а) в F все треугольники равнобедренные (**Принцип равнобедренных треугольников**);
б) любая точка круга является его центром;
в) если окружности пересекаются, то они — концентрические.

Задача 17.2. Пусть $\alpha \in \mathbb{Z}_p$, $\alpha = \{x_0, x_1, \ldots\}$. Докажите, что тогда последовательность $\{x_n\}$ сходится к α в смысле p-адической метрики.

Задача 17.3. Докажите, что $\forall \alpha \in \mathbb{Q}_p\ \exists \{x_n : x_i \in \mathbb{Q}\ \forall i\}$ т.ч. $\{x_n\} \to \alpha$.

Задача 17.4. а) Докажите, что любая ограниченная последовательность p-адических чисел имеет сходящуюся подпоследовательность.

Указание. Сведите всё в $\mathbb{Z}_p$, затем согласно 16.10 для любого натурального k выберите подпоследовательность, попадающую в один смежный класс, затем «диагональным методом» постройте предельную точку.

б) **Критерий Коши в p-адической метрике.** Докажите, что для сходимости последовательности $\{\xi_i : \xi_i \in \mathbb{Q}_p\ \forall i\}$ необходимо и достаточно, чтобы $\lim\limits_{n\to\infty} (\xi_{n+1} - \xi_n) \to 0$.

Указание. Воспользуйтесь 17.4 а) и действуйте аналогично вещественному случаю.

Задача 17.5. Докажите, что для сходимости ряда $\sum\limits_{i=0}^{\infty} \alpha_i$, где $\alpha_i \in \mathbb{O}_p\ \forall i$ необходимо и достаточно, чтобы $\lim\limits_{n\to\infty} \alpha_n \to 0$.

Задача 17.6. Докажите, что при любой перестановке членов сходящегося ряда в поле p-адических чисел его сходимость не нарушается и сумма не меняется, т.е. любой сходящийся ряд сходится абсолютно.

Задача 17.7. Докажите, что каждое ненулевое p-адическое число однозначно записывается в виде:

$$\xi = p^m(a_0 + a_1 p + \ldots + a_n p^n + \ldots), \text{ где } m = \nu_p(\xi),\ 1 \leq a_0 \leq p-1,\ 0 \leq a_i \leq p-1\ \forall i \in \mathbb{N}.$$

Замечание 1. Почти всё, как в $\mathbb{R}$, но в p-адических числах нет двойственности типа $0{,}9999\ldots$.

Замечание 2. Вспоминая, как в листке 39 мы строили из фундаментальных последовательностей рациональных чисел поле $\mathbb{R}$ (метод Кантора), сейчас мы фактически показали (задачи 17.3, 17.4, 17.7), что $\mathbb{Q}_p$ — это пополнение $\mathbb{Q}$ по p-адической метрике.

Задача 17.8. Найдите сумму ряда $1 + p + p^2 + \ldots$ в p-адической метрике.

Задача 17.9. Пусть уравнение $x^2 = 2$ разрешимо в $\mathbb{Z}/p\mathbb{Z}$. Докажите, что тогда при $p \neq 2$ существуют два различных корня этого уравнения.

Указание. Построение решения рассмотрено в преамбуле предыдущего листка.

Задача 17.10. Вычислите (а), б), в) — «в столбик») с четырьмя знаками:
а) $(3+6\cdot 7+2\cdot 7^2+\ldots)\times(4+5\cdot 7+1\cdot 7^2+\ldots)$; б) $(2\cdot 7^{-1}+0\cdot 7^0+3\cdot 7^1+\ldots)-(4\cdot 7^{-1}+6\cdot 7^0+5\cdot 7^1+\ldots)$;
в) $(1+2\cdot 7+4\cdot 7^2+\ldots):(3+5\cdot 7+1\cdot 7^2+\ldots)$; г) $\pm\sqrt{-1}$ в $\mathbb{Q}_{13}$.

Указание. г) Воспользуйтесь техникой из 17.9.

Задача 17.11. Для каких простых $p \in [2;19]$ можно найти $\sqrt{-1}$ в $\mathbb{Q}_p$?

Указание. Сначала докажите, что a — квадрат в F_p^* $(p \neq 2) \Leftrightarrow a^{\frac{p-1}{2}} = 1$ в F_p^*, затем ищите корень, как показано в преамбуле предыдущего листка.

Задача 17.11,5 (Лемма Гéнзеля). Обобщая построение решения уравнений в 17.10 г) и 17.11, докажите *лемму Гéнзеля*: Пусть $F(x) \in \mathbb{Z}_p[x]$, $a_0 \in \mathbb{Z}_p$, $F(a_0) \equiv 0 (\mathrm{mod}\, p)$, $F'(a_0) \not\equiv 0 (\mathrm{mod}\, p)$. Тогда существует единственное $a \in \mathbb{Z}_p$, такое что $F(a) = 0$ и $a \equiv a_0 (\mathrm{mod}\, p)$.

Указание. Используйте индукционное построение.

Задача 17.12. Представьте $-1 \in \mathbb{Z}_p$ в виде ряда $a_0 + a_1 p + a_2 p^2 + ...$, где $a_i \in \mathbb{Z}$ и $0 \leq a_i \leq p-1$ $\forall\ i$.

Задача 17.13. а) Докажите, что $\forall\, \alpha \in \mathbb{Q}$, $\alpha \neq 0$ представление в виде ряда из задачи 17.7 в поле $\mathbb{Q}_p$ имеет периодические коэффициенты, начиная с некоторого места. Покажите, что обратное тоже верно.

Указание. Представьте $\alpha = c - \frac{a}{b}$, где $c \in \mathbb{Z}$, $a, b \in \mathbb{N}$, $\frac{a}{b}$ – правильная дробь. Воспользуйтесь формулой Эйлера: $b \mid (p^{\varphi(b)} - 1)$. Используйте задачу 17.8.

б*) Докажите, что $\forall\, p$ ряд Эйлера $\sum_{n=0}^{\infty} n!$ сходится в $\mathbb{Q}_p$ к иррациональному числу.

Указание. Докажите, что $\forall\, m \in \mathbb{Z}$ число $m \cdot \sum_{n=0}^{\infty} n!$ не будет натуральным.

Задача 17.14. Представьте $-2/3 \in \mathbb{Z}_5$ в виде ряда $a_0 + a_1 p + a_1 p^2 + ...$, где $a_i \in \mathbb{Z}$ и $0 \leq a_i \leq p-1$ $\forall i$.

Указание. Используйте технику из задачи 17.13.

Задача 17.15. Докажите, что уравнение $x^p = 1$ имеет ровно один корень в $\mathbb{Q}_p$, где $p \neq 2$.

Указание. Рассмотрите $f(x) = x^{p-1} + x^{p-2} + \ldots + 1$ и, пользуясь критерием Эйзенштейна 16.11 а), докажите его неприводимость. Рассмотрите $f(x+1)$ и вспомните свойства делимости C_p^n, где $1 \leqslant k < p-1$.

Задача 17.16. Пусть $c \in \mathbb{Z}$, $(c, p) = 1$. Докажите, что:
а) $\exists\, \gamma = \lim\limits_{n\to\infty} c^{p^n}$ в $\mathbb{Q}_p$; б) $\gamma = c\,(\mathrm{mod}\, p)$; в) $\gamma^{p-1} = 1$ в $\mathbb{Q}_p$, т.е. $\gamma_1, \ldots, \gamma_{p-1}$ — корни уравнения $x^{p-1} - 1 = 0$.

Указание. а) Воспользуйтесь формулой Эйлера.

Определение 17.1. Числа $\gamma_1, \ldots, \gamma_{p-1}$ называются *представителями Тейхмю́ллера* в $\mathbb{Q}_p$.

Определение 17.2. Метрики в поле F называются *эквивалентными*, если множества бесконечно малых последовательностей совпадают.

Определение 17.3. Норма $||\ ||$ на поле F называется *тривиальной*, если $\forall\, x \neq 0\ ||x|| = 1$.

Задача 17.17. Теорема Островского. а) Докажите, что любая нетривиальная неархимедова метрика на $\mathbb{Q}$ — p-адическая.

б*) Докажите, что любая нетривиальная архимедова метрика на $\mathbb{Q}$ — абсолютная величина.

Указание. а) Докажите, что только для одного простого p $||p|| < 1$.

Задача 17.18. Докажите, что: а) $\mathbb{Q}_p \ncong \mathbb{Q}_q$ при $p \neq q$; б) $\mathbb{Q}_p \ncong \mathbb{R}$.

Указание. Воспользуйтесь 17.11 и постройте многочлен, приводимый в одном поле и неприводимый в другом.

Задача 17.19. Докажите, что $\operatorname{Aut} \mathbb{Q}_p = \mathrm{id}$.

Указание. С помощью 17.11 докажите, что уравнение $x^n = 1 + pz$ $(z \in \mathbb{Z}_p)$ имеет решение $\forall\, n$: $(n, p) = 1$. Отсюда выведите, что любой автоморфизм $\mathbb{Q}_p$ изометричен, а значит, непрерывен. Затем воспользуйтесь 17.3.

18. Множества. Теорема Кантора-Бернштейна. Лемма Цорна. Базис Гамеля (листок 58, 11 класс)

Задача 18.1. Докажите, что множество всех подмножеств счётного множества равномощно множеству всех бесконечных последовательностей из нулей и единиц.

Задача 18.2. Докажите, что множество алгебраических чисел (алгебраическое замыкание поля $\mathbb{Q}$) счётно.

Задача 18.3. Докажите, что если множество A бесконечно, а B конечно или счётно, то $A \cup B$ равномощно A.

Определение 18.1. Множество называется *бесконечным по Дедекúнду*, если оно равномощно некоторому своему собственному подмножеству.

Задача 18.4. Множество бесконечно тогда и только тогда, когда оно содержит счетное подмножество.

Задача 18.5. Докажите, что квадрат $[0, 1] \times [0, 1]$ равномощен отрезку $[0, 1]$.

Замечание. Существует непрерывное отображение отрезка на квадрат, образ которого проходит через каждую точку квадрата («кривая Пеано»).

Задача 18.6 Теорема Кантора-Бернштейна. Докажите, что если множество A равномощно некоторому подмножеству множества B, а B равномощно некоторому подмножеству множества A, то множества A и B равномощны.

Задача 18.7. Множество всех бесконечных последовательностей из нулей и единиц (канторово множество) несчётно.

Задача 18.8 (**Теорема Кантора**). Никакое множество не равномощно множеству всех своих подмножеств.

Определение 18.2. Бинарное отношение $\leq$ на множестве X называется *отношением частичного порядка*, если выполняются следующие свойства:

– *рефлексивность*: $x \leq x\ \forall\ x \in X$;

– *антисимметричность*: $(x \leq y$ и $y \leq x) \Rightarrow x = y$;

– *транзитивность*: $(x \leq y$ и $y \leq z) \Rightarrow x \leq z$.

Множество с заданным на нём отношением частичного порядка называют *частично упорядоченным множеством* (ЧУМ).

Определение 18.3. Два элемента ЧУМ называются *сравнимыми*, если $x \leq y$ или $y \leq x$. ЧУМ, в котором любые два элемента сравнимы, называется *линейно упорядоченным множеством*.

Определение 18.4. Линейно упорядоченное подмножество ЧУМ называется *цепью*.

Задача 18.9. Приведите 3 примера ЧУМ и цепи в нём. Хотя бы одно из них должно быть не линейно упорядоченным множеством с бесконечной цепью.

Задача 18.10. Приведите примеры естественного бесконечного ЧУМ, в котором любая цепь конечна.

Определение 18.5. Пусть $A \subset X$, X — ЧУМ. Тогда элемент $x \in X$: $a \leqslant x \ \forall\, a \in A$ называется *верхней гранью* A.

Определение 18.6. Пусть X — ЧУМ. Элемент $a \in X$ называется *максимальным*, если не существует большего элемента.

Лемма Цо́рна. *Пусть Z — ЧУМ, в котором всякая цепь имеет верхнюю грань. Тогда в Z есть максимальный элемент, и, более того, $\forall\, a \in Z\ \exists\, b \geqslant a$: b — максимальный элемент в Z.*

Примечание. Лемма Цорна является аксиомой!

Задача 18.11. Пусть R — коммутативное кольцо с единицей. Докажите, что в R существует максимальный идеал, отличный от R.

Задача 18.12. Докажите, что любое поле можно вложить в алгебраически замкнутое поле.

Указание. Воспользуйтесь задачей 18.11.

Задача 18.13. Пусть $K \subset L$ — алгебраическое расширение полей, M — алгебраически замкнутое поле. Докажите, что тогда всякое вложение $\varphi : K \to M$ продолжается до вложения $\psi : L \to M$.

Задача 18.14. Докажите, что алгебраическое замыкание поля единственно с точностью до изоморфизма.

Указание. Примените задачу 18.13.

Задача 18.15. Алгебраическое расширение бесконечного поля равномощно исходному полю.

Определение 18.7. Пусть L — векторное пространство над полем F. Множество векторов $B \subset L$ называется *линейно независимым*, если любая конечная линейная комбинация векторов из B с коэффициентами из F, равная нулю, имеет все коэффициенты, равные нулю.

Линейно независимое множество векторов B называется *базисом Га́меля* пространства L, если любой вектор из L представим в виде конечной линейной комбинации элементов из B.

Задача 18.16. Докажите, что любое линейно независимое множество векторов может быть расширено до базиса Гамеля и разложение любого элемента по этому базису единственно.

Задача 18.17. Пусть $f : \mathbb{R} \to \mathbb{R}$ — функция, удовлетворяющая условию Коши $f(x + y) = f(x) + f(y)\ \forall\, x, y \in \mathbb{R}$ (иначе, это гомоморфизм абелевых групп по сложению). Докажите, что либо $f(x) = cx$ при некотором фиксированном $c \in \mathbb{R}$, либо $f(x)$ всюду разрывна.

Задача 18.18. Используя базис Гамеля, приведите пример разрывной функции $f : \mathbb{R} \to \mathbb{R}$, удовлетворяющей условию Коши.

Задача 18.19*. Докажите, что разрывная функция $f : \mathbb{R} \to \mathbb{R}$, удовлетворяющая условию Коши:

а) разрывна в любой точке;

б) не монотонна ни на каком отрезке и не сохраняет знак ни на каком отрезке;

в) неограниченна на любом отрезке;

г) $f(I)$ всюду плотен в $\mathbb{R}$ для любого отрезка $I \subset \mathbb{R}$;

д) график функции $f(x)$ всюду плотен в $\mathbb{R}^2$.

Ответы, указания, решения

Листок 7,25

Задача 7,25.1. Решение. а) $xyx^{-1}y^{-1} = e$, $xyx^{-1} = y$, $xy = yx$. б) $(xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x]$.

Задача 7,25.2. Решение. $g[xy]g^{-1} = gxyx^{-1}y^{-1}g^{-1} = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} = [gxg^{-1}, gyg^{-1}]$.

Задача 7,25.3. Решение. $g \in G' \Rightarrow \varphi(g) \in H'$. Обратно: если $h \in H'$, то $h = h_1h_2h_1^{-1}h_2^{-1}$, $h_i = \varphi(g_i) \Rightarrow h = \varphi([g_1, g_2])$.

Задача 7,25.4. Решение. Возьмем любой коммутатор $[a, b]$ и посмотрим, в каком он классе смежности: $\overline{[a, b]} = \overline{a}\overline{b}\overline{a^{-1}b^{-1}} = \overline{e}$, т.к. G/H абелева. $[a, b] \in H \Rightarrow G' \in H$.

Задача 7,25.5. Решение. Пусть $g \in G$, $h \in H$. $ghg^{-1} = (ghg^{-1}h^{-1})h = [g, h]h \in H$, поскольку $[g, h] \in G'$, значит, $H \lhd G$. $[\overline{g_1}, \overline{g_2}] = \overline{g_1 \cdot g_2 \cdot g_1^{-1} \cdot g_2^{-1}} = \overline{[g_1, g_2]} = \overline{e}$, значит, G/H абелева.

Задача 7,25.6. Решение. $(ij)(jk) = (ijk)$ — зависимая пара транспозиций. $(ij)(kl) = (ij)(jk)(jk)(kl) = (ikj)(ilk)$ — независимая пара транспозиций. Получаем, что A_n порождается тройными циклами $(ijk) = (ikj)(ikj) = (ij)(jk)(ij)(jk) = (ij)(lm)(jk)(lm)(ij)(lm)(jk)(lm) = [(ij)(lm), (jk)(lm)]$ — когда $n > 4$, A_n порождается произведениями пар независимых транспозиций.

Задача 7,25.7. Решение. $S_n' \subset A_n$ — очевидно (коммутатор —- четная перестановка). $A_n \subset S_n'$, т.к. $(ijk) = [(ij), (jk)]$.

Задача 7,25.8. Решение. $A_4 : e$; (12)(34), (13)(24), (14)(32) — все эти произведения коммутируют между собой. (123) (132); (124) (142); (134) (143); (234) (243) — это все тройные циклы A_4, которые ее порождают. $[(ijk), (ijl)] = (ijk)(ijl)(ikj)(ilj) = (ij)(kl)$. $[(ijk), (ij)(kl)] = (il)(kj)$.

Задача 7,25.9. Решение. Любой тройной цикл является коммутатором, если $n > 4$, то элементов хватит: $(ijk) = [(ij)(lm), (jk)(lm)]$. Так что A_n порождается тройными циклами, поэтому $A_n' = A_n$.

Задача 7,25.10. Решение. $H \subset G \Rightarrow H' \subset G'$

Задача 7,25.11. Решение. $\varphi : G \to G/H$ — эпиморфизм. По задаче 3 $\varphi(G') = (G/H)'$.

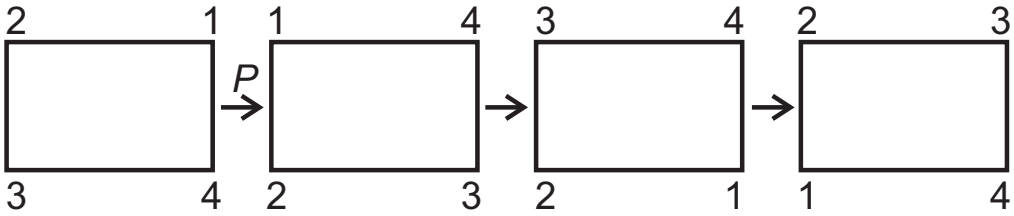
Задача 7,25.12. Решение. G/H разрешима, поэтому $(G/H)^{(k)} = \overline{e}$, значит, $(G)^k \subset H$. H разрешима, поэтому $H^{(l)} = e$, значит, $G^{(k+l)} = e$.

Задача 7,25.13. Решение. Докажем, что коммутант нормальной подгруппы нормален во всей группе. $H \lhd G$. H' порожден $[h_1, h_2]$. Покажем, что $g[h_1, h_2]g^{-1} \in H'$. $g[h_1, h_2]g^{-1} = gh_1h_2h_1^{-1}h_2^{-1}g^{-1} = gh_1g^{-1}gh_2g^{-1}gh_1^{-1}g^{-1}gh_2^{-1}g^{-1} = (gh_1g^{-1})(gh_2g^{-1})(gh_1g^{-1})^{-1}(gh_2g^{-1})^{-1} = [gh_1g^{-1}, gh_2g^{-1}] = [\tilde{h_1}, \tilde{h_2}]$. Тогда $\forall h \in H'$ $ghg^{-1} \in H'$. (Если $h_1, h_2 \in H'$, то $gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = \tilde{h_1}\tilde{h_2} \in H'$.) $G' \lhd G \Rightarrow G^{(k)} \lhd G$ $\forall k$.

Задача 7,25.14. Решение. Группа D_4 содержит 8 элементов: id, две осевые симметрии через середины сторон, две осевые симметрии относительно диагоналей, повороты на $\pm 90°$.

а) C — подгруппа, порожденная центральной симметрией; $C \lhd D_4$, так как $C^* = D_4'$, см. решение 7,25.15 в).

б) D_1 порождена симметрией относительно диагонали. Тогда D_1 не является нормальной подгруппой D_4: если d_1 — симметрия, а p — поворот на $90°$, то pd_1p^{-1} — симметрия относительно другой диагонали.



в) $D_2 \lhd D_4$.

г) $D_1 \lhd D_2$.

Задача 7,25.15. Решение. а) $G = Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, $i^2 = j^2 = k^2 = -1$, $ij = k, jk = i, ki = j$.

Чему равно $[g_1, g_2]$? Если хотя бы один из g_1, g_2 равен ± 1, то $[g_1, g_2] = 1$, так как ± 1 со всеми коммутируют.

Если оба отличны от ± 1, то $g_i^{-1} = g_i$ и $[g_1, g_2] = g_1 g_2 (-g_1)(-g_2) = g_1 g_2 g_1 g_2 = (g_1 g_2)^2 = \pm 1$. $(Q_8)' = \{1, -1\}$.

(*) Заметим, что $G/G' = \mathbb{Z}_2 \oplus \mathbb{Z}_2$, так как она порядка 4 и все квадраты элементов группы единичны.

б) D_3 некоммутативна, $(D_3)' \neq e$. Любой коммутатор сохраняет ориентацию, поэтому в $(D_3)'$ только повороты.

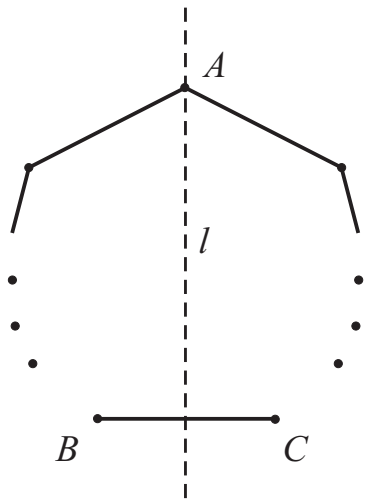
в) D_4 некоммутативна, $(D_4)' \neq e$. Любой коммутатор сохраняет ориентацию, поэтому в $(D_4)'$ могут быть повороты на $\pm 90^\circ$ и центральная симметрия.

Любой элемент $g \in D_4$ либо меняет диагонали (вместе с g^{-1}), либо оставляет их на месте, поэтому коммутатор оставляет их на месте, значит, $(D_4)' = \{e,$ центральная симметрия$\}$.

В этом случае годится также рассуждение (*).

г) D_n некоммутативна, $(D_n)' \neq e$. Коммутатор сохраняет ориентацию, поэтому в коммутаторе содержатся только вращения. Какие?

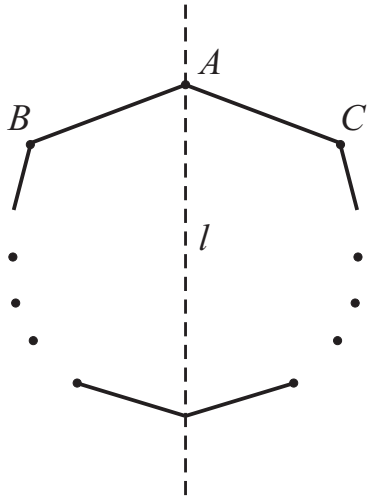
1) n нечетно, $n = 2k + 1$.



Пусть a — отражение относительно оси l, b — поворот от A к B. Тогда $[a, b] = aba^{-1}b^{-1}$ — поворот от B к C. Значит, (D'_{2k+1}) — подгруппа поворотов.

2) n четно, $n = 2k$.

Построим два k-угольника, раскрасим вершины через одну. Коммутатор переводит каждый k-угольник в себя, поэтому остаются только повороты на углы, кратные $2\pi/k$.



Пусть a — отражение относительно l, b — поворот на $2\pi/n$. Тогда $[b,a] = bab^{-1}a^{-1}$ — поворот от C к B. Значит, $(D_{2k})'$ состоит из поворотов на углы, кратные $2\pi/k$.

В этом случае годится также рассуждение (*).

Задача 7,25.16. Решение. $Z \subset G$, Z — центр. $g \in G$, $z \in Z$, тогда $gzg^{-1} = gg^{-1}z = ez = z$.

Задача 7,25.17. Решение. G является объединением непересекающихся орбит при действии сопряжения: $G = \cup_i G_{a_i}$. $|G_{a_i}| = |G|/|St(a_i)|$. По теореме Лагранжа $|St(a_i)|$ делит $|G|$, поэтому $|St(a_i)| = p^{k_i}$. Среди орбит есть орбита длины 1 — орбита элемента e, но она не может быть единственной (если орбита имеет длину > 1, то эта длина делится на p).

Задача 7,25.18. Решение. $|G| = p^2$. Центр G нетривиален. По теореме Лагранжа $|Z| = p^2$ или $|Z| = p$.

1) $|Z| = p^2$, тогда G абелева.

2) $|Z| = p$, тогда $|G/Z| = p$, поэтому обе группы Z, G/Z — циклические. Тогда $\forall g \in G\ g = zb^k$, где $z \in Z$, b — образующий для G/Z. Тогда $g_1g_2 = z_1b^{k_1}z_2b^{k_2} = z_1z_2b^{k_1+k_2} = g_2g_1$.

Задача 7,25.19. Решение. Индукция по степени p. База: $|G| = p$, G — циклическая, поэтому G — абелева, значит $G' = e$, G — разрешима.

Пусть для $k < n$ группа G с $|G| = p^k$ разрешима. Возьмем группу G, $|G| = p^n$. Ее центр Z нетривиален.

