ГРУППЫ, ПОЛЯ, КОЛЬЦА (тезисы лекций по алгебре)

Эти пять лекций читались помимо обычного втузовского курса "высшей"математики. Поэтому в них я не касался таких стандартных тем, как линейные системы, перестановки, определители и матрицы, многочлены, симметрические функции и комплексные числа. Основным сюжетом лекций, таким образом, оказались алгебраические структуры : поля, группы, кольца. К сожалению время не позволило прочитать запланированные 2 лекции про модули ; не прочитанной оказалась и задуманная для украшения лекция о p-адических числах.

Все слушатели были снабжены книгой А.Кострикина "Алгебра"; ссылки на нее даются в виде К-133 (цифры = номер страницы). Предполагались известными:язык теории множеств (К 39-52) и числовые системы $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$.

Лекции здесь записаны в виде тезисов; каждый из них самостоятельное высказывание. Его следует продумать, понять, и, если имеется знак ◀ , доказать (если же доказательство не получается, нужно его выудить из соответствующего места в К). Доказательства, помеченные знаком ◀ , как правило, основаны на важной идее, но все - простые (одноходовые). Исключение составляют тезисы 8°-13° из лекции III; восстановить их доказательства, не заглянув в К и/или в книгу С.Ленга "Алгебра", не легко; поэтому эти доказательства не входят в обязательный минимум требований.

Слушатель может считать лекционный материал освоенным, если он разобрался во всех тезисах, помнит определения и основные формулировки (выделенные курсивом) и умеет довольно быстро восстанавливать отсутствующие доказательства.

Перерешав бóльшую часть упражнений и задач, которые обсуждались на семинарах параллельно с лекциями, он может считать освоенными самые азы алгебры.

Лекция I. ГРУППЫ КАК ГРУППЫ ПРЕОБРАЗОВАНИЙ

1° *Определение группы* $(G,*)$: множество с бинарной операцией $*$ (см. К-133), ассоциативной, обладающей единственным *нейтральным* элементом e (т.е. таким $e \in G$, что $\forall a \in G\ a*e=e*a=a$) и, для каждого элемента a , *симметричным* элементом $\bar{a}$ (т.е. таким $\bar{a}$, что $\bar{a}*a=a*\bar{a}=e$).

Если операция $*$ коммутативна, то группа G называется абелевой или коммутативной. Примеры: $(\mathbb{Q}, +)$, $(\mathbb{R}\setminus 0, \cdot)$; но $(\mathbb{N}, +)$ – не группа.

2^0 Другое определение группы: множество с бинарной ассоциативной операцией, для которой любое уравнение вида

$$a * x = b \text{ или } x * a = b$$

имеет единственное решение. Эти два определения эквивалентны ◄.

3^0 Аксиомы группы 1^0 можно существенно ослабить ◄.

4^0 Примеры: числовые группы ($(\mathbb{Z}, +)$, $(\mathbb{R}^+, \cdot)$ и т.п.), окружность $S^1 = (\{z \in \mathbb{C}, |z| = 1\}, \cdot)$, группа векторов на плоскости по сложению, группа биективных преобразований данного множества М по композиции $(\mathrm{Bij}\, M, \circ)$, группа движений фигуры $(\mathrm{Iso}\, \Phi, \circ)$, группы перестановок, группы матриц, в физике – группы Лоренца, в механике – группы Ли, в химии – кристаллографические группы и т.д. и т.п.

5^0 Для абелевых групп операция обычно называется сложением, нейтральный элемент – нулем, симметричный элемент – противоположным (обозначения $+$, 0, $-a$). Для неабелевых, соответственно, умножением (иногда – композицией, произведением), единицей, обратным (обозначения $\cdot$ (или $\circ$), 1, a^{-1}).

6^0 Из аксиом группы следуют законы сокращения (левый и правый)

$$a * b = a * c \Rightarrow b = c \;; \quad b * a = c * a \Rightarrow b = c$$ ◄

7^0 Биекция φ одной группы $(G, *)$ на другую $(H, \circ)$ называется изоморфизмом, если она сохраняет операцию (т.е. $\varphi(g' * g'') = \varphi(g') \circ \varphi(g'')$; в этом случае G и H называются изоморфными. Обозначение: $G \cong H$.