Если $|Z| = p^n$, то G абелева.

Если $|Z| = p^m$, $0 < m < n$, то $|G/Z| = p^{n-m}$, $0 < n - m < n$. По предположению индукции Z и G/Z разрешимы, поэтому, по задаче 12, G разрешима.

Листок 7,5

Задача 7,5.6,5. Решение. От противного. Пусть $f(x) = h(x)g(x)$. По лемме Гаусса $h, g \in \mathbb{Z}[x]$. Перейдем к редукции по mod p: $\overline{a_0}x^sx^t = (\overline{b_0}x^s + \overline{b_1}x^{s-1} + ...)(\overline{c_0}x^t + \overline{c_1}x^{t-1} + ...)$, $s + t = n$. Легко понять, что $b_i = c = c_j$, где $i, j \geq 1$. Т.е. $b_i, c_j | p$, где $i, j \geq l$, поэтому $a_n = b_sc_t | p^2$. Противоречие. Можно принять во внимание факториальность $\mathbb{Z}_p[x]$: $\overline{a}x^n$ можно разложить только в произведение одночленов.

Задача 7,5.10. Решение. Группа $\mathbb{Z}/m\mathbb{Z}$ изоморфна группе корней из 1. $\mathbb{Z}/m\mathbb{Z}$ — конечная циклическая группа. Все ее подгруппы находятся в взаимно-однозначном соответствии с делителями m. Каждый корень принадлежит соответствующей подгруппе.

Задача 7,5.11. Решение. $\Phi_1(x) = x - 1$. Далее индукция по m, поскольку $x^m - 1 = \Phi_m(x) \prod\limits_{d|m, d\neq m} \Phi_d(x)$.

Листок 8

Задача 8.7. Указание. Если несколько целых чисел $b_1; b_2; ...; b_n$ попарно взаимно просты, то существует их линейная комбинация с целыми коэффициентами $k-i$; $i = 1; ...; n$, равная 1: $k_1b_1 + k_2b_2 + ... + k_nb_n = 1$.

Задача 8.8. Решение. Пусть элемент a — максимального порядка, $p^k a = 0$ и пусть B — максимальная по мощности подгруппа в A, такая что $B \cap \langle a\rangle = 0$. Рассмотрим $H = B \oplus \langle a\rangle$. Очевидно, что $H = \langle B, a\rangle$.

Предположим, что H — собственная подгруппа в A. Тогда возьмем $x \in A \setminus H$, такой что $px \in H$ (это сделать можно: возьмем любой $y \in A \setminus H$; для некоторого s выполнено $p^s y \in H$, выберем минимальное s и положим $x = p^{s-1}y$). Имеем: $px = b + la$, где $b \in B$, $l \in \mathbb{Z}$. Умножим это равенство на p^{k-1}. Так как элемент a имеет максимальный порядок p^k, то $p^k x = 0$. Получаем: $0 = p^{k-1}b + p^{k-1}la$, значит $p^{k-1}b \in B \cap \langle a\rangle$, следовательно, $p^{k-1}b = 0$ и $p^{k-1}la = 0$, откуда $l = pj$, $j \in \mathbb{Z}$.

Возьмем $z = x - ja$, тогда $pz = px - pja$. Но $z \notin H$, иначе $x \in H$. Значит, $\langle B, z\rangle \cap \langle a\rangle = \{0\}$ (поскольку B — максимальная по мощности подгруппа в A, такая что $B \cap \langle a\rangle = \{0\}$). Получается, что существует такое $ra \neq 0$, что $ra \in \langle B, z\rangle$, т.е. $ra = b' + tz$, $b' \in B$, $t \in \mathbb{Z}$. Тогда $tz \in B \oplus \langle a\rangle = H$.

Если p делит t, то $tz \in B$ (так как $pz = px - la = b$), но тогда $ra \in B$, откуда $ra = 0$. Противоречие. Значит, $(p, t) = 1$ и найдутся $m \in \mathbb{Z}$ и $n \in \mathbb{Z}$, такие что $mp + nt = 1$. Но тогда $z = mpz + ntz \in H$ (так как $pz = px - pja \in H$ и $tz \in H$). Противоречие. Получается, что $H = B \oplus \langle a\rangle = A$.

Задача 8.9. Указание. Ввиду задачи 8.7 утверждение достаточно доказать для p-групп. Единственность для p-групп доказывается индукцией по порядку группы. Умножение на p позволит сделать шаг индукции. Дальше надо вспомнить, что порядок группы равен произведению порядков ее прямых слагаемых. Тем самым восстанавливается количество слагаемых, аннулированных умножением на p.

Задача 8.11 б). Указание. Утверждение достаточно доказать для p-групп, т.к. все примарные компоненты инвариантны и любая подгруппа будет раскладываться в прямую сумму подгрупп примарных компонент. По задаче 8.9 примарная p-группа раскладывается на примарные циклические. А у каждой циклической p-группы всегда есть подгруппа, делящая ее порядок. Значит, необходимое количество прямых слагаемых, чтобы получить нужный порядок p-компоненты, мы всегда найдем.

Задача 8.14. Решение. По очевидной задаче 8.13 группа порядка n циклическая титтк $\mathrm{HOK}(\mathrm{ord}(g_1), ..., \mathrm{ord}(g_n)) = n$, где $g_i \in G$. Докажем 8.14 сначала для p-групп, тогда утверждение будет очевидно для любого порядка n. По 8.9 имеем $G = \sum\limits_{i=1}^{n} \oplus \mathbb{Z}/p^{k_i}\mathbb{Z}$, поэтому $\forall g \in G$ $\mathrm{ord}\, g = p^{k_s}$, где $k_s = \max(k_1, ..., k_n)$. Тогда $\forall g \in G$ g — корень уравнения $x^{k_s} - 1 = 0$, поэтому по теореме Безу $|G| \leq p^{k_s}$. Но $|G| = \prod\limits_{i=1}^{n} p^{k_i}$, поэтому $n = 1$, а значит, $G \cong \mathbb{Z}/p^k\mathbb{Z}$. Если $|G| = n$, где $n = p_1^{k_1} \cdot ... \cdot p_n^{k_n}$, то $G = \sum\limits_{i=1}^{n} \oplus \mathbb{Z}/p^{k_i}\mathbb{Z}$ и, очевидно, циклическая.

Листок 8,5

Задача 8,5.15 Решение. Будем говорить, что многочлен $f(x)$ *аннулирует* a, если $f(a) = 0$. По определению, любой многочлен из I_a аннулирует a. Если мы умножим его на произвольный многочлен из $P[x]$, произведение также аннулирует a и значит, принадлежит I_a, поэтому I_a — идеал.

Известно, что идеал I_a порождается принадлежащим ему многочленом μ минимальной степени, т.е. μ делит любой другой многочлен из идеала.

Заметим, что μ неприводим, иначе мы бы нашли порождающий многочлен меньшей степени, чем μ.

Листок 9

Задача 9.1.б) Решение. Очевидно, что P — это фактор-кольцо $\mathbb{Q}[x]/(f)$. Так как f неприводим, то для любого такого g, что f не делит g, имеем $(f,g)=1$. Тогда найдутся такие u,v, что $uf+vg=1$. Это значит, что в фактор-кольце любой ненулевой элемент обратим, поэтому P — поле.

Задача 9.1.в) Решение. Определим отображение $\mathbb{Q}[x] \to \mathbb{Q}(\alpha) : p(x) \mapsto p(\alpha)$, где $p(x)$ — произвольный многочлен из $\mathbb{Q}[x]$. Теперь решение задачи построим в виде достаточно простых последовательных утверждений, каждое из которых нетрудно проверить самостоятельно.

- Это отображение — гомоморфизм.

- Его образ совпадает с $\mathbb{Q}(\alpha)$ (т.е. это эпиморфизм).

- Его ядро есть идеал (f) в $\mathbb{Q}[x]$, порожденный многочленом $f(x)$, т.е. множество многочленов вида $p(x)f(x)$, где $p(x)$ — произвольный многочлен из $\mathbb{Q}[x]$.

- Фактор $\mathbb{Q}[x]/(f)$ изоморфен полю P по построению P.

- С другой стороны, $\mathbb{Q}[x]/(f)$ изоморфен образу при этом гомоморфизме — $\mathbb{Q}(\alpha)$ — по теореме о гомоморфизме для полей (аналогичной соответствующей теореме для групп).

- В итоге P изоморфно $\mathbb{Q}(\alpha)$.

Задача 9.4. Решение. а) Степень 2, базис $\{1,i\}$. б) Степень бесконечна, базис содержит континуум элементов из соображений мощности. (Такой базис — так называемый *базис Гамеля* — существует по лемме Цорна, см. листок 18, после определения 18.6.) в) Степень 3, базис $\{1,a,a^2\}$ по построению фактор-кольца.

Задача 9.5. Решение. Пусть $[L:K]=n$, $\{a_1,...,a_n\}$ — базис расширения L/K. Тогда $L=K(a_1,...,a_n)$.

Задача 9.6. Указания. а) Умножение определяется по модулю $f(x)$.

б) Строим отображение из $K[x]$ в $K_f[x]$: многочлену сопоставляем его остаток от деления на $f(x)$. Проверьте, что это эпиморфизм, ядро которого есть (f). Тогда утверждение следует из теоремы о гомоморфизме для колец.

в) Размерность равна n, базис $1,x,...,x^{n-1}$.

г) Если f приводим, то в $K[x]/f$ есть делители нуля и это не поле. Пусть f неприводим, тогда делаем так же как в задаче 9.1. б) (в следующем решении напишем это подробно).

Задача 9.7. Решение. Сначала дадим независимое решение. Положим $L=F(\alpha)$, где α — формальный корень многочлена $f(x)$. Это значит, что мы рассматриваем множество выражений вида $a_0+a_1\alpha+a_2\alpha^2+...+a_{n-1}\alpha^{n-1}$, где $a_i\in F$, причем $f(\alpha)=0$. Чтобы ввести операции сложения и умножения, удобно посмотреть на эти выражения как на многочлены от переменной α. Тогда сложение определим как обычное сложение многочленов, а умножение как умножение многочленов по модулю $f(\alpha)$. Нетрудно проверить, что получилось коммутативное кольцо с единицей. Теперь рассмотрим ненулевой элемент $g(\alpha)\in F(\alpha)$. В $F[x]$ ему соответствует многочлен $g(x)$. Его степень меньше, чем у $f(x)$, а $f(x)$ неприводим, значит, они взаимно просты. Тогда существуют такие $u(x),v(x)\in F[x]$, что $v(x)g(x)+u(x)f(x)=1$, $\deg v(x)<\deg g(x)$, $\deg u(x)<\deg f(x)$. Возвращаемся в $F(\alpha)$ и получаем: $v(\alpha)g(\alpha)+u(\alpha)f(\alpha)=1$. Тогда $v(\alpha)g(\alpha)=1$, так как $f(\alpha)=0$. Значит, у $g(\alpha)$ есть обратный элемент и $F(\alpha)$ — поле, в котором f имеет корень α.

Теперь заметим, что мы воспроизвели конструкцию задачи 9.6, только заменили букву K на F. Поэтому ответ можно было дать сразу: f имеет корень в поле $F[x]/(f)$ (естественное вложение поля F в L имеет вид $x\mapsto x+(f)$).

Задача 9.10. Решение. Возьмем многочлен μ из решения задачи 8,5.15. Поделим его на ненулевой старший коэффициент и получим единственный минимальный многочлен элемента a.

Задача 9.11. Ответы, указания. а) x^2-2; б) x^7-5, оба пункта — по критерию Эйзенштейна 7,5.6,5. в) $x^{105}-9$, критерий Эйзенштейна не работает, разложить на линейные множители в $\mathbb{C}$. Нужно посмотреть на модуль свободного члена. Он должен быть рациональным. Корень 105-й степени из девяти только в 105-й степени будет рациональным.; г) $x^2-4x+13$; д) $z-(2-3i)$.

Задача 9.12. Решение. $K \subset L$, $[L : K] = n$, $a \in L$ тогда $1, a, a^2, ..., a^n$ линейно зависимы, поэтому существует $f(x) \in K[x]$, такой что $f(a) = 0$. Значит, a алгебраичен.

Задача 9.13. Указание. Обозначим F/K — линейное пространство F над полем K, аналогично E/F. Пусть $\{a_1, ...a_n\}$ — базис в F/K, $\{b_1, ...b_m\}$ — базис в E/F. Проверьте, что $\{a_i \cdot b_j\}$, $i = 1, ...n$, $j = 1, ...m$ — базис в E/K.

Задача 9.14. Решение. Если бы для какого-то i было $[F_{i+1} : F_i] = \infty$, тем более было бы $[F_n : F_1] = \infty$, так как в F_n можно построить бесконечную цепочку линейно независимых векторов над F_i, а значит, и над F_1. В обратную сторону — по теореме о башне полей 9.12.

Задача 9.15. Указание. Воспользуйтесь 9.6 и гомоморфизмом эвалюции $f(x) \mapsto f(a)$. Элементы $1, a, a^2, ..., a^{n-1}$, очевидно, образуют базис (если бы они были линейно зависимыми, мы бы нашли аннулирующий многочлен степени, меньшей n).

Задача 9.16. Решение. $E = K(a_1, ...a_n) = K(a_1)(a_2)...(a_n)$ по 8,5.14 б). Каждое простое алгебраическое расширение конечномерно, так как если элемент a_k алгебраичен над K, то он алгебраичен и над бóльшим полем $F \supset K$. Тогда по теореме о башне полей расширение $K \subset E$ конечно и значит, алгебраично.

Задача 9.17. Решение. Пусть $a \in E$. Расширение $F \subset E$ алгебраично, поэтому есть такой многочлен $\mu(x) = t_n x^n + t_{n-1} x^{n-1} + ... + t_1 x + t_0$, что $t_i \in F$ и $\mu(a) = 0$. t_i алгебраичны над K, поэтому a алгебраичен над $K(t_0, ..., t_n)$.

Размерность $[K(t_0, ..., t_n) : K]$ конечна по задаче 9.16, размерность $[K(a, t_0, ..., t_n) : K(t_0, ..., t_n)]$ также конечна, поэтому размерность $[K(a, t_0, ..., t_n) : K]$ конечна по теореме о башне полей. Значит, a алгебраичен над K.

Задача 9.18. Решение. Пусть $F \subset D$, где D — алгебраически замкнутое поле; такое есть по теореме Штейница. Положим $\overline{F} = \{a \in D : \ a$алгебраичен над $D\}$.

Докажем, что $\overline{F}$ — поле. Пусть $\alpha, \beta \in \overline{F}$, т.е. они алгебраичны. Тогда по 9.16 вложение $F \subset F(\alpha, \beta)$ — алгебраическое, поэтому $\alpha \pm \beta, \alpha \cdot \beta, \alpha/\beta \in F(\alpha, \beta) \subset \overline{F}$, значит $\overline{F}$ — поле.

Докажем, что $\overline{F}$ алгебраически замкнуто. Пусть $f(x) \in \overline{F}[x]$ и $a \in D$ — его корень. Докажем, что $a \in \overline{F}$. Пусть $c_0, ..., c_k$ — коэффициенты $f(x)$. Тогда a алгебраичен над $F(c_0, ..., c_k)$. Из задач 9.16 и 9.17 следует, что a алгебраичен над F. Итак, $\overline{F}$ алгебраически замкнуто.

Задача 9.19. Решение. Допустим, напротив, что $[\overline{\mathbb{Q}} : \mathbb{Q}] = n$. Пусть p не делит n. Рассмотрим многочлен $x^p - 2$. Он неприводим по критерию Эйзенштейна. Присоединим его корень: $\mathbb{Q} \subset \mathbb{Q}(\sqrt[p]{2}) \subset \overline{\mathbb{Q}}$. По теореме о башне полей $p|n$ — противоречие.

Листок 10

Задача 10.1. Решение. Пусть $\deg h = n$. Любой элемент $P(\alpha)$ имеет вид $t = a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0$, $a_i \in P$. При действии на него гомоморфизмом ψ получим $\psi(t) = \psi(a_{n-1})\psi(\alpha)^{n-1} + ... + \psi(a_1)\psi(\alpha) + \psi(a_0) = \varphi(a_{n-1})\psi(\alpha)^{n-1} + ... + \varphi(a_1)\psi(\alpha) + \varphi(a_0)$, так как ψ и φ совпадают на P. Поэтому гомоморфизм ψ определяется значением $\psi(\alpha)$.

Теперь заметим, что, поскольку $h(\alpha) = 0$, то $h^\varphi(\psi(\alpha)) = 0$. Значит, $\psi(\alpha)$ — один из корней многочлена h^φ.

Обратно, если мы возьмем в F любой корень β многочлена h^φ и определим ψ на $P(\alpha)$ формулой $\psi(t) = \varphi(a_{n-1})\beta^{n-1} + ... + \varphi(a_1)\beta + \varphi(a_0)$, то получим гомоморфизм ψ, который на P совпадает с φ — проверьте.

По разным корням β_i получатся разные гомоморфизмы, так как значения $\psi(\alpha)$ будут разные.

Итак, способов продолжения ровно столько, сколько корней h^φ в F.

Задача 10.2. Решение. Построим башню расширений $L_0 \subset L_1 \subset L_2 \subset ...L_i \subset L_{i+1} \subset ...$, где $L_0 = K$, $L_i = K(a_1, ..., a_i)$, так что на каждом шаге $f(x) = (x - a_1) \cdot ... \cdot (x - a_i) f_i(x)$ над L_i. Применим индукцию по i.

База: $L_0 = K$, $f_0 = f$.

Шаг индукции. Если f_i разлагается на линейные множители над L_i, то построение закончено. Иначе $f_i = p_i q_i$, где p_i неприводим над L_i, $\deg p_i > 1$. Присоединим корень многочлена p_i, т.е. положим $L_{i+1} = L_i(a_{i+1})$, где $p_i(a_{i+1}) = 0$. Так за конечное число шагов мы получим минимальное поле, содержащее все корни многочлена f (минимальное, поскольку мы присоединяли только корни), т.е. поле разложения f.

Докажем единственность. Идея доказательства достаточно проста. Поле разложения должно содержать $L_n = K(a_1, ..., a_n)$. Неединственность может возникнуть от того, что корни могут быть присоединены в другом порядке. Тогда изоморфизмом фактически является перестановка корней.

Теперь дадим формальное доказательство. Пусть $\tilde{F}$ — другое поле разложения, $F = K(a_1, ..., a_n)$, $K = L_0 \subset L_1 \subset L_2 \subset ...L_i \subset L_{i+1} \subset ... \subset F$ — построенное нами поле. Рассмотрим $\varphi_0 = Id$ — тождественное вложение K в $\tilde{F}$. По задаче 10.1 продолжим φ_0 на L_1, затем на L_2 и т.д. по индукции.

Пусть уже построено $\varphi_i : L_i \to \tilde{L}_i \subset \tilde{F}$, $a \to \varphi_i(a) = \tilde{a}$. Тогда по индуцированному гомоморфизму $\forall\ g(x) \in L_i[x]$ получаем продолжение $g^{\varphi_i}(x) \in \tilde{L}_i[x]$. Над L_i имеем $f(x) = (x - a_1) \cdot ... \cdot (x - a_i) f_i(x)$, $f_i = p_i q_i$, где p_i неприводим над L_i, $\deg p_i > 1$. Так как L_i и $\tilde{L}_i$ изоморфны, $f_i^{\varphi_i} = p_i^{\varphi_i} q_i^{\varphi_i}$ и $\tilde{p_i} = p_i^{\varphi_i}$ неприводим над $\tilde{L}_i$.

Но $\tilde{F}$ — поле разложения f, поэтому $\exists\, \tilde{a_{i+1}} \in \tilde{F}$, такое что $\tilde{p_i}(\tilde{a_{i+1}}) = 0$. Присоединим $\tilde{a_{i+1}}$ к $\tilde{L}_i$ и положим $\tilde{L}_{i+1} = \tilde{L}_i(\tilde{a}_{i+1})$. По задаче 10.1 $\tilde{L}_i(\tilde{a_{i+1}}) \cong L_i(a_{i+1})$, где a_{i+1} — корень p_i. Так как продолжение гомоморфизма всегда мономорфизм и, очевидно, эпиморфизм, то расширения поля, получаемые присоединением корня данного неприводимого многочлена, изоморфны друг другу. Поскольку $L_i(a_{i+1}) = L_{i+1}$, мы построили изоморфизм $\varphi_{i+1} : L_{i+1} \to \tilde{L}_{i+1}$ и в итоге построим вложение $\varphi : F \to \tilde{F}$. Заметим, что в $\operatorname{Im}\varphi$ многочлен f разлагается на линейные множители по построению, а поле F — минимальное с таким свойством. Значит, $\operatorname{Im}\varphi = \tilde{F}$ и $\varphi : F \to \tilde{F}$ — изоморфизм.

Задача 10.3. Решение. Определим отображение $\varphi : P(\alpha) \to P(\beta)$ формулой $\varphi(a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0) = a_{n-1}\beta^{n-1} + ... + a_1\beta + a_0$. Нетрудно проверить, что это изоморфизм, воспользуйтесь задачей 9.15.

Задача 10.4. Ответы. а) 1; б) 2; в) 2; г) 6; д) 8; е) $p - 1$; ж) $\varphi(n)$ — значение функции Эйлера; з) $p(p - 1)$.

Задача 10.5. Ответы. а) Один класс $\{\pm\sqrt[4]{2}; \pm i\sqrt[4]{2}\}$; б) Два класса $\{\pm\sqrt[4]{2}\}$; $\{\pm i\sqrt[4]{2}\}$; в) Три класса $\{\sqrt[4]{2}\}$; $\{-\sqrt[4]{2}\}$; $\{\pm i\sqrt[4]{2}\}$; г) 4 класса $\{\sqrt[4]{2}\}$; $\{-\sqrt[4]{2}\}$; $\{i\sqrt[4]{2}\}$ $\{-i\sqrt[4]{2}\}$.

Задача 10.7. Решение. Пусть $P \subset F$ — конечное нормальное расширение. Тогда $F = P(a_1, ..., a_n)$ конечно порождено, где все a_i алгебраичны над P, т.е. $\forall\ a_i\ \exists\ \mu_{a_i}(x) \in P[x]$ — аннулирующий a_i многочлен над P. Так как расширение $P \subset F$ нормально, $\forall\ i\ \mu_{a_i}(x)$ раскладывается на линейные множители, поэтому $f = \prod_{i=1}^{n} \mu_{a_i}(x)$ тоже раскладывается на линейные множители. Очевидно, что тогда F есть поле разложения для f.

Обратно, пусть существует $f(x) \in P[x]$, для которого F есть поле разложения. Рассмотрим $p(x) \in P[x]$, такой что p не делит f, p неприводим и p имеет корень α в F. Пусть β — любой другой корень p (он может лежать, например, в алгебраическом замыкании $\overline{P}$ поля P). Нам надо доказать, что $\beta \in F$, это и будет означать нормальность расширения $P \subset F$.

По задачам 10.1 и 10.3 поля $P(\alpha)$ и $P(\beta)$ изоморфны, т.е. тождественное отображение $P \to P$ продолжается до изоморфизма $\psi : P(\alpha) \to P(\beta)$, $\psi(\alpha) = \beta$. Рассмотрим $F(\beta) \subset \overline{P}$. Очевидно, что $F(\alpha)$ — поле разложения f над $P(\alpha)$. Аналогично, $F(\beta)$ — поле разложения f над $P(\beta)$. Так как поля разложения изоморфны, мы можем продолжить ψ до $\gamma : F \to F(\beta)$.

Изоморфизм полей является также изоморфизмом векторных пространств, поэтому размерности $\dim F$ и $\dim F(\beta)$ над полем P равны. Если бы было $\deg \mu_\beta^F(x) > 1$, то пришли бы к противоречию с теоремой о размерности башни, значит, $\deg \mu_\beta^F(x) = 1$, т.е. $\beta \in F$.

Задача 10.8. Ответ. Расширение нормально $\Longleftrightarrow$ оно получается присоединением всех корней

некоторого множества многочленов (конечное расширение — присоединением корней некоторого конечного множества многочленов).

Задача 10.9. Решение. Пусть $a \in L$, $\mu_a^F \in F[x]$. По условию μ_a^P раскладывается на линейные множители в $L[x]$, $\mu_a^F | \mu_a^P$, так как μ_a^F — минимальный, а μ_a^P — аннулирующий. Но в $L[x]$ разложение на множители однозначно, поэтому μ_a^F тоже раскладывается на линейные множители.

Задача 10.10. Решение. а) Нет минимальных многочленов степени больше 2. По теореме о башне полей, если $\mu_a(a) = 0$, то $x - a$ делит μ_a, поэтому μ_a раскладывается на линейные множители.

б) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}\sqrt{\sqrt{2}}$. Но многочлен $x^4 - 2$ неприводим и не распадается на линейные множители, комплексных корней не хватает.

Задача 10.11. Решение. $[P : \mathbb{Z}_p] < \infty$, разложение элементов по базису однозначно.

Задача 10.12. Решение. $(xy)^p = x^p y^p$. $(x+y)^p = x^p + y^p + \sum\limits_{k=1}^{p-1} C_p^k x^k y^{n-k}$, но $C_p^k = p!/k!(p-k)!$. Числитель делится на p, а в знаменателе p не встречается, поэтому p делит C_p^k при $k = 1, ..., p-1$, а тогда $(x+y)^p = x^p + y^p$. Гомоморфизм полей всегда инъективен, а в силу конечности и сюръективен, поэтому Φ — автоморфизм.

Задача 10.13. Решение. Докажем существование. Пусть $f(x) = x^q - x$, где $q = p^n$, $f \in \mathbb{Z}_p[x]$. Возьмем $L = \mathbb{Z}_p(f)$ и рассмотрим F — множество корней f в L, т.е. $F \subset L$. Так как Φ — гомоморфизм, то F — подполе. Действительно, $a \in F \Leftrightarrow a^q = a \Leftrightarrow \Phi^n(a) = a$. Значит, F содержит все корни $f(x)$, т.е. f в F разлагается на линейные множители. Но других элементов F не содержит, поэтому, в силу минимальности поля разложения, $F = L$.

$f'(x) = qx^{q-1} - 1 = -1 \Rightarrow (f, f') = 1 \Rightarrow$ у f нет кратных корней, поэтому f имеет q корней, и тогда $|F| = |L| = q$.

Докажем единственность. Пусть $|F| = p^n$, $q = p^n \Rightarrow$ $\operatorname{char} F = p \Rightarrow \mathbb{Z}_p \subset F$, $|F^*| = q - 1$, где $F^* = F \setminus \{0\} \Rightarrow$ по теореме Лагранжа $\forall\, a \in F^*\ a^{q-1} = 1 \Rightarrow \forall\, a \in F\ a^q - a = 0$. Рассмотрим $f(x) = x^q - x \in \mathbb{Z}_p[x]$. Он имеет q различных корней, все — элементы поля F и его степень равна q. Поэтому $f(x)$ раскладывается на q линейных множителей: $f(x) = \prod\limits_{a_i \in F} (x - a_i)$. Значит, F — поле разложения f над $\mathbb{Z}_p$. Поле разложения единственно с точностью до изоморфизма по 10.2.

Задача 10.14. Решение. Рассмотрим $(GF(p^n))^*$. Это циклическая группа по умножению, т.е. $(GF(p^n))^* = \langle a \rangle$. Тогда $GF(p^n) = \mathbb{Z}_p[a] \cong \mathbb{Z}_p[x]/\mu_a(x)$. Но μ_a неприводим и $\deg \mu_a = n$ по 9.15.

Задача 10.15. Решение. а) Ищем неприводимый многочлен 4-й степени над $\mathbb{Z}_2$. Он не должен иметь корней и не должен быть квадратом $x^2 + x + 1$ — единственного неприводимого над $\mathbb{Z}_2$ квадратного трехчлена. Например, подходит $x^4 + x + 1$. Тогда $GF(16) \cong \mathbb{Z}_2[x]/(x^4 + x + 1) \cong F_2[a]$, где $a^4 + a + 1 = 0$. Найдем образующий мультипликативной группы поля. $|GF(16)^*| = 15$, поэтому у образующего не может быть порядок 3 или 5. Заметим, что $a^3 \neq 1$, так как $\deg \mu_a = 4$; $a^5 = a^4 a = (a+1)a \neq 1$ из тех же соображений, поэтому a — образующий, а значит, все остальные образующие — это a^k, где $(k, 15) = 1$. Перечислим их: a^2, $a^4 = a + 1$, $a^7 = a^3 a^4 = a^3(a+1) = a^4 + a^3 = a^3 + a + 1$, $a^8 = (a^4)^2 = (a+1)^2 = a^2 + 1$, $a^{11} = a^8 a^3 = (a^2+1)a^3 = aa^4 + a^3 = a(a+1) + a^3 = a^3 + a^2 + a$, $a^{13} = a^{11}a^2 = (a^3 + a^2 + a)a^2 = a^5 + a^4 + a^3 = (a+1)^2 + a^3 = a^3 + a^2 + 1$, $a^{14} = a^{13}a = (a^3 + a^2 + 1)a = a^4 + a^3 + a = a^3 + 1$.

б) Ищем многочлен 3-й степени над $GF(3)$ без корней, например, $x^3 - x - 1$. Тогда $GF(27) \cong GF(3)[x]/(x^3 - x - 1)$. Пусть a — корень. $|GF(27)^*| = 26$, поэтому порядок образующего не равен $2, 13$. $a^{13} = (a^3)^4 a = (a+1)^4 a = (a+1)^3(a+1)a = (a^3+1)(a+1)a = (a-1)(a+1)a = (a^2-a)a = a^3 - a = 1$. Заметим, что $GF(27)^* \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{13} \cong \langle -1 \rangle \oplus \langle a \rangle$. Значит, $-a$ порождает $GF(27)^*$. Все образующие суть $(-a)^k$, где $(k, 26) = 1$. Их количество равно $\varphi(26) = 12$. Также заметим, что $GF(27) = \mathbb{Z}_3(a)$, т.е. a — примитивный, но не порождающий мультипликативную группу поля $GF(27)$.

в) Если бы $GF(16) \subset GF(64)$, то $GF(64)$ было бы линейным пространством над $GF(16)$ и должно было бы быть $64 = 16^k$, а это неверно.

г) $GF(p^n) \subset GF(p^m)$ титтк $n|m$, причем в этом случае такое подполе существует и единственно. Поэтому $GF(2) \subset GF(4) \subset GF(1024)$ — одна цепочка и $GF(2) \subset GF(32) \subset GF(1024)$ — вторая, так как у $1024 = 2^{10}$, а у 10 только два собственных делителя. Рассуждения можно также основывать на теории линейных пространств.

Задача 10.16. Решение. Как мы знаем из предыдущего (10.13), все элементы $GF(p^n)$ — корни $f(x)$, где $f(x) = x^{p^n} - x$ или $f(x) = x^q - x$, $q = p^n$. $f'(x) = -1$, поэтому кратных корней нет. По 10.12 Φ — автоморфизм, поэтому $\Phi^2, \Phi^3, ..., \Phi^{n-1}$ — автоморфизмы и $\Phi^n = id$ в силу уравнения $f(x) = 0$. Если бы было $\Phi^k = id$, где $k < n$, то для любого $x \in GF(p^n)$ было бы $x^{p^k} - x = 0$ и следовательно, по теореме Безу $|GF(p^n)| \leq p^k$, т.е. $n \leq k$. Противоречие. Значит, $|\langle\Phi\rangle| = n$.

По 10.14 существует такое a, что $(GF(p^n))^* = \langle a\rangle$, поэтому $GF(p^n) = \mathbb{Z}_p(a)$ и $\deg \mu_a = n$. Имеем $a^{p^n} - a = 0$. Очевидно, что $a, \Phi(a), ..., \Phi^{n-1}(a)$ — корни μ_a и все они различны. Для любого $\theta \in Aut(GF(p^n))$ $\theta(a)$ — корень μ_a и θ определен действием на a. $\mu_a|(x^{p^n} - x)$ по 8,5.15, следовательно, μ_a не имеет кратных корней. Но корень минимального многочлена при автоморфизме переходит в корень минимального многочлена, и автоморфизм полностью определяется действием на образующем. Значит всего автоморфизмов n и мы можем предъявить их все: $\Phi, \Phi^2, ..., \Phi^{n-1}, \Phi^n = id$, поэтому $Aut(GF(p^n)) = \langle\Phi\rangle$ и $\operatorname{ord}\Phi = n$. Одновременно мы доказали, что $\mu_a(x) = \prod\limits_{k=1}^{n}(x - a^{p^k})$, т.е. решена **Задача 10.17**.

Задача 10.18. Решение. а) $\Rightarrow$ $GF(p^n)$ — конечномерное линейное пространство над $GF(p^d)$, поэтому $(p^d)^k = p^n \Rightarrow dk = n \Rightarrow d|n$.

$\Leftarrow$ $n = kd$, $q = p^n$, $r = p^d$. Тогда $q = r^k \Rightarrow q-1 = r^k-1 = (r-1)(r^{k-1}+r^{k-2}+\ldots+r+1) = (r-1)s$. Рассмотрим $x^q - x = x(x^{q-1}-1) = x(x^{(r-1)s}-1) = x(x^{r-1}-1)(x^{(r-1)(s-1)} + x^{(r-1)(s-2)} + ... + x^{r-1} + 1) = (x^r - x)(x^{(r-1)(s-1)} + x^{(r-1)(s-2)} + ... + x^{r-1} + 1)$, т.е. $(x^r - x)|(x^q - x)$. Рассмотрим поле $F_q = GF(p^n)$. Оно является полем разложения многочлена $x^q - x$, но тогда F_q содержит и поле разложения F многочлена $x^r - x$. Но $F \cong F_r = GF(p^d)$, также F состоит из всех корней многочлена $x^r - x$, откуда следует единственность $F_r = GF(p^d)$. Другие элементы поля F_q не могут удовлетворять уравнению $x^r - x = 0$, так как многочлен $x^q - x$ не имеет кратных корней, а все элементы F_r должны удовлетворять уравнению $x^r - x = 0$, и $(x^r - x)|(x^q - x)$. Заметим, что $F_r = \{t \in F_q : \Phi^d(t) = t\}$ — множество всех элементов, остающихся на месте при действии $\langle\Phi^d\rangle$, т.е. поле инвариантов $\langle\Phi^d\rangle$. Мы знаем, что $G = Aut(F_q) = \langle\Phi\rangle$ и $|G| = n$, $\langle\Phi^d\rangle \subset G$, $d|n$. Пусть $\Phi^l \in T = Aut(F_q/F_r)$. Тогда $l = ud + v$. Пусть $F_r^* = \langle a\rangle$. a — это тот элемент F_r, для которого $F^d(a) = a$ и $\forall\, v$, $0 < v < d$, $\Phi^v(a) \neq a$, иначе a не образующий. Тогда $\Phi^l(a) = \Phi^{ud+v}(a) = \Phi^v(a) \neq 0$, поэтому $v = 0$, тогда $d|l$, следовательно, $Aut(F_q/F_r) = \langle\Phi^d\rangle$. Значит, решена и **Задача 10.18 б)**.

Задача 10.19. Решение. $\Leftarrow$ Из предыдущего известно (2.15): если G — абелева группа, $a, b \in G$, $\operatorname{ord} a = n$, $\operatorname{ord} b = m$, то существует такой элемент c, для которого $\operatorname{ord} c = HOK(m, n)$. Рассмотрим $t \in P^*$, для которого $\operatorname{ord} t = n$ максимален. Пусть $c \in P^*$, $\operatorname{ord} c = m$. Тогда существует $s \in P^*$, для которого $\operatorname{ord} s = HOK(m, n)$, но n — максимальный порядок, поэтому $m|n$. Тогда $x^n = 1\,\forall\, x \in P^*$, поэтому по теореме Безу $|P^*| \leq n$; так как P^* — поле, то t — образующий P^*.

$\Rightarrow$ Пусть $P^* = \langle a\rangle$, тогда $P^* \cong \mathbb{Z}/n\mathbb{Z}$ или $P^* \cong \mathbb{Z}$ по 4.10 в), г). Если $P^* \cong \mathbb{Z}/n\mathbb{Z}$, то P^* — конечное поле. Если $P^* \cong \mathbb{Z}$, то $P \supset Q(\mathbb{Z}) \cong \mathbb{Q}$ — поле частных, поэтому $P^* \subset \mathbb{Q}^*$. Но у циклических групп подгруппы циклические, а $\mathbb{Q}$ не циклическая.

Листок 11

Задача 11.1. (Лемма 1.) **Решение.** $K \subset L$ — конечнок расширение. Построим башню простых расширений $K = K_0 \subset K_1 \subset K_2 \subset ... \subset K_s = L$. Пусть $\varphi = \mathrm{Id} : K \to K$. Будем продолжать φ до автоморфизма $\tilde{\varphi} : L \to L$ по задаче 10.1. Каждый раз мы имеем не более n_i продолжений гомоморфизма K_i в L, где $n_i = [K_i : K_{i-1}]$. Значит, автоморфизмов не может быть больше, чем произведение n_1 по всем i от 1 до s. Но по теореме о башне полей это произведение как раз равно n. Поэтому общее число автоморфизмов не больше n.

Задача 11.2. а) **Ответ**: $\mathbb{Z}_2$; б) **Ответ**: Id; в) **Ответ**: $\langle \Phi^k \rangle$, см. задачу 10.18 б); г) **Ответ**: $\mathbb{Z}_2$; д) **Указание**: Легко видеть, что $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$, поэтому по лемме 11.1 автоморфизмов не более четырех. Четыре же есть: $\sqrt{2} \mapsto \pm\sqrt{2}$, $\sqrt{3} \mapsto \pm\sqrt{3}$. Получаем группу четвертого порядка, легко проверить, что она изоморфна $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. е) **Указание**: рассмотрите корни многочлена $x^4 - 2$. Это $\pm\sqrt[4]{2}$ и еще два комплексных. $\sqrt[4]{2}$ может перейти в $-\sqrt[4]{2}$ или в себя, поэтому получаем группу, изоморфную $\mathbb{Z}_2$. ж) Аналогично д). з) **Указание**: у многочлена $x^3 - 2$ два комплексных корня и один действительный — $\sqrt[3]{2}$. Он может перейти только в себя. **Ответ**: Id.

Задача 11.3. а) **Ответ**: $\mathbb{Z}_2$; б) **Указание**: Проверьте, что $\mathbb{Q}(x^3 - 2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$, где ω — первообразный корень степени 3 из единицы. Имеем: $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, поэтому $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] \geq 6$. Элементы $1, \omega, \sqrt[3]{2^2}, \omega\sqrt[3]{2}, \omega\sqrt[3]{2^2}, \sqrt[3]{2}$ порождают все поле разложения многочлена $x^3 - 2$ над $\mathbb{Q}$, поэтому $[\mathbb{Q}(x^3 - 2) : \mathbb{Q}] = 6$. Автоморфизм определяется своими значениями на ω и $\sqrt[3]{2}$, поэтому всего имеем 6 автоморфизмов. Проверьте, что наша группа не коммутативна, тогда это S_3, а не $\mathbb{Z}_6$. в) **Указание**: многочлен $x^4 + 4$ имеет корни $\pm 1 \pm i$, поэтому его поле разложения $\mathbb{Q}(i)$ и наша группа изоморфна $\mathbb{Z}_2$. г) **Указание**: поле разложения $\mathbb{Q}(\xi)$, где ξ — первообразный корень степени n из единицы. Проверьте, что группа $\mathrm{Aut}\,\mathbb{Q}(x^n - 1)$ имеет порядок $\varphi(n)$, φ — функция Эйлера, так как $\deg \Phi_n = \varphi(n)$. А наша группа изоморфна мультипликативной группе обратимых элементов $\mathbb{Z}/n\mathbb{Z}$, так как первообразный корень ξ может переходить при автоморфизме только в первообразный.

Задача 11.4. Ответы и указания: Из 11.2: а) — да; б) — нет, так как $[\mathbb{R} : \mathbb{Q}] = \infty$; в), г), д) — да; е) — нет; ж) — да; з) — нет. Из 11.3: а), б), в), г) — да.

Задачи 11.5., 11.6 — просто на применение соответствующих определений.

Задача 11.7. (Лемма 2.) **Решение.** Так как $G \subset G$, то по 11.5 и 11.6 г) имеем $G = \mathrm{Aut}(L/K) = \mathrm{Aut}(L/L^G)$ и $G \subset \mathrm{Aut}(L/L^G)$, а также $K \subset L^G \subset L$. По 11.1 $|G| \leq [L : L^G] \leq [L : K]$. Так как $|G| = n$, то все неравенства являются равенствами. Значит, по 9.13 (теорема о башне полей) $n = [L : K] = [l : L^G] \cdot [L^G : K] = n[L^G : K]$, поэтому $[L^G : K] = 1$, значит, $L^G = K$.

Задача 11.8. (Лемма 3.) **Решение.** По теореме Виета $\mu(x) = (x - a_1) \cdot ... \cdot (x - a_m) = x^m + C_1 x^{m-1} + ... + C_m$, где $C_k = (-1)^k \sigma_k(a_1, ..., a_m)$, σ_k — элементарный симметрический многочлен. Так как любой элемент $h \in H$ переставляет $a_1, ..., a_m$, то для любого k $\sigma_k(h(a_1), ..., h(a_m)) = h\sigma_k(a_1, ..., a_m) = \sigma_k(a_1, ..., a_m)$, поэтому $C_k \in L^H = K$. Пусть $f(x) \in K[x]$, $f(a) = 0$, т.е. $f(x)$ — аннулирующий a многочлен. Тогда для любого $h \in H$ имеем $h(f(a)) = f(h(a)) = 0$. Значит, $f(a_1) = f(a_2) = ... = f(a_m) = 0$, поэтому $\mu(x) | f(x)$, т.е. $\mu(x)$ — минимальный.

Задача 11.9. (Лемма 4.) **Решение.** Докажем от противного. Допустим, $V = V_1 \cup ... \cup V_k$. Если какое-то из подпространств лежит в объединении некоторых других подпространств, мы его удаляем. Эта процедура закончится за конечное число шагов, так как всего подпространств конечное число. Тогда в каждом из оставшихся подпространств V_i есть "уникальный" вектор $v_i \in V_i$, не принадлежащий ни одному из оставшихся подпространств. Рассмотрим набор векторов $v_1 + cv_2$, $c \in K$. Таких векторов бесконечно много, так как $|K| = \infty$. Но тогда, по принципу Дирихле, найдутся два разных вектора из этого набора, лежащих в одном подпространстве: $v_1 + cv_2 \in V_i$, $v_1 + c'v_2 \in V_i$, $c \neq c'$. Тогда $(c - c')v_2 \in V_i$, поэтому $v_2 \in V_i$, но тогда и $v_1 \in V_i$. Пришли к противоречию с уникальностью векторов v_1 и v_2.

Задача 11.10. (Лемма 5.) **Решение.** 1) Поймем, сколькими способами можно продолжить автоморфизм поля K до автоморфизма поля L. Построим башню простых расширений $K = K_0 \subset K_1 \subset ... \subset K_i = K_{i-1}(a_i) \subset ... \subset K_s = L$. По следствию из леммы 3 (11.8) для любого i минимальный многочлен $\mu_{a_i} \in K[x]$ имеет $\deg \mu_{a_i}$ различных корней в L. Рассмотрим μ_i — минимальный многочлен для a_i над K_{i-1}. Имеем: $\mu_i | \mu_{a_i}$, так как $\mu_{a_i}(a_i) = 0$, то у μ_i нет кратных корней и их количество равно $\deg \mu_i = n_i$. По задаче 10.1 существует n_i способов продолжить любой гомоморфизм $\varphi_{i-1} : K_{i-1} \to L$ до гомоморфизма $\varphi_i : K_i \to L$. Мы воспользовались тем, что $\mu_i, \mu_{a_i} \in K_{i-1}[x]$ и $\mu_i^{\varphi_{i-1}}, \mu_{a_i}^{\varphi_{i-1}} \in \varphi_{i-1}(K_{i-1})[x]$, а также $\mu_{a_i}^{\varphi_{i-1}} = \mu_{a_{i-1}}$, если $\varphi_{i-1}|_K = \mathrm{Id}$. Далее, $\varphi_{i-1}(K_i) \cong K_i$, значит,

число различных корней соответствующих многочленов над изоморфными полями остается неизменным, т.е. $\mu_i^{\varphi_{i-1}}$ имеет n_i различных корней. Значит, $|G| = n_1 n_2 \dots n_s = n$ по теореме о башне расширений.

2) Пусть $g \in G$. Тогда по лемме 3 (11.8) для любого $a \in L$ имеем $\mu_a(x) = (x - a_1) \cdot \ldots \cdot (x - a_n)$, где $\{a_1, \dots, a_n\} \in Ha$. $\mu_a(a) = 0$, поэтому $\mu_a(g(a)) = g(\mu_a(a)) = 0$, т.е. $g(a)$ — тоже корень μ_a, тогда $g(a) \in Ha = \{a_1, \dots, a_n\}$, значит, найдется $h \in H$, для которого $g(a) = h(a) \Leftrightarrow g^{-1}h(a) = a$. Так как $a \in L$ произвольное, то $L = \bigcup\limits_{h \in H} L^{g^{-1}h}$. Заметим, что $L^{g^{-1}h}$ — подполе и значит, линейное подпространство. Докажем, что найдется такое h, что $L^{g^{-1}h} = L$.

а) Пусть L конечно. Тогда $L^* = \langle b \rangle$, поэтому найдется такой $h \in H$, что $b \in L^{g^{-1}h}$ и поэтому $L^{g^{-1}h} = L$.

б) Пусть $|L| = \infty$. Так как $L = \cup_{h \in H} L^{g^{-1}h}$, то по лемме 4 (11.9) $\exists h \in H : L^{g^{-1}h} = L$. Значит, $\forall g \in G \, \exists h \in H : L^{g^{-1}h} = L$, поэтому $g^{-1}h|_L = \mathrm{Id}$. Тогда $g = h$ и значит, $H = G$.

Лемма и Теорема 11.1 доказаны.

Задача 11.11. Решение. $\Rightarrow$ a сепарабелен, поэтому существует сепарабельный многочлен $f \in K[x]$, т.ч. $f(a) = 0$. Значит, $\mu_a | f(x)$, поэтому μ_a не имеет кратных корней ни в каком расширении поля K.

$\Leftarrow$ Так как μ_a сепарабелен, можно взять $f = \mu_a$, a — его корень.

Задача 11.13. Решение. $K \subset E$, $\forall a \in E$ μ_a сепарабелен, так как $a \in F$. Далее, $E \subset F$. Пусть $a \in F$. Имеем $\mu_a^E | \mu_a^K$, так как минимальный многочлен делит аннулирующий. У μ_a^K нет кратных корней, так как $a \in F$ и $K \subset F$ сепарабельно. Значит, μ_a^E не может иметь кратных корней в силу факториальности кольца многочленов над полем.

Задача 11.14. Решение. а) Пусть $|P| < \infty$, $\mathrm{char}\, P = p$. Рассмотрим $\Phi : x \to x^p$ — автоморфизм Фробениуса. Тогда $\forall a \in P \; \exists b \in P : \; b^p = a$.

б) Пусть $P \subset F$ — алгебраическое расширение, $a \in F$. Пусть μ_a не сепарабельный, тогда $(\mu_a, \mu_a') \neq 1$, поэтому $\mu_a' = 0$ и значит, $\mu_a(x) = g(x^p)$ (задача 9 листка 8,5). Далее, $g(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$. При этом $\forall i = 0, \ldots, n \; a_i = b_i^p$, так как P совершенно, $\Rightarrow \mu_a(x) = a_0 x^{np} + a_1 x^{(n-1)p} + \ldots + a_n = (b_0 x^n + b_1 x^{n-1} + \ldots + b_n)^p$, а значит, $\mu_a(x)$ приводим. Получили противоречие, значит, $\mu_a(x)$ — сепарабельный многочлен.

Задача 11.15. Решение. а) Пусть $\theta \in P$, $\theta^p = a$. Тогда $x^p - a = (x - \theta)^p$. Пусть $a \in P^p \setminus P$ и $x^p - a = g(x)h(x)$, где $\deg g(x), h(x) \geq 1$. Возьмем $L = P(x^p - a)$. Пусть β — корень $f(x) = x^p - a$ в L, т.е. $\beta^p = a$. Тогда в $L[x]$ имеем $x^p - a = (x - \beta)^p$, поэтому, в силу факториальности $L[x]$ получаем $g(x) = (x - \beta)^k$, $h(x) = (x - \beta)^l$, $k, l \geq 1, k + l = p$. Рассматривая свободные члены многочленов $g(x), h(x), f(x)$, получаем $\beta^k, \beta^l, \beta^p \in P$. Так как $(p, k) = 1$, то $\exists u, v : up + kv = 1$, поэтому $(\beta^p)^u \cdot (\beta^k)^v = \beta$ и значит, $\beta \in P$, $\beta^p = a$. Получили противоречие, следовательно, $x^p - a$ неприводим.

б) Если поле характеристики ноль, утверждение очевидно. Пусть $\mathrm{char}\, P = p$. Если $P^p = P$, то P совершенно. Если нет, то $\exists a \in P^p \setminus P$, поэтому по пункту а) многочлен $x^p - a$ неприводим. Но $(x^p - a)^l = 0$, тогда $x^p - a$ не сепарабелен. Противоречие с пунктом а).

Задача 11.16. Решение. $f'(x) = 0$, поэтому $f(x)$ не сепарабельный. Рассмотрим $\mathbb{Z}_p[t]$. В нем t — простой элемент, значит он прост и в $\mathbb{Z}_p(t)[x]$, так как $Q(\mathbb{Z}_p[t]) = \mathbb{Z}_p(t)$ и работает факториальность кольца многочленов над факториальным кольцом — Лемма Гаусса. Тогда $x^p - t$ неприводим по критерию Эйзенштейна.

Листок 12.

Задача 12.1. Решение. Утверждение (*): $K \subset L$ нормально и сепарабельно титтк $\forall a \in L$ μ_a раскладывается на линейные, не кратные множители, т.е. количество корней μ_a равно $\deg \mu_a$.

$\Rightarrow$ (*) выполнено по следствию из леммы 3 (задача 11.8).