8^0 Очевидным образом определяется подгруппа Н данной группы $(G, *)$ (такое подмножество $H \subset G$, которое само является группой относительно $*$). Для этого достаточно, чтобы $\forall a, b \in H \; ab^{-1} \in H$. ◄

9^0 На практике важнейший класс групп – это группы преобразований, т.е. подгруппы групп $\mathrm{Bij}\, M$ биекций различных множеств М. Например, S^1 – группа поворотов окружности, группа Лоренца – подгруппа группы биекций "пространства – времени" и т.п. Оказывается, никаких других групп, кроме групп преобразований, нет, как показывает следующая

Теорема Кейли. Всякая группа G является группой преобразований; именно, она изоморфна некоторой подгруппе Н группы $\mathrm{Bij}\, G$

10^0 В качестве Н можно взять группу левых сдвигов G, т.е. совокупность отображений $H = \{\varphi_{g_0} : G \to G, \; g_0 \in G\}$ действующих по правилу $\varphi_{g_0}(g) = g_0 g$, где $g \in G$, относительно операции композиции, Н действительно является подгруппой $Bij\,G$ ◄

11⁰ Искомый изоморфизм устанавливается по естественному правилу
$$G \ni g \mapsto \varphi_g \in H$$ ◄

12⁰ Группы биекций $Bij\,M$, в частном случае, когда М - конечное множество, называется группами перестановок (или подстановок) или симметрическими группами n-ой степени (где n - число элементов) в М) и обозначается $\mathbb{S}_n$. При $n \geqslant 4$ эти группы не абелевы ◄
В $\mathbb{S}_n$ имеется подгруппа A_n из $n!/2$ элементов ◄

13⁰ Из теоремы Кейли сразу следует, что любая конечная группа изоморфна некоторой подгруппе группы перестановок $\mathbb{S}_n$. (В качестве n можно взять число элементов данной группы).

14⁰ Доказательство теоремы Кейли (10⁰, 11⁰) эффективно; для его понимания полезно его провести, скажем, для частного случая группы вращений квадрата ◄

15⁰ Отображение $G\times M \to M$, $(g,m)\mapsto gm$ прямого произведения $G\times M$ группы G на множество М называется (левым) действием G на М, если
(1) $\forall m \in M \quad em = m$
(2) $\forall a,b \in G \ \forall m \in M \quad (ab)m = a(bm)$.

Каждое действие G на М определяет гомоморфизм G в $Bij\,M$ и обратно (К 302) ◄

16⁰ Циклической группой порядка n называется группа поворотов правильного n-угольника (обозначение - $\mathbb{Z}_n$). Группу $(\mathbb{Z}, +)$ иногда называют бесконечной циклической.

Лекция II ПОДГРУППЫ И ФАКТОР-ГРУППЫ

1⁰ Пусть $H = \{e = h_1, h_2, \dots, h_k\}$ подгруппа (I, 8⁰) конечной группы G из n элементов $\{e = g_1, \dots, g_n\}$. Тогда множество
$$aH = \{a, ah_2, \dots, ah_k\}$$
называется левым смежным классом элемента а относительно подгруппы Н. Все его элементы различны ◄ и ни одни из них не входят в Н если $a \notin H$ ◄

2⁰ Если $b \notin H$ и $b \notin aH$, то элементы смежного класса
$$bH = \{b, bh_2, \dots, bh_k\}$$
все различны и ни один из них не входит ни в Н, ни в aH ◄

3⁰ Продолжая таким образом, мы получим разбиение множества G на классы (которые отвечают отношению эквивалентности $a \sim b \Leftrightarrow a^{-1}b \in H$) ; в каждом из них - k элементов, поэтому к делит n.

4^0 Порядком группы $\operatorname{ord} G$ называется число ее элементов; порядком элемента $a \in G$ – наименьшее число $k = \operatorname{ord} a$, такое, что $\underbrace{aa \cdots a}_{k} = e$; индексом подгруппы $H \subset G$ – число смежных классов (см. 3^0); индекс обозначается $[G:H]$. Мы показали, что

$$(\operatorname{ord} H)[G:H] = \operatorname{ord} G$$

Словами это обычно формулируется так:

Теорема Лагранжа. Порядок подгруппы – делитель порядка (конечной) группы.