$\Leftarrow$ Пусть (*) выполнено. Тогда тождественный автоморфизм Id: $K \to K$ мы можем продолжить до автоморфизма $L \to L$ ровно $[L:K]$ способами. Это доказывается так же, как начало доказательство леммы 5 (задача 11.10). Значит, $|\mathrm{Aut}(L/K)| = [L:K]$.

Задача 12.2. Решение. $\Rightarrow L = K(a_1, \ldots, a_s)$. Рассмотрим, $f = (\mu_{a_1} \cdot \ldots \cdot \mu_{a_s})_{\mathrm{red}}$, где минимальные многочлены включаем только с кратностью 1. Теперь $L = K(f)$, f сепарабелен, так как $\forall i$ μ_{a_i} сепарабелен по 12.1, а если $\mu_{a_i} \neq \mu_{a_j}$,, то наборы корней у них различны по задаче 10 листка 8,5. $L = K(f)$, так как все корни f лежат в L из-за того, что $K \subset L$ нормально (по 12.1) и по определению $L = K(a_1, \ldots, a_s)$, поэтому меньшего поля построить нельзя.

$\Leftarrow$ $f = c(x - a_1) \cdot \ldots \cdot (x - a_n)$, где $c \in K$, $a_1, \ldots, a_n \in L$, $a_i \neq a_j$ при $i \neq j$. Рассмотрим башню расширений $K = K_0 \subset K_1 \subset \ldots \subset K_i = K_{i-1}(a_i) \subset \ldots \subset K_n = L$ и аналогично, как в начале доказательства леммы 5 (задача 11.10), получим, что $|\mathrm{Aut}(L/K)| = [L:K]$. Тогда $K \subset L$ — расширение Галуа.

Задача 12.3. Решение. Расширение $K \subset M$ сепарабельно. $M = K(a_1, \ldots, a_s)$, для любого i a_i сепарабелен над K, т.е. все μ_{a_i} сепарабельны. Положим $f = (\mu_{a_1} \cdot \ldots \cdot \mu_{a_s})_{red}$, тогда f сепарабелен. $L = K(f)$, тогда $M \subset L$ —- расширение Галуа над K по 12.2.

Задача 12.4. Ответы. а) Поле разложения $\mathbb{Q}(x^3 - 2)$; б) Поле разложения $\mathbb{Q}(x^4 - 2)$.

Задача 12.5. Решение. $I_g(H) \subset G$ $\forall g \in G$, $H \subset G$. Критерий подгруппы: $a, b \in H \Rightarrow ab^{-1} \in H$. Теперь докажем а). Действительно, $I_g(a)I_g(b^{-1}) = I_g(ab^{-1}) \subset I_g(H)$. Если $I_g(H_1) = I_g(H_2)$, то $H_1 = H_2$. Очевидно, что $I_g(I_{g^{-1}}(H)) = H$, поэтому I_g — биекция. Далее, очевидно, что $I_{g_1}I_{g_2} = I_{g_1g_2}$, поэтому I_g — гомоморфизм группы G в группу биекций множества S.

Утверждения б) и в) следуют из определений.

Задача 12.6. Решение. Сразу заметим, что если $K \subset M \subset L$, а $K \subset L$ — расширение Галуа, то $M \subset L$ — расширение Галуа по задачам 11.13, 10.9, 12.1. Далее, $K \subset M$ — расширение Галуа титтк $K \subset M$ — нормальное расширение.

Докажем утверждения а), б).

Установим соответствие $M \mapsto H = \{g \in \mathrm{Gal}(L/K) : g(a) = a \ \forall a \in M\}$. $H = \mathrm{Gal}(L/M)$, так как $M \subset L$ — расширение Галуа. Докажем, что соответствия $M \mapsto H = \mathrm{Gal}(L/M)$ и $H \mapsto M = L^H$ взаимно обратны. Применим лемму 5 (задача 11.10) к нашей конструкции. $M \subset L$ — конечное расширение степени n, $\mathrm{Aut}(L/M) = G$. Пусть $H \subset G$ — такая подгруппа, что $L^H = M$, тогда $H = G$ и $|G| = n$. Значит, если $M = L^H$, то $H = \mathrm{Aut}(L/M)$. Обратно, если $H = \mathrm{Aut}(L/M)$, $M \subset L$ — расширение Галуа, то $|\mathrm{Aut}(L/M)| = [L:M]$ а это, по теореме 1 листка 11 выполняется титтк $L^H = M$.

в) Пусть $K \subset M \subset L$, найдем $\mathrm{Aut}(M/K)$. Разложим $M \subset L$ в цепочку простых расширений $M = M_0 \subset M_1 \subset \ldots \subset M_i = M_{i-1}(a_i) \subset \ldots \subset M_s = L$. Продолжим $\varphi \in \mathrm{Aut}(M/K)$ до автоморфизма $g \in G = \mathrm{Gal}(L/K)$ постепенно по этажам нашей башни. Для продолжаемости $\varphi_{i-1} : M_{i-1} \to L$ до $\varphi_i : M_i \to L$ нужно, чтобы $\mu_i(x)$ имел корень в L, где $\mu_i(x)$ — минимальный многочлен a_i над M_{i-1}. Но μ_i делит $\mu_{a_i}^K$, который разлагается на линейные множители в $L[x]$, так как $K \subset L$ — нормально, поэтому любой автоморфизм M над K можно продолжить до автоморфизма L над K.

Это можно сделать, потому что μ_i и $\mu_i^{\varphi_{i-1}}$ делят μ_{a_i}, поэтому $\mu_i^{\varphi_{i-1}}$ имеет корень, тогда гомоморфизм продолжить можно по задаче 10.1.

Пусть $M = L^H$, тогда для любого $g \in G$ имеем $g(M) = L^{gHg^{-1}}$. Действительно, $a \in g(M)$ титтк $g^{-1}(a) \in M$ титтк $hg^{-1}(a) = g^{-1}(a)$ для любого $h \in H$ (так как $M = L^H$ — поле инвариантов), это по определению означает, что $ghg^{-1}(a) = a$ для любого $h \in H$.

По биективности соответствия Галуа разным подполям соответствуют разные подгруппы. Так как при автоморфизме базисы переходят в базисы, то $G(M) \subset M \ \Rightarrow \ g(M) = M$. Значит, $gHg^{-1} = H$, так как $L^{gHg^{-1}} = L^H$ а это как раз определение элемента нормализатора (определение 12.2), Рассмотрим гомоморфизм из $N(H)$ в $\mathrm{Aut}(M/K)$, определенный так: $\varphi : L \to L$ переходит в $\tilde{\varphi} : M \to M$, где $\tilde{\varphi} = \varphi|_M$.

Так как $L^H = M$, очевидно, что ядро — подгруппа H. Он сюръективен, так как для любого $\varphi \in \mathrm{Aut}(M/K)$ существует его продолжение до автоморфизма L над K, поэтому $\mathrm{Aut}(M/K) \cong N(H)/H$, где $N(H)$ — нормализатор H в G.

По теореме о башне расширений $[L:K] = [L:M]\cdot[M:K]$. Так как L/K и L/M — расширения Галуа, то $[L:K] = |G|$, $[L:M] = |H|$, поэтому $[M:K] = |G|/|H|$.

По определению $M \supset K$ — расширение Галуа титтк $|\mathrm{Aut}(M/K)| = [M:K]$. Но $|\mathrm{Aut}(M/K)| = |N(H)|/|H|$, а $[M:K] = |G|/|H|$, поэтому $|\mathrm{Aut}(M/K)| = [M:K]$ титтк $|N(H)| = |G|$ титтк $H \lhd G$ по 12.5 в).

Задача 12.7. Ответы. а) $\mathbb{Z}_d$, где $dk = n$, см. задачу 10.18 б); б) $(\mathbb{Z}/n\mathbb{Z})^*$ — группа обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$, см. задачу 11.3 г); в) $V_4 = \mathbb{Z}_2 \oplus \mathbb{Z}_2$, см. задачу 11.2 д); г) $V_4 = \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Задача 12.8. (Это теорема о примитивном элементе). **Решение.** $K \subset M$ — конечное сепарабельное расширение. Вложим его в расширение Галуа. По задаче 12.3 Существует $L : K \subset L$ — расширение Галуа и $L \supset M$. По ОТТГ — основной теореме теории Галуа 12.6 для любого F, такого что $K \subset F \subset L$, существует единственная $H \in G = \mathrm{Gal}(L/K)$, такая что $F = L^H$. Так как $|G| < \infty$, таких F конечное число. Значит, и промежуточных F, таких, что $K \subset F \subset M$ — конечное число. Пусть M конечно. Тогда $M^* = \langle a\rangle$, поэтому $M = K(a)$. Пусть теперь $|M| = \infty$. Тогда, по лемме 4 из листка 11 (задача 11.9), так как F — линейное подпространство, существует такое a, что для любого F — собственного подполя M, $a \notin F$. Тогда $K(a) = M$.

Задача 12.9. Решение. а) Пусть f над K, $G = Gal(L/K)$. Пусть $L = K(a_1, \dots a_n)$ и G действует на $a_1, \dots a_n$ не транзитивно, т.е. найдется элемент a_i, для которого $G(a_i) = \{a_{i_1}, \dots a_{i_n}\}$, где $k < n$. Согласно 11.8 $\mu_{a_i}(x) = (x - a_{i_1}) \dots (x - a_{i_k})$, $\deg \mu_{a_i} = k$ и $\mu_{a_i} | f(x)$, поэтому f приводим. Обратно, если G действует на $a_1, \dots a_n$ транзитивно, то для любого a_i $\mu_{a_i}(x) = (x - a_1) \dots (x - a_n)$ по 11.8. Тогда $f = c\mu_{a_i}$, где $c \in K$, т.е. f неприводим.

б) Следует из 11.8 и 9.15.

Задача 12.10. Решение. а) По 11.3 б) $G = Gal(\mathbb{Q}(x^3-2)/\mathbb{Q}) \cong S_3$. Корни $f(x) = x^3 - 2$ такие: $x_{1,2,3} = \varepsilon, \varepsilon\omega, \varepsilon\omega^2$, где $\varepsilon = \sqrt[3]{2}$, ω — первообразный корень 3-й степени из 1. Так как $[\mathbb{Q}(x^3-2) : \mathbb{Q}] = 6$, то найдем элемент в $\mathbb{Q}(x^3-2)$ с орбитой длины 6. Рассмотрим циклы $\sigma : \varepsilon \to \varepsilon\omega \to \varepsilon\omega^2 \to \varepsilon = (1,2,3)$ и $\tau : \varepsilon \to \varepsilon, \varepsilon\omega \to \varepsilon\omega^2 = (2,3)$ — сопряжение. Заметим, что $\sigma(\omega) = \sigma(\frac{\varepsilon\omega^2}{\varepsilon\omega}) = 1/\omega^2 = \omega$, $\tau(\omega) = \omega^2$, так как $\tau(\varepsilon) = \varepsilon$. Мы знаем, что $G = \{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma\tau, \tau\sigma\}$ по 0.4 д). Рассмотрим $G(\varepsilon + \omega) = \{\varepsilon + \omega, \varepsilon\omega + \omega\,\varepsilon\omega^2 + \omega\,\varepsilon + \omega^2, \varepsilon\omega + \omega^2, \varepsilon\omega^2 + \omega^2\}$. Значит, $\varepsilon + \omega$ —примитивный элемент $\mathbb{Q}(x^3-2) \supset \mathbb{Q}$.

б) $\mathbb{Q}(\sqrt{p}, \sqrt{q})$. Очевидно, что $\{1, (\sqrt{p}, \sqrt{q}\sqrt{pq}\}$ —- это базис, $x^2 - p$, $x^2 - q$ неприводимы, поэтому $b : \sqrt{p} \mapsto -\sqrt{p}$, $\delta : \sqrt{q} \mapsto -\sqrt{q}$ —- автоморфизмы, причем $b^2 = \delta^2 = id$. Рассмотрим $\theta = b : \sqrt{p} + \sqrt{q}$, $\mu_\theta(x) = (x - (\sqrt{p} + \sqrt{q}))(x - (\sqrt{p} + \sqrt{q}))(x(\sqrt{p} - \sqrt{q}))(x + (\sqrt{p} - \sqrt{q})) = x^4 - 2(p+q)x^2 + (p-q)^2$ — неприводим, так как все корни иррациональны, а любое попарное произведение линейных множителей —- многочлен, не лежащий в $\mathbb{Q}[x]$. Заметим, что $\theta^2 = p + q + 2\sqrt{pq}$, $\theta^3 = \sqrt{p}(2q+p) + \sqrt{q}(2p+q)$. Значит, $\sqrt{pq} = (1/2)(\theta^2 - p - q)$, $\sqrt{p} = \frac{1}{2(q-p)}(\theta^3 - (3p+q)\theta)$, $\sqrt{q} = \frac{1}{2(p-q)}(\theta^3 - (3q+p)\theta)$, т.е. θ —- примитивный и $\mu_\theta(x)$ —- его минимальный многочлен.

в) Аналогично б), имеем расширение $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt{2}, i]$ 4-й степени, базис $1, \sqrt{2}, i, i\sqrt{2}$. Докажем, что $\theta = \sqrt{2} + i$ —- примитивный. Аналогично б), $\pm\sqrt{2} \pm i$ — корни минимального многочлена $x^4 - 2x^2 + 9 = \mu_\theta(x)$, и элементы группы $G = Gal(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ действуют на многочлены $x^2 - 2$ и $x^2 + 1$ (см. решение 11.2 д)), поэтому $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ (группа Клейна). Так как $\theta = \sqrt{2} + i$, $\theta^2 = 1 + 2\sqrt{2}i$, $\theta^3 = 5i - \sqrt{2}$, то $i = (\theta^3 + \theta)/6$, $i\sqrt{2} = (\theta^2 - 1)/2$, $\sqrt{2} = (5\theta - \theta^3)/6$, поэтому $1, \theta, \theta^2, \theta^3$ —- базис в $\mathbb{Q}[\sqrt{2}, i]$.

г) Так как $[\mathbb{Q}(\sqrt{2}, i)] = 4$, а $\mu_{-1/2+i\sqrt{2}/2} = x^2 + x + 3/4$, то $-1/2 + i\sqrt{2}/2$ не может быть примитивным элементом.

Задача 12.11. Решение. Так как $\mathbb{Q}(x^4 - 2)$ — поле разложения сепарабельного многочлена, то это расширение Галуа по 12.2. Согласно 10.4 д) $|G| = |Gal(\mathbb{Q}(x^4-2)/\mathbb{Q})| = 8$. Так как $\mathbb{Q}(x^4 - 2) \supset$

$\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$ — не нормальное расширение (расширение $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$ не содержит комплексных корней многочлена $x^4 - 2$, то по ОТТГ 12.6 соответствующая подгруппа G не нормальна, поэтому G не коммутативна, так как в абелевой группе любая подгруппа нормальна. Значит, согласно указанию, G — это D_4 или $\mathbb{Q}_8$.

Но в $\mathbb{Q}_8$ все подгруппы нормальны. Действительно, ± 1 лежат в центре группы, а для $\pm i$, $\pm j$, $\pm k$ обратными будут $\mp i$, $\mp j$, $\mp k$. Значит, $(\mathbb{Q}_8)'$ — это $\{\pm 1\}$. Очевидно, что любая неединичная подгруппа содержит $\mathbb{Q}'_8$, тогда по задаче 7,25.5 все подгруппы нормальны.

Другое рассуждение: $|\mathbb{Q}_8/\pm 1| = 4$, значит, эта группа абелева, тогда по задаче 7,25.4 $\{\pm 1\}$ — коммутант; $\mathbb{Q}_8$ не абелева, значит, по 7,25.5 все ее подгруппы нормальны.

Итак, $Gal(\mathbb{Q}(x^4 - 2)/\mathbb{Q}) \cong D_4$.

Листок 13.

Задача 13.1. Решение. Доказываем индукцией по длине цепочки полей. При $i = 1$ $K \subset K$ — радикальное расширение Галуа. Пусть имеем цепочку $K = K_0 \subset K_1 \subset ... \subset K_{i-1} \subset K_i = K_{i-1}(b_i) \subset ... \subset K_s = F$, где $K \subset E_{i-1}$ — радикальное расширение Галуа. По условию $b_i^{n_i} = c_i \in K_{i-1}$. Рассмотрим многочлен $\mu_{c_i}^K = (x - c_i)(x - c'_i)(x - c''_i)....$ Он разлагается на линейные множители, так как $K \subset E_{i-1}$ — расширение Галуа. Заметим, что $\operatorname{char} K = 0$, тогда по 11.12 все минимальные многочлены сепарабельны, поэтому, согласно 12.1, чтобы получилось расширение Галуа, достаточно нормальности.

$K \subset E_{i-1}$ — расширение Галуа. Значит, есть такой $g(x) \in K[x]$, что $E_{i-1} = K(g(x))$ — по 12.2. Рассмотрим $f(x) = \mu_{c_i}^K(x^{n_i}) = (x^{n_i} - c_i)(x^{n_i} - c'_i)(x^{n_i} - c''_i)...$ и положим $E_i = E_{i-1}(f(x))$. Очевидно, что $E_i = E_{i-1}(f(x)) = K(f(x)g(x))$ — по 8,5.14 б). Поэтому $K \subset E_i$ — расширение Галуа. По предположению индукции $K \subset E_{i-1}$ — радикальное расширение. $E_{i-1} \subset E_i$ — радикальное расширение, так как добавлены все корни степени n_i из $c_1, c'_i, c''_i, ...$, поэтому $K \subset E_i$ — радикальное расширение Галуа. Теперь надо организовать вложение K_i в E_i. Заметим, что $K_{i-1} \hookrightarrow E_{i-1}$ по предположению индукции[1], $E_{i-1} \hookrightarrow E_i$ по построению, поэтому $K_{i-1} \hookrightarrow E_i$. Но $K_i = K_{i-1}(b_i)$, b_i — корень $f(x)$, так как $b_i^{n_i} = c_i$, тогда по 10.1 вложение $K_{i-1} \hookrightarrow E_i$ можно продолжить до $K_i \hookrightarrow E_i$, так как $b_i \in E_i$. При $i = s$ мы получим нужное радикальное расширение Галуа.

Задача 13.2. Решение. Рассмотрим $\Gamma = \{\gamma \in L : \gamma^n = 1\}$. Так как $(x^n - 1, nx^{n-1}) = 1$ в силу нулевой характеристики, то $|\Gamma| = n$. Так как Γ — конечная подгруппа мультипликативной группы поля и значит, циклическая (по 3.9), то $\Gamma = \langle\xi\rangle$, где $\operatorname{ord}\xi = n$. Значит, $L = K(\xi)$, поскольку $L = K(f)$. Далее, для любого $g \in G$ имеем $g(\xi) = \xi^k$, так как g переводит корень $f(x)$ в корень $f(x)$. Поэтому k полностью определяет g. Пусть $h \in G$, $h(\xi) = \xi^l$. Тогда $gh(\xi) = g(\xi^l) = (g(\xi))^l = (\xi^k)^l = \xi^{kl} = \xi^{lk} = hg(\xi)$. Т.е. для любых $g, h \in G$ имеем $gh = hg$, G — абелева.

Задача 13.3. Решение. Случай $c = 0$ тривиален. Если x_1, x_2 — корни $f(x)$, где $f(x) = x^n - c$, то $x_1/x_2 = \gamma$, где $\gamma^n = 1$. Любое такое $\gamma \in \Gamma$ — группе корней из 1, поэтому все корни $f(x) = x^n - c$ лежат в $F = K(b)$, где $b^n = c$. Значит, $F = L$, где $L = K(f)$. Для любых $g, h \in G = Aut(L/K)$ g, h переводят корни $f(x)$ в корни $f(x)$, значит, $g(b) = \gamma b$, $h(b) = \delta b$, где $\gamma, \delta \in \Gamma \subset K$. Тогда $gh(b) = g(\delta b) = \delta g(b) = \delta\gamma b = (\gamma\delta)b$, так как g, h действуют на $\Gamma \subset K$ тождественно. Поскольку автоморфизмы g и h однозначно определяются своим действием на b, мы получаем вложение $G \hookrightarrow \Gamma \cong \mathbb{Z}/n\mathbb{Z}$, $g \mapsto \gamma = g(b)/b$, т.е. G — подгруппа группы $\mathbb{Z}/n\mathbb{Z}$. Поэтому G — циклическая и $|G|$ делит n. Мономорфность очевидна.

Задача 13.4. Решение. Проведем индукцию по n. $n = 1$, база индукции: $c_1\delta_1(x) = 0$ для любого $x \in L$, тогда $c_1 = 0$.

Шаг индукции: пусть для $n-1$ утверждение выполнено. Пусть $c_1\delta_1(x) + \ldots + c_n\delta_n(x) = 0$ (*) для любого $x \in L$, причем для любого i $c_i \neq 0$, иначе все сводится к индукционному предположению. Возьмем произвольное $a \neq 0$, $a \in L$. Получим $c_1\delta_1(xa) + \ldots + c_n\delta_n(xa) = 0$, тогда $c_1\delta_1(x)\delta_1(a) +$

[1] Стрелка здесь и далее $\hookrightarrow$ обозначает мономорфизм.

$\ldots + c_n\delta_n(x)\delta_n(a) = 0$. Вычтем отсюда равенство (*), умноженное на $\delta_n(a)$. Получим $c_1(\delta_1(a) - \delta_n(a))\delta_1(x) + \ldots + c_{n-1}(\delta_{n-1}(a) - \delta_n(a))\delta_{n-1}(x) = 0$ для любого $x \in L$. Так как $\delta_1, \ldots \delta_{n-1}$ линейно независимы, то все коэффициенты нулевые: $c_i(\delta_i(a) - \delta_n(a)) = 0$ для всех $i = 1, \ldots, n$. Но так как δ_i и δ_n, $i = 1, \ldots, n-1$, — различные автоморфизмы, то для всех $i = 1, \ldots, n-1$ можно так выбрать $a \in L$, что $\delta_i(a) \neq \delta_n(a)$, значит, $c_i = 0$ для всех $i = 1, \ldots, n-1$. Тогда и $c_n = 0$. Противоречие.

Задача 13.5. Решение. Рассмотрим $g, g^2, \ldots, g^n = id$. Если бы $r(\alpha) = 0$ для любого $\alpha \in L$, то мы получили бы линейную зависимость автоморфизмов $g, g^2, \ldots, g^n$, так как $\xi^i \neq 0$ для всех $i = 1, \ldots, n$. Это противоречит 13.4.

Задача 13.6. Решение. По 13.5 существует $r(\alpha) \neq 0$, $g(r(\alpha)) = \xi r(\alpha)$, поэтому $g^l r(\alpha) = \xi^l r(\alpha)$, тогда $Gr(\alpha) = \{\xi^i r(\alpha), i = 0, \ldots, n-1\}$. Орбита содержит n различных элементов, поэтому по 12.9 б) $r(\alpha)$ — примитивный элемент расширения. Заметим, что $g(r(\alpha)^n) = (g(r(\alpha)))^n = (\xi r(\alpha))^n = \xi^n r(\alpha)^n = r(\alpha)^n$. Поэтому $r(\alpha)^n \in L^G = K$, то есть $r(\alpha)$ — искомый элемент.

Задача 13.7. Решение. G разрешима, значит, существует такой ряд: $G \triangleright G' \triangleright G'' \triangleright \ldots \triangleright G''' = \{e\}$. Согласно 7,25.2 и 7,25.4 $G \triangleright G'$, $H = G/G'$ абелева и конечна. Рассмотрим $\varphi : G \to G/G'$ — естественный эпиморфизм. Рассмотрим $M \subset H$ — подгруппу максимального порядка (вложение строгое). $\varphi^{-1}(M) \supset G'$, поэтому по 7,25.4 $\varphi^{-1}(M) \triangleleft G$ и $G/\varphi^{-1}(M) \cong \mathbb{Z}_{p_i}$, иначе M не имела бы максимальный порядок, здесь мы воспользовались обратной теоремой Лагранжа для абелевых групп 8.11 б). У $G/\varphi^{-1}(M)$ не может быть собственных подгрупп и $G/\varphi^{-1}(M)$ абелева, так как $\varphi^{-1}(M) \supset G'$, снова по 7,25.4. Очевидно, что $\varphi^{-1}(M)$ разрешима, см. 7,25.10 и $|\varphi^{-1}(M)| < |G|$, поэтому можно применить индукцию по порядку группы.

Задача 13.8. Решение. $\Rightarrow$ По 13.1 можем считать, что $K \subset L \subset F$, где $K \subset F$ —- радикальное расширение Галуа. Но $K \subset L$ — тоже расширение Галуа как поле разложения сепарабельного многочлена ($\operatorname{char} K = 0$, см. 11.12 и 12.2), поэтому $G = Gal(f) \cong Gal(F/K)/Gal(F/L)$ по 12.6 в) (ОТТГ)). Поэтому для разрешимости G достаточно показать, что $Gal(F/K)$ разрешима (7,25.11). Значит, считаем, что $L = F$, $K = K_0 \subset K_1 \subset \ldots \subset K_i = K_{i-1}(b_i) \subset \ldots \subset K_s = F = L$, где $b_i^{n_i} = c_i \in K_{i-1}$, $n_i \in \mathbb{N}$. Пусть $n = HOK(n_1, n_2, \ldots, n_s)$. Добавим в каждое подполе корни степени n из 1, т.е. корни уравнения $x^n - 1 = 0$.

Так как существует ξ — первообразный корень степени n из 1, то достаточно добавить к каждому полю ξ. Очевидно, $L(\xi) = K((x^{n-1})f(x))$, $K(\xi) = K(x^n - 1)$. Значит, $L(\xi) \supset K$ — расширение Галуа и $L \supset K$ — подрасширение Галуа, поэтому по 12.6 в) $G = Aut(L(\xi)/K)/Aut(L(\xi)/L)$ и по 7,25.11 достаточно доказать, что $\tilde{G} = Aut(L(\xi)/K)$ разрешима.

Имеем башню расширений $K(\xi) \subset K_1(\xi) \subset \ldots \subset K_{i-1}(\xi) \subset K_i(\xi) \subset \ldots \subset L(\xi)$. По ОТТГ 12.6 имеем ряд $\tilde{G} \triangleright H_0 \triangleright \ldots H_{i-1} \triangleright H_i \triangleright \ldots \triangleright H_s = \{id\}$. Нормальность подгрупп следует из того, что $K_i(\xi) = K_{i-1}(\xi)(x^{n_i} - b_i^{n_i})$ (достаточно очевидно из 13.3), поэтому имеем расширение Галуа, а значит, по 12.6 в), нормальность соответствующей подгруппы. Для любого i $K_i(\xi) \subset L(\xi)$ — расширение Галуа, так как $K \subset L(\xi)$ — расширение Галуа, см. 12.6 а), б). По 13.2 группа $\tilde{G}/H_0$ абелева, по 13.3 группа H_i/H_{i-1} — циклическая. Значит, по 7,25.12, применяя s раз, получаем, что группа G разрешима.

$\Leftarrow$ G разрешима, поэтому по 13.7 можно построить ряд $G = H_0 \triangleright \ldots H_{i-1} \triangleright H_i \triangleright \ldots \triangleright H_s = \{id\}$ такой что $H_{i-1}/H_i \cong \mathbb{Z}_{p_i}$, где p_i — простое число. По ОТТГ 12.6 в) этому ряду соответствуют ряд подполей в поле L: $K = K_0 \subset K_1 \subset \ldots \subset K_{i-1} \subset K_i \subset \ldots \subset K_s = L$. Положим $n = HOK(p_1, \ldots, p_s)$ и присоединим к каждому полю башни все корни степени n из 1 или просто ξ — первообразный корень степени n из 1. Получим башню $K_0(\xi) \subset K_1(\xi) \subset \ldots \subset K_{i-1}(\xi) \subset K_i(\xi) \subset \ldots \subset L(\xi) = F$. $H_{i-1} \triangleright H_i$, отсюда по 12.6 в) следует, что расширение $K_{i-1} \subset K_i$ нормально, тогда по 10.7 найдется. такой $f(x)$ что $K_i = K_{i-1}(f) \Rightarrow K_i(\xi) = K_{i-1}(\xi)(f(x))$ (достаточно очевидно, так как мы просто расширили поле коэффициентов), поэтому $K_{i-1}(\xi) \subset K_i(\xi)$ — расширение Галуа. (На сепарабельность внимания не обращаем в силу нулевой характеристики.)

Если $g \in Gal(K_i(\xi)/K_{i-1}(\xi))$, то он неподвижен на ξ и на элементах из K_{i-1}, значит, $\forall a \in K_i$ $g(a) \in K_i$ так как если бы $g(a) \in K_i(\xi)$, то было бы $a = g^{-1}(g(a)) \in K_i(\xi)$ (так как $g^{-1}(\xi) = \xi$ для

любого $g \in Gal(K_i(\xi)/K_{i-1}(\xi)))$, что противоречит выбору a. Поэтому $g|_{K_i} \in Gal(K_i/K_{i-1})$. Ясно, что гомоморфизм ограничения на K_{i-1} $\psi : Gal(K_i(\xi)/K_{i-1}(\xi)) \to Gal(K_i/K_{i-1})$ мономорфен, так как ξ остается на месте и подъем наверх однозначен, т.е. ψ — мономорфизм: $Gal(K_i(\xi)/K_{i-1}(\xi)) \hookrightarrow Gal(K_i/K_{i-1}) \cong \mathbb{Z}_{p_i}$. Значит, $Gal(K_i(\xi)/K_{i-1}(\xi))$ либо тривиальна, либо изоморфна $\mathbb{Z}_{p_i}$, поэтому по 13.6 $K_i(\xi) = K_{i-1}(\xi, b_i)$, где $b_i^{p_i} \in K_{i-1}(\xi)$. Значит, $K \subset F$ — радикальное расширение.

Задача 13.9. Решение. а) Пусть $f = p/q$ — симметрическая дробно-рациональная функция. Рассмотрим $\tilde{q} = \prod\limits_{\sigma \in S_n} \sigma(q)$, $\tilde{p} = (\prod\limits_{\sigma \in S_n, \sigma \neq id} \sigma(q))p$. Очевидно, что $f = \tilde{p}/\tilde{q}$, так как мы просто домножили числитель и знаменатель на $\prod\limits_{\sigma \in S_n, \sigma \neq id} \sigma(q)$. Но $\tilde{q}$ — симметрический многочлен, поэтому $\tilde{p} = f\tilde{q}$. — тоже симметрический. Значит, по теореме о представлении симметрического многочлена многочленом от элементарных симметрических многочленов утверждение доказано.

б) Пусть L — поле разложения $f(x)$ над $K(c_1, ..., c_n)$. По определению, $L = K(c_1, ..., c_n)[a_1, ..., a_k]$, где $a_1, ..., a_k$ — корни $f(x)$. Рассмотрим $T = K(x_1, ..., x_n)$, где $x_1, ...x_n$ — независимые переменные и $K(x_1, ..., x_n)$ — поле рациональных функций. Рассмотрим группу перестановок переменных $\{x_1, ...x_n\}$, которая изоморфна S_n. Ясно, что S_n действует на поле $K(x_1, ..., x_n) = T$, т.е. имеется гомоморфизм $\psi : S_n \to Aut(K(x_1, ..., x_n)/K)$, который просто переобозначает переменные. Посмотрим, что будет полем инвариантов T^{S_n} группы S_n. Очевидно, что на месте остаются только симметрические дробно-линейные функции, т.е. по 13.9 а) дробно-линейные функции от симметрических многочленов. Итак, $T^{S_n} = K(\sigma_1, ..., \sigma_n)$. Мы знаем, что $\sigma_1, ..., \sigma_n$ алгебраически независимы, т.е. никакой ненулевой многочлен от них не становится нулевым. Значит, имеет место изоморфизм $\varphi : K(c_1, ...c_n) \to K(\sigma_1, ..., \sigma_n)$, $\varphi(c_i) = (-1)^n \sigma_i(x_1, \ldots, x_n)$. Но так как $(-1)^i \sigma_i(a_1, ...a_n) = c_i$, то при продолжении этого изоморфизма до изоморфизма $\tilde{\varphi} : L \to T$ a_i должно переходить в x_i, т.е. $L \cong K(x_1, ..., x_n)$, $L^{S_n} \cong K(c_1, ..., c_n)$, поэтому $Aut(L/K(c_1, ..., c_n)) \cong S_n$, т.е. $Gal(f)$ над $K(c_1, ..., c_n)$ изоморфна S_n и значит, неразрешима при $n > 4$.

Вывод: формулы общего решения уравнения степени 5 и выше в радикалах не существует (теорема Абеля-Руффини).

в) Пусть G — конечная группа. Тогда по теорема Кэли 5.10 $G \subset S_n$, где $n = |G|$. По 13.9 б) существует $L \supset K$ — расширение Галуа, такое что $Gal(L/K) \cong S_n$. По ОТТГ 12.6 для любой подгруппы $G \subset S_n$ найдется $E : L \supset E \supset K$, $L^G = E$ и $L \supset E$ — расширение Галуа, причем $Gal(L/E) = G$. Теорема доказана.

Задача 13.10. **Решение.** Пусть $|G| = p^k m$, $(m, p) = 1$, p — простое.

1) Если G — абелева, то возьмем ее p-компоненту, так как $G = \oplus_p G_p$, где $G_p = \{x \in G : \mathrm{ord}(x) = p^l, l \in \mathbb{N} \cup \{0\}\}$. По 8.7.

2) Если $|G| = p^n$, то $H = G$.

3) Пусть $|G| = p^n m$, $(m, p) = 1$, $m > 1$. Проведём индукцию по $|G|$. Рассмотрим $Z(G)$ — центр.

а) Пусть p делит $|\mathbb{Z}(G)|$, тогда по 8.11 б) существует такая подгруппа $A \subset Z(G)$, что $|A| = p$. Очевидно, что $A \triangleleft G$, поэтому $|G/A| = n/p = p^{n-1}m < |G|$, . Тогда существует $\overline{B} \subset G/A$, такая что $|\overline{B}| = p^{n-1}$ (по индуктивному предположению). $\overline{B} = B/A$, где $B = \pi^{-1}(\overline{B})$ — прообраз при естественном гомоморфизме. $\overline{B} = B/A \subset G/A$ и $A \subset B \subset G$. Значит, $|B| = |A| \cdot |B/A| = p^n$, поэтому B — силовская подгруппа.

б) Пусть p не делит $|Z(G)|$. Подействуем на G сопряжением и разобьем G на классы сопряженности. По формуле из 5.8 $|G| = |Z(G)| + \sum\limits_{i=1}^{r} |G|/|St(x_i)|$. Так как p не делит $|Z(G)|$, то существует такой $x_i \in G$, что p не делит $|G|/|St(x_i)|$. Но $|St(x_i)| < |G|$, так как $x_i \notin Z(G)$, поэтому можно применить индукцию. Очевидно, что p^n делит $|St(x_i)|$. Так как p не делит $|G|/|St(x_i)|$, то существует $H \subset St(x_i)$, такая что $|H| = p^n$ поэтому H — силовская подгруппа.

Задача 13.11. Решение. Так как $\mathrm{char}\, K = 0$, то f — сепарабельный неприводимый многочлен и $Gal(f)$ действует на корнях $f(x)$ транзитивно по 12.9 а). По 8,5.6 любой $g \in Gal(f)$ переводит

корень $f(x)$ в корень $f(x)$ и разные корни переводит в разные корни, так как g — автоморфизм. Заметим, что $K(f) = K(a_1, ..., a_n)$, где $n = \deg f(x)$, $a_1, ..., a_n$ — корни $f(x)$, т.е. любой автоморфизм однозначно определяется действием на $\{a_1, ..., a_n\}$. Значит, мы построили вложение $Gal(f)$ в S_n.

Задача 13.12. Решение. а) Теми же рассуждениями, что и ниже в 13.12 б), находим в S_5 две перестановки $\sigma = (1, 2)$ и $\tau = (1, 2, 3, 4, 5)$ второго и пятого порядков. Но $\operatorname{ord}\sigma\tau = 4$, $\operatorname{ord}\sigma\tau^2 = 6$, поэтому G должна содержать минимум 60 элементов по теореме Лагранжа. $|S_5| = 120$, значит $G \triangleleft S_5$ как группа индекса 2, см. 4.4 б) и $S_5/G \cong \mathbb{Z}_2$ коммутативна, поэтому $(S_5)' \subset G$ по 7,25.4. Но в G есть нечетная транспозиция $(1, 2)$, $(S_5)' = A_5$, поэтому $G = S_5$.

б) Рассмотрим действие G на $\{1, 2, ..., p\}$. Так как действие транзитивно, то есть только одна орбита длины p, поэтому $|G| = p|St(x_0)|$, $x_0 \in \{1, 2, \dots, p\}$, по 5.8. Значит, по теореме Силова 13.10 в G есть силовская из p элементов и порядки всех ее неединичных элементов равны p. Поскольку p — простое число, порядок p может иметь только цикл длины p. Напомним, что любую перестановку можно разложить в произведение независимых циклов, см. 0.4 а), ее порядок равен НОК длин этих циклов, 0.10 б). Пусть τ_0 — образующая этой силовской подгруппы.

Для удобства будем считать, что в G есть транспозиция (12). Заметим, что существует такая степень k, $k \in \{1, \dots, p-1\}$, что $\tau_0^k(1) = 2$. Действительно, можно представить, что числа $i_1, i_2, \dots, i_p$ стоят по кругу, а цикл τ_0 — это просто поворот круга на $360/p$ градусов, цикл в квадрате — это два таких поворота и т.д. Поскольку среди чисел есть число 2, после нескольких поворотов число 1 доберется до него. Переобозначив элементы множества $\{1, 2, \dots, p\}$, без ограничения общности будем считать, что в группе G есть транспозиция $\sigma = (12)$ и цикл $\tau = \tau_0^k = (1, 2, \dots, p)$. Имея σ и τ, мы можем получить любую перестановку из S_p, см. 0.4 д).

Задача 13.13. Решение. По 13.11 $Gal(f) \subset S_p$, по 12.9 а) $Gal(f)$ действует на корнях $\{a_1, ..., a_p\}$ $\cong \{1, 2, ..., p\}$ транзитивно. Комплексное сопряжение будет перестановкой невещественных корней (остальные корни останутся на месте), а значит, транспозицией. Применим 13.12 б) и получим, что $Gal(f) \cong S_p$.

Задача 13.14. Решение. Методами математического анализа можно установить, что многочлен $f(x) = x^5 - 10x + 5$ имеет ровно три действительных корня на отрезке $[-2, 2]$. За пределами отрезка функция $y = f(x)$ уходит на $\pm\infty$. Имеем: $f(-2) = -7$, $f(0) = 5$, $f(1) = -4$, $f(2) = 17$, $f'(x) = 4x^4 - 10 < 0 \Leftrightarrow |x| < \sqrt[4]{2,5} < 1,26$. Отсюда следует существование ровно трех вещественных корней на указанном отрезке. Остальные два комплексных корня комплексно сопряжены, поэтому, по 13.13 $Gal(f) \cong S_5$, а значит, f неразрешим в радикалах. Неприводимость $f(x)$ следует из критерия Эйзенштейна, см. 7,5.6,5.

Листок 14.

Задача 14.1. Решение. В $\mathbb{R}^2$ прямые описываются уравнениями 1-й степени, а окружности — 2-й. Значит, их пересечение будет описываться или рациональным выражением от исходных точек, или через квадратные радикалы. Есть также процедура выбора точки в определенной области, но так как $\mathbb{Q}^2$ всюду плотно в $\mathbb{R}^2$, то точку можно выбрать с рациональными координатами.

Задача 14.3. Указание. См. решение следующей задачи.

Задача 14.4. **Решение.** Очевидно, что если $[K : M] = 2$, тогда если $\deg\mu_\alpha = 2$, то $\mu_\alpha = x^2 + px + q$ не имеет корней в M. Поэтому $\sqrt{D} = x_1 - x_2$, где x_1, x_2 — корни μ_α в M. Т.е. $K = M(\sqrt{D})$ — радикальное расширение Галуа. Нормальность следует из 10.10 а), сепарабельность поля нулевой характеристики — из 11.12. Вспомним доказательство 13.1. Первый шаг индукции очевиден из предыдущих рассуждений. В базе индукции потребуем, чтобы $[E_{i-1} : P] = 2^l$, где $l \in \mathbb{N}$ или $l = 0$. Так как $[P_i : P_{i-1}] = 2$, то $P_i = P_{i-1}(\sqrt{c_i})$ и $\mu_{c_i}^p = (x - c_i)(x - c_i')(x - c_i'')$.... Значит $f(x) = (x^2 - c_i)(x^2 - c_i')(x^2 - c_i'')$..., так как $P \subset P(\mu_z)$ нормально как поле разложения (по 10.7) и $E_i = E_{i-1}(f(x))$ получается путем последовательного присоединения квадратных корней из $c_1, c_1', c_1'', ...$ На каждом этапе присоединения мы получаем степень расширения 2 или 1. Значит, на последнем

этапе $E_n \supset P_n$ мы получаем $L = E_n$ — радикальное расширение Галуа над P, $[L : P] = 2^k$, для некоторого $k = 0, 1, 2, ...$

Задача 14.5. Решение. $\Rightarrow$ Если число z можно построить с помощью циркуля и линейки из отмеченных точек $z_1, ..., z_n$, то согласно 14.1 оно лежит в башне квадратичных расширений над $P = \mathbb{Q}(z_1, ..., z_n)$, $P = P_0 \subset P_1 \subset \ldots \subset P_n$. По 14.4 построим $L \supset P$ — радикальное расширение Галуа с 2-группой $Gal(L/P)$. $z \in P_n \subset L$, поэтому μ_z разлагается в L на линейные множители, значит $P \subset P(\mu_z) \subset L$, и все расширения — расширения Галуа, так как $\operatorname{char} P = 0$, см. 11.12; $P \subset P(\mu_z)$ — поле разложения, см. 12.2, $P \subset L$ по 14.4, $P(\mu_z) \subset L$. Тогда по 12.6 в) $Gal(\mu_z)$ — фактор-группа 2-группы $Gal(L/P)$ и значит, тоже 2-группа.

$\Leftarrow$ Пусть $Gal(\mu_z)$ — 2-группа. Значит, по 7,25.16 она разрешима и согласно 13.7 для $Gal(\mu_z)$ существует композиционный ряд $Gal(\mu_z) = H_0 \triangleright H_1 \triangleright H_2 \triangleright ... \triangleright H_s = \{id\}$, где $H_{i-1}/H_i \cong \mathbb{Z}_2$. Но по 12.6 этому ряду соответствуют цепочка квадратичных расширений полей над $P = \mathbb{Q}(z_1, ..., z_n)$. Тогда по 14.2 мы умеем строить z.

Задача 14.6. Решение. Построение правильного n-угольника эквивалентно построению первообразного корня ξ степени n из 1. По 7,5.14 $\mu_\xi = \Phi_n(x)$, где $\deg \Phi_n(x) = \varphi(n)$ см. 7,5.8. Значит $\varphi(n) = 2^k$, по 14.5.

Задача 14.7. Решение. а) Согласно 11.3 г) $G = Gal(x^n - 1) \cong (\mathbb{Z}_n)^*$ — группа обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$. При $n = 5$, очевидно, $(\mathbb{Z}_5)^* = \mathbb{Z}_4 = \langle 3 \rangle$. В $\mathbb{Z}_4$ есть только одна циклическая подгруппа порядка 2. Очевидно, что комплексное снаряжение — образующий подгруппы 2-го порядка. Пусть $\xi = \cos(2\pi/5) + i \sin(2\pi/5)$ — первообразный корень. Рассмотрим $\alpha = \xi + \overline{\xi}$. Очевидно, что $\overline{\alpha} = \alpha$, поэтому $\mathbb{Q}(\alpha)$ остается на месте при сопряжении и $\mathbb{Q}(\alpha)$ не содержит $\mathbb{Q}(\xi)$, так как $\alpha \in \mathbb{R}$. Найдем μ_α. ξ — корень многочлена $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, $\xi^5 = 1$. Заметим, что $\overline{\xi} = \xi^4 = 1/\xi$. Тогда $\alpha^2 = (\xi + \xi^4)^2 = \xi^2 + \xi^3 + 2$. Так как $\Phi_5(\xi) = 0$, то $\alpha^2 + \alpha - 1 = 0$, значит, $\alpha = (\pm\sqrt{5} - 1)/2$. Но $\alpha = 2\cos(2\pi/5)$, тогда $\cos(2\pi/5) = (\sqrt{5} - 1)/4$. Построение этого числа с помощью циркуля и линейки очевидно.

Задача 14.8. Решение. Дано: $2^k + 1$ — простое число. Пусть $s \neq 1$ — нечетное и $s|k$, т.е. $k = st$. Тогда $2^t \equiv -1 \,(\mathrm{mod}(2^t + 1))$, поэтому $2^{ts} \equiv -1 \,(\mathrm{mod}(2^t + 1))$, значит, $2^{ts} + 1 \equiv 0 \,(\mathrm{mod}(2^t + 1))$ и тогда $2^k + 1$ — составное число. Итак, $k = 2^l$.

Задача 14.9. Решение. При $k = 0, 1, 2, 3, 4$ получаем $M = 3, 5, 17, 257, 65537$ — простые числа. Но при $k = 5$ имеем $641|(2^{32} + 1)$. Остальные простые числа пока не найдены.

Задача 14.10. Решение. По 14.6 $\varphi(n) = 2^k$. Пусть $n = p_1^{k_1} \cdot ... \cdot p_r^{k_r}$. Тогда $\varphi(n) = p_1^{k_1 - 1}(p_1 - 1) \cdot ... \cdot p_r^{k_r - 1}(p_r - 1)$. По основной теореме арифметики все сомножители — степени двойки. Тогда или $p_i = 2$, или $k_1 = 1$ и $p_i = 2^{2^k} + 1$ (по 14.8), поэтому $n = 2^s p_1 ... p_l$, где p_i — простые числа Ферма.

Задача 14.11. Решение. Многочлен $4x^3 - 3x - \alpha$ можно рассматривать как элемент $(\mathbb{Z}[\alpha])[x]$, $(\mathbb{Z}[x])[\alpha]$ или $\mathbb{Z}[\alpha, x]$. Лемма Гаусса 7,5.5 и факториальность 7,5.6 работают. Как многочлен от α над $\mathbb{Z}[x]$ он линейный со старшим коэффициентом -1 и свободным членом $4x^3 - 3x$. Неприводимость очевидна.

Задача 14.12. Решение. Имеем $\cos 3\varphi = 4\cos^3 \varphi - 3\cos \varphi$. Если $\alpha = \cos 3\varphi$ и $x = \cos \varphi$, то $4x^3 - 3x - \alpha = 0$. Надо решить это уравнение в квадратных радикалах, тем самым мы сможем построить $\cos \varphi$ при помощи циркуля и линейки. В общем случае оно неразрешимо по 14.11, поэтому присоединение решения уравнения будет расширением третьей степени, что противоречит 14.5. Полагаем $z_1 = \cos 3\varphi$, тогда присоединение решений даст группу Галуа, порядок которой делится на 3. Противоречие.

Задача 14.13. Решение. $\alpha = \cos 3\varphi = \cos 2\pi/3$, поэтому уравнение трисекции угла будет таким: $8x^3 + 6x - 1 = 0$. По 7,5.1 кандидатами на рациональные корни могут быть только $\pm 1, \pm 1/2, \pm 1/4, \pm 1/8$. Так как ни один из них не подходит, то многочлен неприводим над $\mathbb{Q}$, а значит, по 14.5 его решение не выражается в квадратных радикалах.

Задача 14.14. Решение. Пусть $\xi = e^{i\varphi}$. Очевидно, что $\theta = e^{i\varphi/3}$ должен лежать в квадратичном расширении над $\mathbb{Q}(\xi)$, по 14.5. $\mu_\theta | (x^3 - \xi)$ (минимальный многочлен делит аннулирующий). Значит, по 14.5, многочлен $x^3 - \xi$ не может быть неприводимым. Тогда у него есть корень в $\mathbb{Q}(\xi)$. Тогда ξ является кубом в $\mathbb{Q}(\xi)$. Обратно, пусть ξ является кубом в $\mathbb{Q}(\xi)$. Тогда существует $\tau \in \mathbb{Q}(\xi)$, такое что $\tau^3 = \xi$. Значит, многочлен $x^3 - \xi$ разложим, поэтому θ лежит в $\mathbb{Q}(\xi)$ или в его квадратичном расширении, т.е. построимо над $\mathbb{Q}(\xi)$ по 14.5.

Задача 14.15. Решение. Рассмотрим башню $\mathbb{Q} \subset \mathbb{Q}(e^{i2\pi/n}) \subset \mathbb{Q}(e^{i2\pi/3n})$. По 10.4 ж) $[\mathbb{Q}(e^{i2\pi/n}) : \mathbb{Q}] = \varphi(n)$. Заметим, что $\varphi(3n) = 3\varphi(n)$, если $3|n$, и $\varphi(3n) = 2\varphi(n)$, если $(3, n) = 1$. Это легко следует из разложения n по степеням простых чисел. Значит, $[\mathbb{Q}(e^{i2\pi/3n}) : \mathbb{Q}(e^{i2\pi/n})] = 2$ или 3 по 9.13. Тогда по 14.5 $(n, 3) = 1$ титтк $e^{i2\pi/n}$ допускает трисекцию.

Задача 14.16. Решение. Имеем: $\cos 3^\circ = \frac{1}{8}(\sqrt{3}+1)\sqrt{5+\sqrt{5}} + \frac{1}{16}(\sqrt{6}-\sqrt{2})(\sqrt{5}-1)$. Это получается так. Из 14.7 а) мы знаем $\cos 72^\circ = \sin 18^\circ$. Тогда $\cos 18^\circ = \frac{1}{4}\sqrt{10+2\sqrt{5}}$. Из $\cos 30^\circ$ делением пополам получаем $\cos 15^\circ = \sqrt{1-(2-\sqrt{3})/4}$. И наконец, вычисляем $\cos 3^\circ = \cos(18^\circ - 15^\circ)$.

Задача 14.17. Решение. Построение грани куба объемом 2 — это построение отрезка $\sqrt[3]{2}$. Имеем $\deg \mu_{\sqrt[3]{2}} = 3$, так как $x^3 - 2$ неприводим по критерию Эйзенштейна, задача 7,5.6,5. Поэтому по 14.5 этот отрезок не построим.

Задача 14.18. Решение. Построить сторону квадрата, равновеликого кругу радиуса 1, — это значит, построить отрезок $\sqrt{\pi}$. Тогда по 14.5 число $\sqrt{\pi}$ должно быть алгебраическим над $\mathbb{Q}$, значит, и π должно быть алгебраическим над $\mathbb{Q}$, так как $A = \overline{\mathbb{Q}}$ — поле. Получили противоречие с транцендентностью π (доказана Линдеманом в 1882 г.).

Листок 15.

Задача 15.1. Решение. а), б) легко получаются методами математического анализа.

в) Пусть $[P : \mathbb{C}] = 2$, тогда, для любого $\alpha \in P$ $\deg \mu_\alpha = 2$ или 1. Но $x^2 + px + q = (x-a)^2 - b^2$, где $a, b \in \mathbb{C}$, поэтому $\deg \mu_\alpha = 1$ для любого α.

г) Так как $[\mathbb{C} : \mathbb{R}] = 2$, а 2 — простое число, то по 9.13 не существует промежуточных полей между $\mathbb{R}$ и $\mathbb{C}$. Пусть $[P : \mathbb{R}] = 2$, $\alpha \in P \setminus \mathbb{R}$, $\deg \mu_\alpha = 2$. По 15.1 б) многочлен μ_α разлагается в $\mathbb{C}$ на линейные множители, т.е. $\mathbb{R} \subset \mathbb{R}(\mu_\alpha) \subset \mathbb{C}$. Имеем $P = \mathbb{R}(\alpha) = \mathbb{R}(\mu_\alpha)$, очевидно из 9.13 и 9.15. Значит, $P = \mathbb{R}(\alpha) = \mathbb{R}(\mu_\alpha) = \mathbb{C}$.

Задача 15.2. Решение. Пусть $[K : \mathbb{R}] = 2k+1$, где $k = 0, 1, 2, ...$ Пусть $\alpha \in K$, тогда $\deg \mu_\alpha = 2l$ по 15.1 а), поэтому $\mathbb{R} \subset \mathbb{R}(\alpha) \subset K$. Значит, по теореме о башне полей $[K : \mathbb{R}]$ кратно 2. Получили противоречие, поэтому $K = \mathbb{R}$.

Задача 15.3. Решение. Пусть $g = f\overline{f}$. Так как $\overline{g} = g$, то $g \in \mathbb{R}[x]$. Если c — корень g, то $\overline{c}$ — тоже корень g, так как $g \in \mathbb{R}[x]$. Но c также корень f или $\overline{f}$, поэтому $\overline{c}$ — тоже корень $\overline{f}$ или f.

Задача 15.4. Решение. Пусть $f(x) \in \mathbb{C}[x]$. Рассмотрим $g(x) = f(x)\overline{f(x)} \in \mathbb{R}[x]$. По 15.3 достаточно показать, что g имеет корень в $\mathbb{C}$. Рассмотрим $\mathbb{R}(g)$. Тогда $\mathbb{R} \subset \mathbb{R}(g)$ — расширение Галуа по 12.2. При этом $|Gal(g)| = [\mathbb{R}(g) : \mathbb{R}]$. По 15.2 $|Gal(g)| = 1$ или 2 делит $|Gal(g)|$. В первом случае корень g уже найден. Во втором рассмотрим H — силовскую 2-группу в $Gal(g)$ и воспользуемся ОТТГ 12.6. Пусть $K = \mathbb{R}(g)^H$, имеем $\mathbb{R} \subset K \subset \mathbb{R}(g)$, где $[\mathbb{R}(g) : K] = |H| = 2^l$. $[K : \mathbb{R}]$ нечетно по теореме Силова 13.10. Но по 15.2 $K = \mathbb{R}$, поэтому $Gal(g)$ — 2-группа, а значит, она разрешима, см. 7,25.16. Тогда по 13.7 существует композиционный ряд для $G = Gal(g)$: $G = H_0 \triangleright H_1 \triangleright H_2 \triangleright ... \triangleright H_s = \{e\}$, где $H_{i-1}/H_i \cong \mathbb{Z}_2$. Снова применяем ОТТГ 12.6. Если $\mathbb{R}(g) \neq \mathbb{R}$, то квадратичное расширение $\mathbb{R}$ изоморфно $\mathbb{C}$ по 15.1 г), а квадратичное расширение $\mathbb{C}$ изоморфно $\mathbb{C}$ по 15.1 в). Значит, $\mathbb{R}(g)$ — это $\mathbb{R}$ или $\mathbb{C}$, теорема доказана.

Задача 15.5. Указание. Для многочлена $x^3 + ax^2 + bx + c$ сделайте замену переменной $x = y - a/3$.

Задача 15.6. Решение. $D = \prod\limits_{i<j}(x_i - x_j)^2 = -4\sigma_2^3 - 27\sigma_3^2$ по теореме о симметрических многочленах, поэтому $D(f) = -4p^3 - 27q^2$. Так как $\sqrt{D} = \prod\limits_{i<j}(x_i - x_j)$, а любая перестановка — произведение инверсий, причем каждая инверсия меняет знак $\sqrt{D}$, то $\sqrt{D}$ инвариантен относительно A_3.

Задача 15.7. Решение. Имеем: $r_1^3(x_1) = (x_1 + \rho x_2 + \rho^2 x_3)^3 =$

$x_1^3 + x_2^3 + x_3^3 + 3(\rho x_1^2 x_2 + \rho^2 x_1 x_2^2 + \rho^2 x_1^2 x_3 + \rho x_1 x_3^2 +$

$\rho x_2^2 x_3 + \rho^2 x_2 x_3^2) + 6x_1x_2x_3 =$

$(x_1^3 + x_2^3 + x_3^3) + 3\frac{-1+\sqrt{-3}}{2}(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) +$

$3\frac{-1-\sqrt{-3}}{2}(x_1 x_2^2 + x_2 x_3^2 + x_3 x_1^2) + 6x_1x_2x_3 =$

$(x_1^3 + x_2^3 + x_3^3) - \frac{3}{2}\sum\limits_{i\neq j} x_i^2 x^j + 6x_1x_2x_3 - \frac{3}{2}\sqrt{-3}\sqrt{D}.$

Выражаем симметрические многочлены через элементарные симметрические многочлены методом неопределенных коэффициентов, получаем:

$x_1^3 + x_2^3 + x_3^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3,$

$\sum\limits_{i\neq j} x_i^2 x^j = \sigma_1\sigma_2 - 3\sigma_3,$

$x_1x_2x_3 = \sigma_3$. Учитывая, что $\sigma_1(x_1, x_2, x_3) = 0$, $\sigma_2(x_1, x_2, x_3) = p$, $\sigma_3(x_1, x_2, x_3) = -q$ по теореме Виета, получаем: $r_1^3(x_1) = -(27/2)q + (3/2)\sqrt{-3}\sqrt{D}$.

Аналогично $r_2^3(x_1) = -(27/2)q - (3/2)\sqrt{-3}\sqrt{D}$.

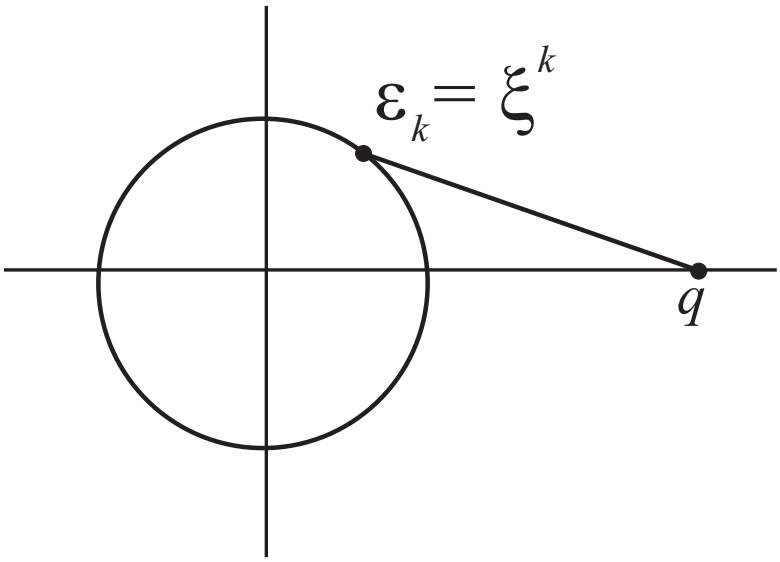
Задача 15.8. Решение. Имеем: $r_1(x_1)r_2(x_1) = (x_1^2 + x_2^2 + x_3^2) + (\rho + \rho^2)x_1x_2 + (\rho + \rho^2)x_1x_3 + (\rho + \rho^2)x_2x_3 = (x_1^2 + x_2^2 + x_3^2) - (x_1x_2 + x_1x_3 + x_2x_3) = \sigma_1^2 - 3\sigma_2 = -3p$. Мы использовали, что $\rho + \rho^2 = -1$, так как это корни многочлена $x^2 + x + 1$, а также теорему Виета и разложение на элементарные симметрические многочлены.

Задача 15.9. Решение. Запишем очевидные равенства

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1 + \rho x_2 + \rho^2 x_3 = r_1(x_1) \\ x_1 + \rho^2 x_2 + \rho x_3 = r_2(x_1) \end{cases} \tag{1}$$

Сложив эти равенства, получим: $3x_1 = r_1(x_1) + r_2(x_1)$. Заметим, что, как в предыдущей задаче, $\rho + \rho^2 = -1$. Теперь домножим соотношения (1) построчно на $1, \rho^2, \rho$ и сложим. Получим $3x_2 = \rho^2 r_1(x_1) + \rho r_2(x_2)$. Аналогично, если домножить (1) построчно на $1, \rho, \rho^2$ и сложить, получим $3x_3 = \rho r_1(x_1) + \rho^2 r_2(x_1)$.

Задача 15.11. Решение.



Так как $\Phi_n(q)|(q-1)$, то $|\Phi_n(q)| \leq |q-1|$.

Имеем: $|\Phi_n(q)| = \prod\limits_{(k,n)=1} |q - \xi^k|$, где ξ — первообразный корень степени n из 1. Очевидно, что равенство модулей, см. рисунок, будет только при $n = 1$.

Задача 15.12. Решение. Пусть D — тело, $|D| < \infty$. Положим $F = Z(D)$ — центр D — поле. Пусть размерность или степень расширения $[D : F] = n$.

Доказываем индукцией по n. База $n = 1$ — утверждение очевидно.

Пусть $|F| = q$, D^* — мультипликативная группа, т.е. D без нуля, F^* — центр D^*. Заметим, что $|D| = q^n$, где $q = |D|$. Это доказывается так же, как в случае конечных полей, см. 10.11.

Подействуем на D^* сопряжением. Запишем формулу классов, см. 5.8: $|D^*| = |Z(D^*)| + \sum\limits_{i=1}^{s} \frac{|D^*|}{|ST(x_i)|}$ или, по-другому $q^n - 1 = (q-1) + \sum\limits_{i=1}^{s} \frac{q^n-1}{|St(x_i)|}$. Заметим, что стабилизатор при действии сопряжением называется централизатором $C(x_i) = \{y \in D^* : x_i y = y x_i\}$.

Рассмотрим $S(x_i) = St(x_i) + \{0\}$. Очевидно, что это тело и линейное пространство над F, и так как $x_i \notin F$, то $d_i = \dim_F S(x_i) < n = \dim_F D$, поэтому $S(x_i)$ — поле по индукционному предположению. Тогда D — линейное пространство над $S(x_i)$ и $|D| = |S(x_i)|^{k_i}$, аналогично 10.11.

Аналогично и $|S(x_i)| = q^{d_i}$, поэтому $n = k_i d_i$, а значит, формула классов выглядит так: $q^n - 1 = (q-1) + \sum\limits_{i=1}^{s} \frac{q^n-1}{q^{d_i}-1}$. По 7,5.10 и 7,5.12, примененных к $x = q$, имеем: $q^n - 1 = \prod\limits_{d|n} \Phi_d(q)$ и $q^n - 1 = (q^d - 1)\Phi_n(q)h_q(q)$ для любых $d|n$ и $h_d(x) \in \mathbb{Z}[x]$. т.е. $\Phi_n(q)|q^n - 1$, $\Phi_n(q)|\frac{q^n-1}{q^{d_i}-1}$ для всех $d_i|n$. Применим это свойство к формуле классов и получим, что $\Phi_n(q)|(q-1)$, тогда $n = 1$ по 15.11.

Листок 16.

Задача 16.1. Решение. Если $m = n$ в $\mathbb{Z}_p$, то $p^n|(m-n)$ для любого $n \in \mathbb{N}$, поэтому $m = n$.

Задача 16.2. Решение. Очевидно, что если $0 \leq x_n < p^{n+1}$ и $0 \leq x'_n < p^{n+1}$ для любого $n > 0$, а также $(x_n - x'_n)|p^{n+1}$ для любого $n > 0$, то $x_n = x'_n$ для любого $n > 0$.

Задача 16.3. Решение. Рассмотрим каноническую запись $\{x_0, x_1, x_2, ...\}$ по 16.2. По определению 16.1 $x_{n+1} \equiv x_n (\mathrm{mod}\, p^n)$, поэтому $x_{n+1} - x_n = a_{n+1}p^{n+1}$. По определению 16.2 имеем $0 \leq x_{n+1} < p^{n+2}$ и $0 \leq x_n < p^{n+1}$. Значит, $0 \leq a_n < p$ для любого $n \geq 0$. Очевидно, что любая такая запись будет канонической записью целого p-адического числа.

Задача 16.4. Решение. Рассмотрим отрезок $[0, 1]$ и запишем произвольное число в p-ичной системе счисления. Каждому числу $0, a_0 a_1 a_2 ...$, где $0 \leq a_i < p$, поставим в соответствие целое

p-адическое число $\{a_0, a_0 + a_1p, a_0 + a_1p + a_2p^2, ...\}$. Склейки-неоднозначности вида $0, a_0a_1a_2...a_n\ p-1\,p-1\,p-1...$ при p-ичном представлении чисел отрезка можно проигнорировать, так как они соответствуют рациональным числам и их счетное количество, поэтому $\mathbb{Z}_p$ имеет такую же мощность, как отрезок, т.е. континуум.

Задача 16.5. Решение. Следует из определения (можно применить индукцию).

Задача 16.6. Решение. Пусть $\alpha = \{x_0, x_1, ...\}$ обратим, тогда существует такой $\beta = \{y_0, y_1, ...\}$, что $\alpha\beta = 1$. Тогда $x_0y_0 \equiv 1(\mathrm{mod}\, p)$, поэтому $x_0 \not\equiv (\mathrm{mod}\, p)$.

Обратно, пусть $x_0 \not\equiv 0(\mathrm{mod}\, p)$. Тогда найдется такой y_0, что $x_0y_0 \equiv 1(\mathrm{mod}\, p)$, так как $\mathbb{Z}/p\mathbb{Z}$ — поле. Из определения 16.1 следует, что $x_n \equiv x_{n-1} \equiv ... \equiv x_0(\mathrm{mod}\, p)$, тогда $x_0 \not\equiv 0(\mathrm{mod}\, p)$, поэтому $x_n \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^*$ и значит, найдется такой $y_n \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^*$, что $x_ny_n \equiv 1(\mathrm{mod}\, p^{n+1})$ для любого $n \geq 0$. Так как по определению 16.1 $x_n \equiv x_{n-1}(\mathrm{mod}\, p^n)$, $x_ny_n \equiv x_{n-1}y_{n-1}(\mathrm{mod}\, p^n)$, то $y_n \equiv y_{n-1}(\mathrm{mod}\, p^n)$, поскольку можно сокращать равенства в $(\mathbb{Z}/p^n\mathbb{Z})^*$ $(ab = ac \Rightarrow b = c)$. Поэтому последовательность $\{y_0, y_1, ...y_n, ...\}$ определяет целое p-адическое число β, такое что $\alpha\beta = 1$. По-другому: сравнения можно сокращать на числа, взаимно простые с модулем, так как если $a|bc$ и $(a, b) = 1$, то $a|c$.

Задача 16.7. Решение. Пусть $\alpha \in \mathbb{Z}_p$ и $\alpha = \{a_0, ...a_n, ...\}$, $a_i \in \mathbb{Z}$ — каноническая запись. Если $a_0 \neq 0$, то α — делитель единицы по 16.6 и тогда $\alpha = p^0\alpha$. Если $a_i = 0$ для всех i, то $\alpha = 0$, иначе найдется такое минимальное m, что $a_m \neq 0(\mathrm{mod}\, p^{m+1})$. Тогда при всех $s \geq 0$ имеем $a_{m+s} \equiv a_{m-1} \equiv 0(\mathrm{mod}\, p^m)$, поэтому число $b_s = a_{m+s}/p^m \in \mathbb{Z}$. Так как $p^mb_s - p^mb_{s-1} = a_{m+s} - a_{m+s-1} \equiv 0(\mathrm{mod}\, p^{m+s})$, то $b_s \equiv b_{s-1}(\mathrm{mod}\, p^s)$ для всех $s \geq 1$. Значит, последовательность $\{b_s\}$ определяет число $\varepsilon \in \mathbb{Z}_p^*$ по 16.6, так как $b_0 = a_m/p^m \not\equiv 0(\mathrm{mod}\, p)$, то $\alpha = p^m\varepsilon$.

Докажем единственность. От противного: пусть $\alpha = p^m\varepsilon$ и $\alpha = p^kh$, где $\varepsilon, h \in \mathbb{Z}_p^*$, $k \geq 0$. Если последовательность z_s определяет число h, то $p^mb_i \equiv p^kz_s(\mathrm{mod}\, p^{s+1})$ для любого $s \geq 0$, так как это запись числа α: $\{a_i\}$ определяет α и $\{p^kz_s\}$ определяет α. Причем по 16.6 $p \nmid b_s$ и $p \nmid z_s$ для всех $s \geq 0$. При $s = m$ получаем $p^mb_m \equiv p^kz^m \not\equiv 0(\mathrm{mod}\, p^{m+1})$, откуда следует неравенство $k \leq m$. Поменяем k и m местами и получим $k \geq m$, поэтому $k = m$. Тогда $p^mb_s \equiv p^mz_s(\mathrm{mod}\, p^{s+1})$ для всех $s \geq 0$. Заменим s на $s + m$ и сократим сравнение на p^m. Получаем $b_{s+m} \equiv z_{s+m}(\mathrm{mod}\, p^{s+1})$. Но $b_{s+m} \equiv b_s(\mathrm{mod}\, p^{s+1})$ и $z_{s+m} \equiv z_s(\mathrm{mod}\, p^{s+1})$, так как это записи p-адических чисел ε и h. Значит, $b_s \equiv z_s(\mathrm{mod}\, p^{s+1})$ для всех $s \geq 0$ и тогда $\varepsilon = h$.

Задача 16.8. Решение. а) Следует из 16.7.

б) Пусть $\alpha = p^m\varepsilon$, $\beta = p^kh$ по 16.7. Пусть $m > k$. Положим m в качестве евклидовой нормы N. Имеем $\alpha = \beta p^{m-k}(\varepsilon/h) + 0$, $\beta = 0 \cdot \alpha + \beta$, причем $N(\beta) < N(\alpha)$. Также $N(\alpha\beta) \geq N(\alpha)$, значит, $\mathbb{Z}_p$ — евклидово кольцо.

в) По 16.7 для любого $\alpha \neq 0$ имеем $\alpha = p^m\varepsilon$, где ε обратим. Значит, p — единственный простой элемент в $\mathbb{Z}_p$, а (p) — единственный максимальный идеал в $\mathbb{Z}_p$, т.е. $\mathbb{Z}_p$ — локальное кольцо (область целостности с единственным максимальным идеалом).

Задача 16.9. Решение. Утверждения а), б), г) очевидны.

в) Пусть $\alpha = p^m\varepsilon$, $\beta = p^kh$. Если $m > k$, то $\alpha + \beta = p^k(p^{m-k}\varepsilon + h)$. Так как $m - k > 0$, то первый член $p^{m-k}\varepsilon$ делит p. Но первый член h не делится на p, поэтому, по 16.6, $p^{m-k}\varepsilon + h$ обратим, а значит, $\nu(\alpha + \beta) = k$, так как, опять по 16.7, представление единственно.

Задача 16.10. Решение. Рассмотрим гомоморфизм редукции $\varphi : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$. Для любого $\alpha \in \mathbb{Z}_p$ имеем $\alpha = \alpha_0 + \alpha_1p + \alpha_2p^2 + ... + \alpha_{n-1}p^{n-1} + p^nz$, где $0 < \alpha_i \leq p-1\ \forall\, i$, $z \in \mathbb{Z}_p$. Положим $\varphi(\alpha) = \alpha_0 + \alpha_1p + \alpha_2p^2 + ... + \alpha_{n-1}p^{n-1} \in \mathbb{Z}/p^n\mathbb{Z}$. Очевидно, что определение корректно и φ — эпиморфизм. Его ядро — это идеал в $\mathbb{Z}_p$, а все идеалы — это $(p), (p^2), ..., (p^n)$. Ясно, что тогда $\mathrm{Ker}\,\varphi = (p^n)$ и результат получается по теореме о гомоморфизме для колец.

Задача 16.11. Решение. а) Формулировка: Пусть $f(x) \in \mathbb{Z}_p[x]$ и $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n$, причем $p|a_0$, $p|a_i$ для всех $i \in \{1, ..., n\}$, $p^2 \nmid a_n$. Тогда $f(x)$ неприводим в $\mathbb{Q}_p[X]$.

Доказательство. Аналогично задаче 7,5.6,5, поскольку кольцо $\mathbb{Z}_p$ евклидово и p — единственный простой элемент.

б) По пункту а) многочлен $f(x) = x^n - p$ неприводим при любом простом p. Присоединим к $\mathbb{Q}_p$ корень $f(x)$ и получим расширение степени n.

Задача 16.12. Решение. $\Rightarrow$ Так как $1 \cdot 1 = 1$, то $|1 \cdot 1| = |1| \cdot |1| = |1|$, поэтому $|1| = 1$. Тогда $|1 + 1 + ... + 1| \leq \max(|1|, ...|1|) = 1$, по индукции.

$\Leftarrow$ Пусть $|n|$ для любого $n = 1+...+1 \in \mathbb{N}$. Рассмотрим такие x, y, что $|x| \geq |y|$. Имеем $|(x+y)^n| = |x+y|^n$. Но $|(x+y)^n| \leq \sum\limits_{k=0}^{n} |C_n^k||x|^k|y|^{n-k}$. Так как $C_n^k \in \mathbb{N}$, то $|C_n^k| \leq 1$, поэтому $|x+y|^n \leq \sum\limits_{k=0}^{n} |x|^k|y|^{n-k}$. Пусть $M = |x| \geq |y|$. Тогда $|x|^k|y|^{n-k} \leq M^n$, а значит, поскольку у нас $n+1$ слагаемых, $|x+y|^n \leq (n+1)M^n$. Извлечем корень степени n из этого неравенства и получим $|x+y| \leq (n+1)^{1/n}M$. Устремим n к бесконечности, получим $(n+1)^{1/n} \to 1$, поэтому $|x+y| \leq M = \max(|x|, |y|)$, а значит, норма неархимедова.

Задача 16.13. Решение. По определению, $\mathbb{Q}_p = Q(\mathbb{Z}_p)$. По 16.7, для любого $\alpha \in \mathbb{Z}_p$ имеем $\alpha = p^m\varepsilon_1$, где $m = \nu(\alpha)$, $\varepsilon_1 \in \mathbb{Z}_p^*$. Пусть $\beta \in \mathbb{Z}_p$, $\beta = p^n\varepsilon_2$. Очевидно, что класс, в $Q(\mathbb{Z}_p)$, $\{\alpha, \beta\} = \{p^k, z\}$, где $z = \varepsilon_2/\varepsilon_1$, $k = m - n$. Единственность представления следует из единственности представлений α и β, с применением прямых преобразований по определению.

Задача 16.14. Решение. Следует из простой арифметики в $\mathbb{Q}_p$ над числами вида α/p^k, по 16.13.

Задача 16.15. Решение. Следует из 16.9.

Задача 16.16. Решение. а) $\|1 - 26\|_5 = \| - 5^2\|_5 = 5^{-2} = 0,04$.

б) $\|1/9 + 1/16\|_5 = \|(16 + 9)/144\|_5 = 5^2/144 = 5^{-2} = 0,04$.

в) Согласно известной формуле $\nu_p(N!) = [N/p] + [N/p^2] + [N/p^3] + ...$ Значит, $\nu_3(9!) = 3 + 1 = 4$, поэтому $\|(9!)^2/3^9\|_3 = 3^{-(8-9)} = 3$.

г) $\nu_2((2^N)!) = 2^{N-1} + 2^{N-2} + ... + 1 = 2^N - 1$, поэтому $\|2^{2^N}/(2^N)!\|_2 = 2^{-(2^N-(2^N-1))} = 2^{-1} = 0,5$.

Задача 16.17. Решение. Пусть $|x| = p_1^{k_1} \cdot ... \cdot p_n^{k_n}$, где $k_i \in \mathbb{Z}$, p_i — простые. Тогда $\|x\|_{p_i} = p_i^{-k_i}$, если $p_i \in \{p_1, ..., p_n\}$, и $\|x\|_{p_i} = 1$, если $p_i \notin \{p_1, ..., p_n\}$. Поэтому $\prod\limits_{p=2}^{\infty} \|x\|_p = 1$.

Листок 17.

Задача 17.1. Решение. а) Пусть x, y, z — вершины треугольника. Если $|y - x| = |z - y|$, то все доказано. Пусть $|y - x| > |z - y|$, тогда $|z - x| = |(y - x) + (z - y)| \leq \max(|y - x|, |z - y|) = |y - x|$. Но $|y - x| = |(y - z) + (z - x)| \leq \max(|y - z|, |z - x|) = |z - x|$, так как $|y - x| > |z - y| = |y - z|$. Поэтому $|y - x| = |z - x|$ — если две стороны не равны, то третья сторона равна бóльшей из них.

б) Пусть z — центр круга радиуса r, x, y — его точки (может, и граничные), т.е. $|x - z| \leq r$, $|y - z| \leq r$. Тогда $|x - y| = |(x - z) + (y - z)| \leq \max(|x - z|, |z - y|) \leq r$, поэтому ввиду произвольности x, y любая точка круга является его центром.

в) Следует из б).

Задача 17.2. Решение. Если $\alpha \in \mathbb{Z}_p$, то по 16.3 имеем $\alpha = \{a_0, a_0+a_1p, a_0+a_1p+a_2p^2, ...\}$, где $0 \leq a_i < p$ для любого i. Рассмотрим последовательность частичных сумм $\{a_0, a_0+a_1p, a_0+a_1p+a_2p^2, ...\}$ как чисел в $\mathbb{Z}_p$. Очевидно, что $\|\alpha - \sum\limits_{i=0}^{n} a_ip^i\|_p \leq p^{-n-1}$, т.е. $\sum\limits_{i=0}^{n} a_ip^i \to \alpha$.

Задача 17.3. Решение. Пусть $\alpha \in \mathbb{Q}_p$, тогда существуют единственные $m \in \mathbb{Z}$, $\varepsilon \in \mathbb{Z}_p^*$, такие что $\alpha = p^m\varepsilon$ — по 16.13. По 17.2 существует последовательность $\varepsilon_0, \varepsilon_1, \varepsilon_2, ... \to \varepsilon$ в $\mathbb{Z}_p$, поэтому, очевидно, $p^m\varepsilon_0, p^m\varepsilon_1, p^m\varepsilon_2, ... \to \alpha$ в $\mathbb{Q}_p$, причем $p^m\varepsilon_i \in \mathbb{Q}$.

Задача 17.4. Решение. а) Если $\beta_n \in \mathbb{Q}_p$ для любого $n \in \mathbb{N}$ и существует $k \in \mathbb{Z}$, такое что $|\beta_n| < p^k$ для любого $n \in \mathbb{N}$, то $\alpha_k = p^k\beta_n \in \mathbb{Z}_p$ для любого $n \in \mathbb{N}$. Проведем доказательство для последовательности $\{\alpha_n\}$ По 16.10 $|\mathbb{Z}_p/(p)| = p$, поэтому найдется такой $x_0 \in \{0, ..., p-1\}$, что сравнение $\alpha_n \equiv x_0 (\mathrm{mod}\, p)$ имеет бесконечно много решений. Выберем из $\{\alpha_n\}$ эту бесконечную

подпоследовательность решений и назовем ее $\{\alpha_n^{(1)}\}$. Аналогично, из $\{\alpha_n^{(1)}\}$ выбираем бесконечную подпоследовательность $\{\alpha_n^{(2)}\}$, такую что $\alpha_n^{(2)} \equiv x_1 (\mathrm{mod}\, p^2)$, где $x_1 \in \{0, ..., p^2 - 1\}$.

Продолжая, получим $\alpha_n^{(k)} \equiv x_{k-1} (\mathrm{mod}\, p^k)$, где $x_k \in \{0, ..., p^k - 1\}$. Так как $\{\alpha_n^{(k+1)}\} \subset \{\alpha_n^{(k)}\}$ и $x_k \equiv \alpha_n^{(k+1)} (\mathrm{mod}\, p^{k-1})$, то $x_k \equiv x_{k-1} (\mathrm{mod}\, p^k)$ для любого $k \in \mathbb{N}$. Значит, $\{x_n\}$ определяет целое p-адическое число α. Составим диагональную последовательность $\{\alpha_n^n\} \subset \{\alpha_n\}$. Докажем, что $\{\alpha_n^n\} \to \alpha \in \mathbb{Z}_p$. По построению $\alpha \equiv x_{n-1} (\mathrm{mod}\, p^n)$, $\alpha_n^{(n)} \equiv x_{n-1} (\mathrm{mod}\, p^n)$, поэтому $\alpha_n \equiv \alpha (\mathrm{mod}\, p^n)$, а значит, $\alpha_n^{(n)} \to \alpha$ в $\mathbb{Z}_p$. Но тогда $\beta_n \to \alpha / p^k$ в $\mathbb{Q}_p$.

б) $\Leftarrow$. $|\xi_{n+1} - \xi_n| \to 0$, значит, найдется $n_0 \in \mathbb{N}$, такое что для любого $k \geq n_0$ выполнено $|\xi_{k+1} - \xi_k| \leq 1$. Поэтому для любого ξ_k с $k > n_0$ имеем $|\xi_k| = |(\xi_k - \xi_{n_0}) + \xi_{n_0}| = |(\xi_k - \xi_{k-1}) + (\xi_{k-1} - \xi_{k-2}) + ... + (\xi_{n_0+1} - \xi_{n_0}) + \xi_{n_0}| \leq \max(|\xi_k - \xi_{k-1}|, ..., |\xi_{n_0+1} - \xi_{n_0}|, |\xi_{n_0}|) \leq \max(1, |\xi_{n_0}|)$. Значит, последовательность ξ_n ограничена. По пункту а) найдется сходящаяся подпоследовательность $\xi_{n_i} \to \xi$. Пусть $k \in \mathbb{N}$. Тогда найдется такое N, что для любого $n_i > N$ имеем $|\xi_{n_i} - \xi| \leq p^{-k}$ и существует такое M, что для любого $n > M$ будет $|\xi_{n_i} - \xi_n| \leq p^{-k}$. Тогда для любого $n > n_i > \max(N, M)$ получим $|\xi_n - \xi| = |(\xi_n - \xi_{n_i}) + (\xi_{n_i} - \xi)| = |(\xi_n - \xi_{n-1}) + (\xi_{n-1} - \xi_{n-2}) + ... + (\xi_{n_i+1} - \xi_{n_i}) + (\xi_{n_i} - \xi)| \leq p^{-k}$, так как каждое слагаемое $\leq p^{-k}$. Поэтому $\xi_n \to \xi$.

$\Rightarrow$ Последовательность $\xi_i \to A$: по определению это означает, что $|\xi_i - A| < \varepsilon$ для любых $\varepsilon > 0$ и $i > N(\varepsilon)$. Поэтому $|\xi_i - \xi_{i+1}| = |(\xi_i - A) + (A - \xi_{i+1})| \leq \max(|\xi_i - A|, |A - \xi_{i+1}|) < \varepsilon$, так как $i, i+1 > N(\varepsilon)$.

Задача 17.5. Решение. Следует из 17.4 б).

Задача 17.6. Решение. Пусть $\varphi : \mathbb{N} \to \mathbb{N}$ – биекция, т.е. перестановка натурального ряда. По критерию Коши 17.5 $\sum\limits_{n=1}^{\infty} \alpha_n \to A \Leftrightarrow \alpha_n \to 0 \stackrel{\text{def}}{=} \forall\, \varepsilon > 0\ \exists\, N\colon \forall\, i > N\colon |a_i| < \varepsilon$. $\sum\limits_{n=1}^{\infty} a_n \to A \stackrel{\text{def}}{=} A_n \to A$, где $A_n = \sum\limits_{i=1}^{n} a_i$.

Мы хотим доказать, что $|A_n - B_n| \to 0$, где $B_n = \sum\limits_{i=1}^{n} a_{\varphi(i)}$. Очевидно, что $\exists\, k \in \mathbb{N}\colon \{1, 2, \ldots, N\} \subset \{\varphi(1), \varphi(2), \ldots, \varphi(k)\}$.

Очевидно, что $k \geqslant N$. Рассмотрим $|A_k - B_k|$. Слагаемые с номерами $\leqslant N$ в этой сумме взаимно сократятся и останутся только слагаемые с p-адической нормой $< \varepsilon$, а значит и вся сумма будет меньше ε. Значит, $|A_k - B_k| \to 0$ при $k \to \infty \Rightarrow \sum\limits_{i=1}^{\infty} a_{\varphi(i)} \to A$.

Задача 17.7. Решение. Следует из 16.13, 16.6 и 16.3.

Задача 17.8. Решение. Аналогично вещественному случаю, $S_n = 1 + p + \ldots + p^n$, $pS_n = S_n + p^{n+1} - 1 \Rightarrow S_n = \dfrac{p^{n+1} - 1}{p - 1} \Rightarrow S_n \to \dfrac{1}{1 - p}$ при $n \to \infty$ т.к. $p^{n+1} \to 0$.

Задача 17.9. Решение. Т.к. $p \neq 2$, многочлен $x^2 - 2$ сепарабелен в F_p, $(x^2 - 2)' = 2x \not\equiv 0$, поэтому если корни есть, то их два. Или проще: $x_0^2 \equiv 2 \,(\mathrm{mod}\ p) \Rightarrow (-x_0)^2 \equiv 2 \,(\mathrm{mod}\ p)$ и $x_0 \neq -x_0 \,(\mathrm{mod}\ p)$, т.к. $2x_0 \equiv 0 \,(\mathrm{mod}\ p)$, $p \neq 2$. Из мультипликативности метрики если x — корень, то $x \in \mathbb{Z}_p^*$. $x \equiv \pm x_0 \,(\mathrm{mod}\ p)$. $x = x_0 + x_1 p + x_2 p^2 + \ldots \Rightarrow (x_0 + x_1 p)^2 = x_0^2 + x_1^2 p^2 + 2x_0 x_1 p \equiv 2 \,(\mathrm{mod}\ p^2)$, т.к. умножение в $\mathbb{Z}_p$ — почленное.

Как можно заметить, ключевой момент в нахождении $x_1, x_2, x_3, ...$ — это то, что $2x_0 \not\equiv 0 \,(\mathrm{mod}\ p)$ (см. преамбулу к листку 16). В лемме Гензеля 17.11,5 и её доказательстве мы найдём общее объяснение: $f(x) = x^2 - 2$, $f'(x) = 2x$, т.к. мы строим решение рекуррентно, исходя из разложения Тейлора $f(x + h) = f(x) + f'(x)h +$ члены более высокого порядка. $f(x_0) \equiv 0 \,(\mathrm{mod}\ p)$, $f'(x_0) \not\equiv 0 \,(\mathrm{mod}\ p)$ и строим индукционно: $a_n = a_{n-1} + b_n p^n$, где $b_n \in \{0, 1, \ldots, p - 1\}$.

Задача 17.10. Решение. а), б), в). Техника выполнения операций сложения, вычитания, умножения и деления p-адических чисел во многом напоминает соответствующие операции с десятичными дробями, изучаемые в начальной школе. Единственное отличие в том, что «занимание», «перенос

в другой разряд», «умножение столбиком» и т.д. делаются слева направо, а не справа налево. Вот несколько примеров вычислений в $\mathbb{Q}_7$:

$$\begin{array}{rr} & 3+6\times7+2\times7^2+\dots \\ \times & \underline{4+5\times7+1\times7^2+\dots} \\ & 5+4\times7+4\times7^2+\dots \\ & \quad 1\times7+4\times7^2+\dots \\ & \qquad\qquad 3\times7^2+\dots \\ \hline & 5+5\times7+4\times7^2+\dots \end{array} \qquad \begin{array}{rr} & 2\times7^{-1}+0\times7^0+3\times7^1+\dots \\ - & \underline{4\times7^{-1}+6\times7^0+5\times7^1+\dots} \\ & 5\times7^{-1}+0\times7^0+4\times7^1+\dots \end{array}$$

$$\begin{array}{r|l} 1+2\times7+4\times7^2+\dots & 3+5\times7+1\times7^2+\dots \\ \underline{1+6\times7+1\times7^2+\dots} & \hline 5+1\times7+6\times7^2+\dots \\ \quad 3\times7+2\times7^2+\dots & \\ \quad \underline{3\times7+5\times7^2+\dots} & \\ \qquad 4\times7^2+\dots & \\ \qquad \underline{4\times7^2+\dots} & \end{array}$$

г) Надо найти решение уравнения $x^2+1=0$ в $\mathbb{Q}_{13}$, $x_0=5$, $x_0'=8$. Строим решение, как в 17.9. $2\cdot5\not\equiv0\,(\mathrm{mod}\ 13)$, $2\cdot8\not\equiv0\,(\mathrm{mod}\ 13)\Rightarrow$ решение строится рекуррентно:

$x_1=5\cdot13^0+5\cdot13^1+1\cdot13^2+0\cdot13^3$, $x_2=8\cdot13^0+7\cdot13^1+11\cdot13^2+12\cdot13^3$.

Задача 17.11. Решение. Общее указание: a — квадрат в F_p^* титтк $a^{(p-1)/2}=1$, поэтому если $a=b^2$, то $a^{(p-1)/2}=b^{p-1}=1$, так как $|F_p^*|=p-1$.

Действительно, рассмотрим $(F_p^*)^2\subset F_p^*$ — подгруппу квадратов в F_p^*. F_p^* — циклическая по 3.9, поэтому $(F_p^*)^2$ — циклическая и $F_p^*/(F_p^*)^2$ — тоже циклическая. Заметим, что $(F_p^*)^2\neq F_p^*$, так как, из предыдущего, для любого $a\in(F_p^*)^2$ имеем $a^{(p-1)/2}=1$, но для образующих группы F_p^* это неверно: для любого $a\in F_p^*$ $a^2\in(F_p^*)^2$, поэтому $F_p^*/(F_p^*)^2=\{\pm1\}$, так как она циклическая. Значит, квадратов и не квадратов в F_p^* поровну. Для любого $a\in F_p^*$ $a^{(p-1)/2}$ — корень уравнения $x^2=1$, т.е. $a^{(p-1)/2}=\pm1$. Но корней уравнения $x^{(p-1)/2}=1$ не больше, чем $(p-1)/2$, поэтому a — квадрат титтк $a^{(p-1)/2}=1$ для любого $a\in F_p^*$.

1) $p=2$. $x\in\mathbb{Q}_2$, $x^2=-1$. Ясно, что $x\in\mathbb{Z}^*$, т.е. $x=\{1,a_1,a_2,...\}$, где a_1 — нечетно, поэтому $a_2^2=1(\mathrm{mod}\,4)$. Противоречие.

2) $p=3$. $(-1)^{(3-1)/2}=-1$, поэтому в $\mathbb{Q}_3$ не существует $\sqrt{-1}$, согласно указанию: очевидно, для любого p если $x^2=-1$, то $x\in\mathbb{Z}_p^*$, поэтому имеем $x_0^2=-1(\mathrm{mod}\,p)$, где $x=\{x_0,x_1,...\}$, следовательно, $(-1)^{(p-1)/2}=-1$ титтк $x_0^2=-1(\mathrm{mod}\,p)$.

3) $p=5$. $(-1)^{(5-1)/2}=1$, поэтому уравнение $x^2=-1$ разрешимо в F_5^*: его корни $\{2,3\}$. Аналогично преамбуле листка 16, $(2+a_15)^2\equiv1(\mathrm{mod}\,5^2)$ титтк $4+20A_1\equiv-1(\mathrm{mod}\,25)$ титтк $1+4A_1\equiv0(\mathrm{mod}\,5)$ и т.д. Легко доказать (в общем случае это называется леммой Гензеля), что решение можно продолжать до бесконечности, аналогично 17.9. Можно доказывать по индукции. В нашем случае $2x_0\not\equiv0(\mathrm{mod}\,p)$ — это ключевой момент!

4) $p=7$. $(\frac{-1}{p})=-1$, поэтому решения нет.

5) $p=11$. $-1/11=-1$, поэтому решения нет.

6) $p=13$. $-1/13=1$, поэтому имеем два решения, для которых $x_0\in\{5;8\}$.

7) $p=17$. $-1/17=1$, поэтому имеем два решения, для которых $x_0\in\{4;13\}$.

8) $p=19$. $-1/19=-1$, поэтому решения нет.

Задача 17.11,5 (Лемма Гензеля). Решение. Строим $a_n\to a$ – решение $F(a)=0$, $a\equiv a_0\,(\mathrm{mod}\ p)$, где $a_i\in\mathbb{Z}\ \forall\, i=0,1,\dots$ – последовательность, т.ч.

1) $F(a_n)\equiv0\,(\mathrm{mod}\ p^{n+1})$

2) $a_n\equiv a_{n-1}\,(\mathrm{mod}\ p^n)$

3) $0\leqslant a_n<p^{n+1}$, т.е. $\{a_i\}\in\mathbb{Z}_p$.

Индукция. $n=1$:

Выбираем $\widetilde{a_0} \in \mathbb{Z}$: $\widetilde{a_0} \equiv a_0 \pmod p$ и $\widetilde{a_0} \in \{0, 1, \ldots, p-1\}$ и этот выбор единственный.

Из условий 2) и 3) $\Rightarrow a_1 = \widetilde{a_0} + b_1 p$, где $0 \leqslant b_1 \leqslant p-1$. Рассмотрим $F(\widetilde{a_0} + b_1 p)$ с точки зрения по $\pmod{p^2}$. Пусть $F(x) = \sum\limits_{i=0}^{n} c_i x^i$. Значит, $F(\widetilde{a_0} + b_1 p) = \sum\limits_{i=0}^{n} c_i (\widetilde{a_0} + b_1 p)^i = \sum\limits_{i=0}^{n} (c_i \widetilde{a_0}^i + i c_i \widetilde{a_0}^{i-1} b_1 p + p^2 \cdot (\ldots)) \equiv \sum\limits_{i=1}^{n} c_i \widetilde{a_0}^i + \sum\limits_{i=1}^{n} i c_i \widetilde{a_0}^{i-1} b_1 p \pmod{p^2} = F(\widetilde{a_0}) + F'(\widetilde{a_0}) b_1 p$.

Т.е., как в вещественном матанализе, $F(x+h) = F(x) + F'(x) \cdot h +$ члены более высокого порядка.

Т.к. $F(a_0) \equiv 0 \pmod p \Rightarrow F(\widetilde{a_0}) \equiv \alpha \cdot p \pmod{p^2}$, где $\alpha \in \{0, 1, \ldots, p-1\}$. Значит, сравнение $F(a_1) \equiv 0 \pmod{p^2} \Leftrightarrow \alpha p + F'(\widetilde{a_0}) \cdot b_1 p \equiv 0 \pmod{p^2} \Leftrightarrow \alpha + F'(\widetilde{a_0}) b_1 \equiv 0 \pmod p$, а это разрешимо в $GF(p)^*$, т.к. $F'(\widetilde{a_0}) \neq 0$ в $GF(p)$. Т.е. $b_1 \equiv -\alpha / F'(\widetilde{a_0}) \pmod p$. Очевидно, что выбор b_1 однозначен.

Шаг индукции. $a_1, \ldots, a_{n-1}$ нашли, надо найти a_n.

По индукционному предположению: (2) и (3) $a_n \equiv a_{n-1} \pmod{p^n}$, $a \leqslant a_n < p^{n+1}$, т.е. $a_n = a_{n-1} + b_n p^n$, $b_n \in \{0, \ldots, p-1\}$.

Рассмотрим $F(a_n) = F(a_{n-1} + b_n p^n)$, отбрасывая члены, кратные p^{n+1} (аналогично случаю $n = 1$). $F(a_n) \equiv F(a_{n-1}) + F'(a_{n-1}) \cdot b_n p^n \pmod{p^{n+1}}$. По (1) $F(a_{n-1}) \equiv 0 \pmod{p^n} \Rightarrow F(a_{n-1}) \equiv \alpha' p^n \pmod{p^{n+1}}$. Значит, условие $F(a_n) \equiv 0 \pmod{p^{n+1}} \Leftrightarrow \alpha' + F'(a_{n-1}) b_n \equiv 0 \pmod p$. Но в $GF(p)$ $a_{n-1} = a_0$ (по транзитивности сравнений) $\Rightarrow F'(a_{n-1}) \not\equiv 0 \pmod p \Rightarrow b_n$ вычисляется однозначно: $b_n \equiv -\alpha' / F'(a_{n-1}) \pmod p$.

Теперь рассмотрим $a = \widetilde{a_0} + b_1 p + b_2 p + \ldots \in \mathbb{Z}_p$. Тогда $F(a) \equiv F(a_n) \equiv 0 \pmod{p^{n+1}}\ \forall n \in \mathbb{N} \Rightarrow F(a) = 0$ в $\mathbb{Z}_p$.

Единственность. Пусть $a' \in \mathbb{Z}_p$: $F(a') = 0$, $a' \equiv a_0 \pmod p$, $\widetilde{a_0} \in \mathbb{Z}$, $\widetilde{a_0} \in \{0, 1, \ldots, p-1\}$, $\widetilde{a_0} \equiv a_0 \pmod p$. Но дальнейшее построение a' из $\widetilde{a_0}$ однозначно, т.к. $F(a') \equiv 0 \pmod{p^{n+1}}\ \forall n \in \mathbb{N}$.

Задача 17.12. Решение. $-1 = \dfrac{p-1}{1-p} = (p-1)(1 + p + p^2 + \ldots) = (p-1) + (p-1)p + (p-1)p^2 + \ldots$.

Задача 17.13. Решение. $\Rightarrow$ Представим $\alpha = c - \frac{a}{b}$, где $a, b, c \in \mathbb{Z}$, $b \in \mathbb{N}$, $0 \leqslant a < b$, т.е. $\frac{a}{b}$ – правильная дробь.

Пусть $r = \varphi(b)$, $(p, b) = 1 \Rightarrow p^r - 1 = bu$, $u \in \mathbb{N}$, т.е. $-\dfrac{a}{b} = \dfrac{au}{1-p^r}$. Заметим, что $au < bu = p^r - 1$, т.к. $a < b$. Значит, $au = a_0 + a_1 p + \ldots + a_{r-1} p^{r-1}$. В $\mathbb{Q}_p$ числа принято записывать справа налево $au = \overline{a_{r-1} a_{r-2} \ldots a_0}$.

По формуле геометрической прогрессии $\dfrac{1}{1-p^r} = 1 + p^r + p^{2r} + p^{3r} + \ldots$. Пусть $c = \overline{c_k c_{k-1} \ldots c_0}$. Тогда $-\frac{a}{b} = \overline{\ldots a_{r-1} \ldots a_0 a_{r-1} \ldots a_0}$. Очевидно, что $\alpha = c - \frac{a}{b}$ имеет периодические коэффициенты в каноническом разложении в $\mathbb{Q}_p$.

$\Leftarrow$ Пусть $\alpha \in \mathbb{Q}$. $\overline{\ldots a_{r-1} \ldots a_0 a_{r-1} \ldots a_0 c_k \ldots c_0} = \alpha$

$\overline{c_k, \ldots, c_0} = c \in \mathbb{Q}$ (очевидно). Оставшийся периодический «хвост» (как мы видели ранее) равен $(a_0 + a_1 p + \ldots + a_{r-1} p^{r-1}) \cdot \dfrac{1}{1-p^r} \in \mathbb{Q}$ (очевидно).

Задача 17.14. Решение. Согласно задаче 17.13: $5^{\varphi(3)} - 1 = 8 \cdot 3 \Rightarrow -\dfrac{2}{3} = \dfrac{2 \cdot 8}{1-5^2} = \dfrac{1 + 3 \cdot 5}{1-5^2} = (1 + 3 \cdot 5)(1 + 5^2 + 5^4 + 5^6 + \ldots) = 1 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + 3 \cdot 5^5 + \ldots$

Задача 17.15. Решение. $(x^p - 1) = (x-1)(x^{p-1} + x^{p-2} + \ldots + 1)$. Докажем неприводимость $g(x) = x^{p-1} + x^{p-2} + \ldots + 1$ в $\mathbb{Q}_p[x]$, используя критерий Эйзенштейна 16.11 а). Если $g(x)$ разложим, то $g(x+1)$ разложим и обратно; это очевидно, так как замена $y = x + 1$ линейная. $g(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + p x^{p-2} + \ldots + p$. Так как $p | C_p^k$ при $k = 1, \ldots, p-1$, то критерий Эйзенштейна работает. Значит, $g(x)$ не имеет корней в $\mathbb{Q}_p$.

Задача 17.16. Решение. а), б), в). Докажем, что $\{c, c^p, c^{p^2}, \ldots, c^{p^n}, \ldots\}$ — целое p-адическое число γ. Очевидно, что $c \equiv \gamma \pmod p$. Т.к. $c \not\equiv 0 \pmod p \Rightarrow (c, p^{n+1}) = 1 \Rightarrow c^{\varphi(p^{n+1})} \equiv 1 \pmod{p^{n+1}}$. Но $\varphi(p^{n+1}) = p^n (p-1) \Rightarrow (c^{p^n})^{p-1} \equiv 1 \pmod{p^{n+1}}$.

Домножим обе части равенства в $(\mathbb{Z}/p^{n+1}\mathbb{Z})^*$ на c^{p^n}. Очевидно, что $c^{p^n} \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^*$, т.к. $p \nmid c \Rightarrow$ равенство сохраняется: $c^{p^{n+1}} \equiv c^{p^n} \pmod{p^{n+1}}$. А это и есть определение целого p-адического числа γ_c — представителя Тейхмюлера, т.е. $\gamma_c = \{c, c^p, c^{p^2}, \ldots, c^{p^n}, \ldots\}$.

По правилам умножения целых p-адических чисел, чтобы возвести γ_c в $(p-1)$ степень, нужно любой член последовательности возвести в $(p-1)$-ю степень, т.к. $p \nmid c$. $(c^{p^n})^{p-1} = c^{\varphi(p^{n+1})} \equiv 1 \pmod{p^{n+1}}$. Т.е. мы получаем $\{1, 1, 1 \ldots\} = 1 \in \mathbb{Z}_p \Rightarrow \gamma_c^{p-1}$ – корень уравнения $x^{p-1} = 1$. Т.к. $\gamma_1 \ldots \gamma_{p-1}$ – все различны $\Rightarrow$ это весь набор корней в $\mathbb{Q}_p$ и многочлен $(x^{p-1} - 1)$ разлагается на линейные.

Задача 17.17. Решение. а) По 16.12 $|n| \leqslant 1\ \forall n \in \mathbb{N}$. Пусть $\forall p \in P$ – простого $|p| = 1$. По основной теореме арифметики $\forall n \in \mathbb{N}\ n = p_1^{k_1} \cdot \ldots \cdot p_n^{k_n} \Rightarrow |n| = 1 \Rightarrow \forall \frac{p}{q} \in \mathbb{Q}, |\frac{p}{q}| = 1 \Rightarrow$ норма тривиальна $\Rightarrow \exists p \in P$: $|p| < 1$.

Пусть $\exists q \in P$: $|q| < 1$, $q \neq p$. Тогда $\exists l, s \in \mathbb{N}$: $|p^l| < \frac{1}{2}$, $|q^s| < \frac{1}{2}$, $(p^l, q^s) = 1 \Rightarrow \exists u, v$: $1 = up^l + vq^s$ $\Rightarrow 1 = |1| = |up^l + vq^s| \leqslant |u||p^l| + |v||q^s| < 1 \cdot \frac{1}{2} + 1 \cdot \frac{1}{2} = 1$ Противоречие $\Rightarrow \exists! p \in P$ — простое, т.ч. $|p| < 1$ и $\forall q \in P$, $q \neq p$, $|q| = 1 \Rightarrow$ По основной теореме арифметики $\forall n \in \mathbb{N}\ n = p^k \cdot q_1^{n_1} \cdot \ldots \cdot q_t^{n_t}$, тогда $|n| = |p|^k \cdot 1$. Но $|p| < 1 \Rightarrow \exists \alpha\ 0 < \alpha < 1$: $|p| = \alpha$. Но в такой метрике $x_i \to 0 \Leftrightarrow |x_i|_p \to 0$, где $x_i \in \mathbb{Q}$, т.е. эта метрика эквивалентна p-адической.

б) Сначала докажем, что если $\alpha \in \mathbb{R}$: $0 < \alpha \leqslant 1$, то $|x|^\alpha$ — тоже метрика на $\mathbb{Q}$. Пусть $|x| \geqslant y$, $x \neq 0$. Тогда $|x + y|^\alpha = |x|^\alpha \cdot |1 + \frac{y}{x}|^\alpha \leqslant x^\alpha(1 + |\frac{y}{x}|)^\alpha \leqslant |x|^\alpha(1 + |\frac{y}{x}|) \leqslant |x|^\alpha(1 + |\frac{y}{x}|^\alpha) = |x|^\alpha + |y|^\alpha$. Очевидно, что эта метрика эквивалентна абсолютной.

Если φ – архимедова, то по 16.12 $\exists a \in \mathbb{N}$: $\varphi(a) > 1$. Т.к. $\varphi(1+1+\ldots+1) \leqslant \varphi(1)+\varphi(1)+\ldots+\varphi(1) = n$ $\forall n$, то $\exists \alpha \in \mathbb{R}\ 0 < \alpha \leqslant 1$: $\varphi(a) = a^\alpha$. Пусть N — произвольное. Запишем его в a-ичной системе: $N = x_0 + x_1 a + \ldots + x_{k-1}a^{k-1}$, где $0 \leqslant x_i \leqslant a-1$ $(0 \leqslant i \leqslant k-1)$, $x_{k-1} \geqslant 1$. Значит, $a^{k-1} \leqslant N < a^k$. По свойствам метрики имеем: $\varphi(N) \leqslant \varphi(x_0) + \varphi(x_1)\varphi(a) + \ldots + \varphi(x_{k-1})\varphi(a)^{k-1} \leqslant (a-1)(1 + a^\alpha + \ldots + a^{(k-1)\alpha}) = (a-1)\frac{a^{k\alpha} - 1}{a^\alpha - 1}$ (как сумма геометрической прогрессии) $< (a-1) \cdot \frac{a^{k\alpha}}{a^\alpha - 1} = \frac{(a-1) \cdot a^\alpha}{a^\alpha - 1} \cdot a^{(k-1)\alpha)} \leqslant \frac{(a-1)a^\alpha}{a^\alpha - 1} N^\alpha = C\, N^\alpha$, т.е. $\varphi(N) < C\, N^\alpha$, где C — константа. Заменим N на N^m, $m \in \mathbb{N}$. Получаем: $\varphi(N^m) = \varphi(N)^m < C\, N^{m\alpha} \Rightarrow \varphi(N) < \sqrt[m]{C}\, N^\alpha$. При $m \to \infty$ $\varphi(N) \leqslant N^\alpha$.

Теперь наоборот. Положим: $N = a^k \cdot b$, где $0 < b < a^k - a^{k-1}$. Т.к. $a^k = N + b \Rightarrow \varphi(a^k) \leqslant \varphi(N) + \varphi(b)$ $\Rightarrow \varphi(N) \geqslant a^{\alpha k} - \varphi(b)$. Из предыдущего $\varphi(b) \leqslant b^\alpha \leqslant (a^k - a^{k-1})^\alpha$. Значит, $\varphi(N) \geqslant a^{\alpha k} - (a^k - a^{k-1})^\alpha = (1 - (1 - \frac{1}{\alpha})^\alpha)a^{\alpha k} = c_1 a^{\alpha_k} > c_1 N^\alpha$, где c_1 – константа. Аналогично предыдущему, меняем N на N^m, извлекаем корень m-й степени и устремляем $m \to \infty$. $\varphi(N) > \sqrt[m]{c_1} N^\alpha \Rightarrow \varphi(N) \geqslant N^\alpha \Rightarrow \varphi(N) = N^\alpha$. Т.к. $\forall x \in \mathbb{Q}$, $x \neq 0$ $x = \pm\frac{N_1}{N_2} \Rightarrow \varphi(x) = |x|^\alpha$, которая, очевидно, эквивалентна абсолютной метрике.

Задача 17.18. Решение. а) По критерию Эйзенштейна 16.11 а) многочлен $x^n - p$ неприводим в $\mathbb{Q}_p$ $\forall n > 1$. Пусть $p < q$. Т.к. $F_q^* = <b> \Rightarrow \exists l \in \{2, \ldots, q-2\}$ и $\exists b \in F_q^*$: $b^l = p$ Случаи $p = 2$, $q = 3$ разбираются отдельно. Значит, $b^l = p \Rightarrow b^l - p \equiv 0 \pmod{q}$. Но $l \cdot b^{l-1} \not\equiv 0 \pmod{q} \Rightarrow$ по лемме Гензеля 17.11,5 многочлен $x^l - p$ приводим в $\mathbb{Q}_q \Rightarrow \mathbb{Q}_p \ncong \mathbb{Q}_q$.

б) Уравнение $x^2 = p$ имеет решение в $\mathbb{R}$, но не в $\mathbb{Q}_p$.

Задача 17.19. Решение. Пусть $a = 1 + pz$, где $z \in \mathbb{Z}_p$ — главная p-адическая единица. Пусть $(n, p) = 1$.

Рассмотрим $F(x) = x^n - a$ и применим лемму Гензеля. $F(1) \equiv 0 \pmod{p}$, $F'(1) \not\equiv 0 \pmod{p}$. Значит, $\exists! t \in \mathbb{Z}_p$, такое что $t \equiv 1 \pmod{p}$, $t^n = a$, $\forall n$, такого что $(n, p) = 1$.

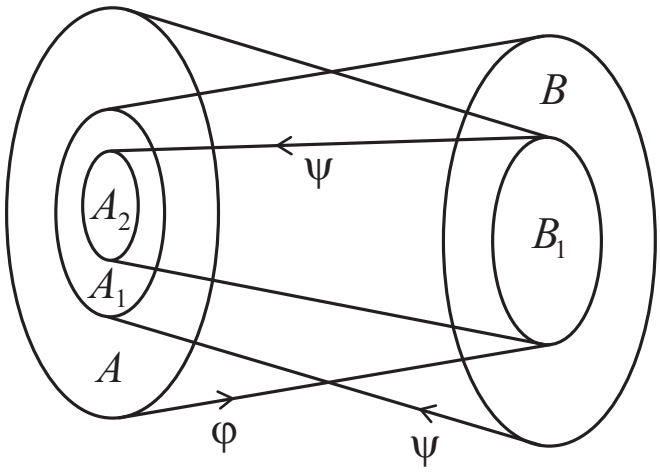
Пусть δ: $\mathbb{Q}_p \to \mathbb{Q}_p$ – автоморфизм, и $a = 1 + pz$, где $z \in \mathbb{Z}_p$. Рассмотрим $\nu(\delta(a))$ — p-показатель ν_p. Т.к. $\forall n$, для которого $(n, p) = 1$, $\exists t$: $t^n = a \Rightarrow \delta(t)^n = \delta(a) \Rightarrow n \cdot \nu(\delta(t)) = \nu(\delta(a))$, поскольку $\nu(y^n) = n \cdot \nu(y)$, см. 16.9 а). Так как ν: $\mathbb{Q}_p \to \mathbb{Z} \Rightarrow n \mid \nu(\delta(a))$ $\forall a \in \mathbb{Z}_p$, такого что $a \equiv 1 \pmod{p}$, и $\forall n$, такого что $(n, p) = 1$, то $\nu(\delta(a)) = 0$, т.е. δ сохраняет норму на главных p-адических единицах.

Но $\delta \mid_{\mathbb{Q}} = \mathrm{id}$, т.к. $\mathbb{Q}$ — минимальное подполе. По 16.6 и 16.13 $\forall q \in \mathbb{Q}_p$ $q = t \cdot p^m \cdot \xi$, где $(t, p) = 1$, ξ — главная p-адическая единица $\Rightarrow \nu(\delta(q)) = \nu(\delta(\xi) \cdot t \cdot p^m) = m \Rightarrow \delta$ сохраняет норму на $\mathbb{Q}_p$, т.е. изометричен и, значит непрерывен. $\forall x \in \mathbb{Q}_p\ \exists \{x_n\} \to x$: $x_n \in \mathbb{Q}$ (по 17.3).

Так как $|x_n - x| \to 0 \Rightarrow |\delta(x_n) - \delta(x)| \to 0$, поскольку δ — изометрия $\Rightarrow \delta(x_n) \to \delta(x)$. Но $\delta(x_n) = x_n \ \forall n \in \mathbb{N}$, так как $x_n \in \mathbb{Q} \Rightarrow x_n \to \delta(x)$. Но $x_n \to x \Rightarrow x = \delta(x)$ в силу единственности предела последовательности $\Rightarrow \delta = \mathrm{id}$.

Листок 18.

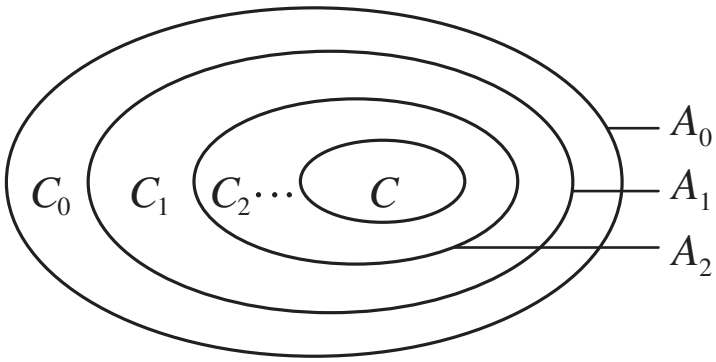
Задача 18.6. Решение. Пусть $\varphi : A \to B_1 \subset B$, $\psi : B \to A_1 \subset A$, φ, ψ — биекции. Имеем $\psi(B_1) = A_2 \subset A_1$, $A \sim B_1 \sim A_2$. Надо доказать, что $A \sim A_1$, см. рисунок.



Достаточно доказать следующую лемму:

Лемма. *Если* $A_2 \subset A_1 \subset A_0$ *и* $A_2 \sim A_0$, *то* $A_0 \sim A_1$.

Доказательство. Пусть $f : A_0 \to A_2$ — биекция. Тогда $f(A_1) = A_3 \subset A_2$, $f(A_2) = A_4 \subset A_2$. Продолжая по индукции, получим: $A_0 \supset A_1 \supset A_2 \supset A_3 \supset A_4 ...$ Обозначим $f^{(n)}(x) = f(f(f...(x)...))$ — отображение f применено n раз. Тогда $f(A_i) = A_{i+2}$, т.е. $A_{2n} = f^{(n)}(A_0)$, $A_{2n+1} = f^{(n)}(A_1)$. Пусть $C = \bigcap\limits_i A_i$, $C_i = A_i \setminus A_{i+1}$, см. рисунок.



Так как f — биекция, то $f(C_0) = C_2$, $f(C_2) = C_4$ и т.д. Аналогично, $f(C_1) = C_3$, $f(C_3) = C_5$ и т.д. Определим $g : A_0 \to A_1$: $g(x) = f(x)$, если $x \in C_{2k}$ и $g(x) = x$, если $x \in C_{2k+1}$ или $x \in C$. Очевидно, что $C_i \cap C_{i+1} = \emptyset$, поэтому $C_i \cap C_j = \emptyset$ для любых i, j, таких что $i \neq j$. Также очевидно, что $C \cap C_i = \emptyset$ для любого i. Таким образом, $A_0 = \cup_i C_i \cup C$ и все составляющие попарно не пересекаются. Имеем: $A_0 = C_0 + C_1 + C_2 + C_3 + C_4 + ... + C$, $A_1 = C_1 + C_2 + C_3 + C_4 + ... + C$. C_0 отображаем в C_2, C_2 — в C_4 и т.д.; C_1 отображаем в C_1, C_3 — в C_3 и т.д. Очевидно, что в результате имеем биекцию.

Задача 18.8. Решение. Пусть X — множество, $P(X)$ — множество всех его подмножеств. Допустим, существует биекция $\varphi : X \to P(X)$. Рассмотрим элементы $y \in X$, такие что $y \notin \varphi(y)$. Образуем множество $\mathbb{Z} = \{y : y \notin \varphi(y)\}$. Пусть $\mathbb{Z} = \varphi(z)$, $z \in X$. Тогда $z \in \mathbb{Z} \Leftrightarrow z \notin \varphi(z) \Leftrightarrow z \notin \mathbb{Z}$, так как

по предположению $\mathbb{Z} = \varphi(z)$ и φ — биекция. Получили противоречие. Так как вложение $X \hookrightarrow P(x)$ очевидно существует, мощность $P(X)$ больше мощности X.

Задача 18.11. Решение. Пусть R — коммутативное кольцо с единицей. Рассмотрим множество $M = \{I \subset R,\ I - \text{идеал},\ 1 \notin I$. M — частично упорядоченное множество по вложению, в котором любая цепь имеет верхнюю грань, а именно, объединение элементов цепи (очевидно, это идеал). Тогда по лемме Цорна любой собственный идеал лежит в некотором максимальном идеале.

Задача 18.12. Решение. Поместим наше поле K в $P(K)$ — множество всех подмножеств K. По 18.8 $|K| < |P(K)|$. По 9.15–9.17 мы можем строить алгебраические расширения, факторизуя кольца многочленов. Рассмотрим множество алгебраических расширений K, содержащихся в $P(K)$. По 18.15 $|L| = |K|$, так как декартов квадрат бесконечного множества равномощен ему самому — это следует из 18.6. Множество алгебраических расширений образуют ЧУМ, удовлетворяющее условию леммы Цорна. Максимальный элемент ЧУМ будет алгебраическим замыканием поля K (очевидно) .

Задача 18.13. Решение. Рассмотрим множество пар $T = \{(F, \sigma) : K \subset F \subset L,\ \sigma : F \to M,\ \sigma|_K = \varphi\}$. Множество T не пустое, так как $\{(K, \varphi) \in T\}$. Определим на T порядок, так что оно станет ЧУМ: по определению, $(F_1, \sigma_1) \leq (F_1, \sigma_1) \Leftrightarrow F_1 \subset F_2,\ \sigma_2|_{F_1} = \sigma_1$. Для цепи $(F_i, \sigma_i),\ i \in I$ верхней гранью будет (F, σ), где $F = \cup_i F_i$, $\sigma(x) = \sigma_i(x)$ при $x \in F_i$. По лемме Цорна существует максимальный элемент (P, θ). Если $P \subset L$ и $P \neq L$, то существует элемент $a \in L \setminus P$, алгебраичный над K. Тогда по 10.1 мы можем продолжить θ, так как M алгебраически замкнуто, и (P, θ) — не максимальный, противоречие. Значит, $(P, \theta) = (L, \psi)$.

Задача 18.14. Решение. Пусть $K \subset L$ — алгебраическое расширение, L и M алгебраически замкнуты, $K \subset M$ — тоже алгебраическое расширение. Тогда по 18.13 φ =id продолжается до $\psi : L \to M$, где ψ — мономорфизм по 8,5.5, т.е. $\psi(L) \cong L$ и $K \subset \psi(L) \subset M$, $K \subset M$ — алгебраическое расширение, поэтому $K \subset \psi(L)$ — также алгебраическое расширение, а также и $\psi(L) \subset M$, что очевидно. Но $\psi(L)$ алгебраически замкнуто по 8,5.6 г). Но над алгебраически замкнутым полем не бывает алгебраических расширений, поэтому $\psi(L) = M$, т.е. $L \cong M$.

Задача 18.16. Решение. Пусть $I = \{\alpha_1, ..., \alpha_\omega, ...\}$ — множество линейно независимых векторов. Построим ЧУМ $\{J : I \subset J\}$ относительно включения. По лемме Цорна существует такой максимальный элемент M, что $I \subset M$. Очевидно, M — базис Гамеля.

Докажем единственность разложения. Пусть $\alpha = \sum\limits_{i=1}^{n} x_i \alpha_i$, $\alpha = \sum\limits_{j=1}^{k} x'_j \alpha'_j$ — два несовпадающих разложения; здесь $\alpha, \alpha_i, \alpha'_j \in L$ — векторы, а $x_i, x'_j \in F$ — коэффициенты. Объединим все векторы $\{\alpha_1, ..., \alpha_n\}$ и $\{\alpha'_1, ..., \alpha'_k\}$; если какие-то два элемента совпали, один из них удалим. Получим конечную систему линейно независимых векторов. Множество всех линейных комбинаций этих векторов с коэффициентами из F образует конечномерное векторное пространство и оба разложения вектора α записаны в нем. Но в конечномерном пространстве разложение единственно. Противоречие.

Задача 18.17. Решение. Так как для любых $x, y \in \mathbb{R}$ имеем $f(x + y) = f(x) + f(y)$, то, просуммировав n одинаковых слагаемых, получим: $f(x) + ... + f(x) = f(nx) = nf(x)$. Аналогично ($m$ слагаемых), $f(x/m) + ... + f(x/m) = f(x) = mf(x/m)$, поэтому для любого $q \in \mathbb{Q}$ имеем $f(qx) = qf(x)$. f — гомоморфизм, поэтому $f(0) = 0$. Мы получили, что f — линейное отображение в $\mathbb{R}$ как линейном пространстве над $\mathbb{Q}$. Для $q \in \mathbb{Q}$, очевидно, $f(q) = qc$, где $c = f(1)$.

Пусть f ограничена на некотором отрезке $I \subset \mathbb{R}$. Тогда линейно-рациональным преобразованием $t = kx + e$, $k, e \in \mathbb{Q}$ можно перевести I в отрезок, лежащий внутри отрезка $[-\delta, \delta]$ для некоторого $\delta > 0$, т.е. в окрестность нуля. Получим, что $|f(x)| \leq M$ в некоторой окрестности нуля $(-\delta, \delta)$. Тогда $\forall \varepsilon > 0\ \exists N : M/N < \varepsilon$, поэтому, в силу $\mathbb{Q}$-линейности $|f(x/N)| = |f(x)/N| \leq M/N < \varepsilon$, т.е. $\forall x \in (-\delta/N, \delta/N)\ |f(x)| < \varepsilon$, а значит, $f(x)$ непрерывна в нуле. Снова в силу $\mathbb{Q}$-линейности, $f(x) = f(x - x_0 + x_0) = f(x - x_0) + f(x_0) \to f(x_0)$ при $x \to x_0$, поэтому $f(x)$ непрерывна на всем $\mathbb{R}$, но тогда $f(x) = cx$, так как $\mathbb{Q}$ всюду плотно в $\mathbb{R}$.

Если же $f(x)$ не ограничена ни на каком отрезке, то она разрывна в каждой точке, т.к. функция ограничена в некоторой окрестности точки непрерывности.

Задача 18.18. Решение. Можно задать $f(x)$ на базисе Гамеля $\{\alpha_1, ...\alpha_\omega, ...\}$. Зафиксируем элемент базиса $\alpha_\gamma \neq \alpha_1$. Положим $f_{\alpha_\gamma}(x)$ — коэффициент при α_γ в разложении x по базису $\{\alpha_1, ...\alpha_\omega, ...\}$. Тогда, очевидно, f_{α_γ} удовлетворяет условию Коши и $f_{\alpha_\gamma}(x) \neq cx$. Действительно, $f_{\alpha_\gamma}(\alpha_1) = 0 \neq c\alpha_1$. Поэтому функция f_{α_γ} везде разрывна.

Задача 18.19. Решение. а) Если функция, удовлетворяющая условию Коши, разрывна, то она не имеет вида $f(x) = cx$, а значит, разрывна всюду по 18.17.

б) Если f монотонна на некотором отрезке, то она ограничена на нем и тогда по решению 18.17 имеет вид $f(x) = cx$ для всех действительных x — противоречие.

Сохранение знака на некотором отрезке противоречит 18.19 д).

в) Следует из решения 18.17.

г) Следует из 18.19 д).

д) Достаточно доказать, что для любой точки $\mathbb{Q}^2$ найдется сколь угодно близкая к ней точка графика — тогда мы используем, что $\mathbb{Q}^2$ плотно в $\mathbb{R}^2$ и неравенство треугольника. Зафиксируем (x_0, y_0) и произвольное $r > 0$. Так как $f(x)$ разрывна, то найдется такое α, что $f(\alpha) = c\alpha + \delta$, где $c = f(1)$, $\delta \neq 0$. Обозначим $\beta = (y_0 - cx_0)/\delta$. Положим $M = \max(|c|, 1)$ и выберем такие рациональные $b \neq 0$, a, что $|b-\beta| < r/(3|\delta|)$, $|a-\alpha| < r/(3|b|M)$. Рассмотрим точку графика $(X, f(X))$, где $X = x_0 + b(a-\alpha)$. Тогда по $\mathbb{Q}$-линейности получим: $f(X) = cx_0 + b((c\alpha+\delta) - ca) = c(x_0 + b(\alpha - a)) + b\delta = cX + b\delta$. Из предыдущего $y_0 = \beta\delta + cx_0$, тогда $f(X) - y_0 = cX + b\delta - \beta\delta - cx_0 = c(X - x_0) + \delta(b - \beta)$. По неравенству треугольника имеем: $|f(X) - y_0| \leq |c||X - x_0| + |\delta||b - \beta| = |c| \cdot |b| \cdot |a - \alpha| + |\delta||b - \beta| < r/3 + r/3 = 2r/3$. Тогда расстояние от точки графика $(X, f(X))$ до (x_0, y_0) равно $\sqrt{(X - x_0)^2 + (f(X) - y_0)^2} < r\sqrt{1/9 + 4/9} < r$. Тем самым нашлась точка графика, близкая к $(x_0, y_0) \in \mathbb{Q}^2$.

Рекомендуемая литература

1. Ван дер Варден Б.Л. Алгебра. - М.: “Наука”, 1976.

2. Винберг Э.Б. Курс алгебры. - М.: “Факториал Пресс”, 2001.

3. Кострикин А.И. Введение в алгебру. Часть III. Основные алгебраические структуры. - М.: “Физико-математическая литература”, 2000.

4. Ленг С. Алгебра. - М.: “Мир”, 1968.

5. Сборник задач по алгебре / под редакцией А.И. Кострикина. - М.: МЦНМО, 2021.

6. Верещагин Н.К., Шень А. Начала теории множеств. - М.: МЦНМО, 2012.

7. Коблиц Н. p-адические числа, p-адический анализ и дзета-функции. - М. “Мир”, 1982.

8. Боревич З.И., Шафаревич И.Р. Теория чисел. - М.: Главная редакция физико-математической литературы, 1985.

9. Серр Ж.-П. Курс арифметики. - М.: “Мир”, 1972.

ISSN 1992-6138