Следствие. Порядок элемента – делитель порядка конечной группы ◀. Однако не для всякого делителя d порядка группы существует подгруппа порядка d. Например $d=6$ и A_4 ◀ (см Ш, 8^0)

5^0 Любая группа простого порядка p изоморфна группе $\mathbb{Z}_p$ ◀

6^0 Конструкция тезисов 1^0 – 3^0 обобщается на случай групп любых порядков (снова нужно рассмотреть отношение $a \sim b \Leftrightarrow a^{-1}b \in H$) ◀ В общем случае индекс $[G:H]$ может быть бесконечным. Кроме левых смежных классов, можно рассматривать правые: $a \sim b \Leftrightarrow ab^{-1} \in H$ ◀

7^0 Пусть дана подгруппа $H \subset G$; будем обозначать через $\bar{a}$ смежный класс (например, левый) содержащий элемент a. Естественно определить операцию в множестве смежных классов, положив $\bar{a}\,\bar{b} = \overline{ab}$. К сожалению, это определение не корректно: в качестве примера рассмотрите $S_3 \supset \{[123],[132]\} = H$ ◀

8^0 Предыдущий тезис показывает, что понятие подгруппы – не адекватное для факторизации. Для этого служит понятие нормальной подгруппы (говорят еще – "нормальный делитель"): это такая подгруппа, все правые смежные классы которой совпадают с левыми, т.е. $\forall g \in G \ \ gH = Hg$.

9^0 Любая подгруппа абелевой группы – нормальная ◀

10^0 Если H – нормальная подгруппа G, то в множество (левых = правых) смежных классов можно ввести операцию (см. 7^0) по формуле $\bar{a}\,\bar{b} = \overline{ab}$; получится снова группа ◀, которая называется фактор-группой G по H и обозначается G/H.

11^0 Примеры: $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$, $\mathbb{Z}_6/3\mathbb{Z}_6 \cong \mathbb{Z}_2$, $S_n/A_n = \mathbb{Z}_2$.

12^0 Гомоморфизмом $\varphi : G \to H$ группы G в группу H называется отображение, сохраняющее операцию, т.е. обладающее свойством

$$\forall a,b \in G \quad \varphi(ab) = \varphi(a)\varphi(b)$$

(здесь пустым символом обозначено как умножение в G, так и в H). Ядром гомоморфизма называется множество $\mathrm{Ker}\,\varphi=\{a\in G, \varphi(a)=1\}$ образом - множество $\mathrm{Im}\,\varphi=\varphi(G)=\{b\in H, \exists a\in G\ \varphi(a)=b\}$

I3⁰ Ядро любого гомоморфизма - нормальная подгруппа ◀

I4⁰ Обратно, любая нормальная подгруппа $H\subseteq G$ является ядром некоторого гомомоморфизма, именно т.н. канонического гомоморфизма (или проэкции) $pr: G\to G/H$, определенного правилом $a\mapsto \bar{a}$, где а - смежный класс G по H, содержащий элемент а ◀.

I5⁰ Если $H\subset G$ нормальная подгруппа, то последовательность

$$0\to H \xrightarrow{\subseteq} G \xrightarrow{pr} G/H \to 0$$

которую называют короткой точной последовательностью, обладает свойством точности: образ каждого гомоморфизма совпадает с ядром следующего ◀

I6⁰ Гомоморфизм $\varphi: G\to H$ называется эпиморфизмом, если $\mathrm{Im}\,\varphi=H$ и мономорфизмом, если $\mathrm{Ker}\,\varphi=1$ (последнее условие эквивалентно инъективности φ ◀).

I7⁰ Последовательность гомоморфизмов $0\to A\xrightarrow{\varphi} B\to 0$ точна $\Leftrightarrow$ φ - изоморфизм

Лекция Ш КОНЕЧНЫЕ И КОНЕЧНО-ПОРОЖДЕННЫЕ АБЕЛЕВЫ ГРУППЫ

I⁰ Прямым произведением группы G и H называется множество $G\times H=\{(g,h), g\in G, h\in H\}$ с покоординатным умножением; $(g,h)(g',h')=(gg',hh')$; $G\times H$ с такой операцией - группа ◀. Если G и H абелевы,(а иногда и в общем случае), прямое произведение называют прямой суммой и обозначают $\oplus$; это, очевидно, тоже абелева группа.

2⁰ Говорят, что группа G является внутренним прямым произведением своих подгрупп H_1 и H_2, если

$$\forall g\in G\ (\exists!\ h_1\in H_1, h_2\in H_2)\quad g=h_1h_2$$

Внутренне прямое произведение - частный случай определения I⁰ (которое иногда называют "внешним"), т.е. $G\cong H_1\times H_2$ ◀

3⁰ Пример: $\mathbb{Z}_2\oplus\mathbb{Z}_2\cong$(группа изометрий прямоугольника)◀

4⁰ Свободной абелевой группой ранга r называется любая группа, изоморфная прямой сумме $\mathbb{Z}\oplus\mathbb{Z}\oplus\ldots\oplus\mathbb{Z}$ из r

слагаемых.

5^0 Системой образующих $S=\{g_\alpha, \alpha\in J\}$ для группы G называется набор элементов g_α из G, таких, что любой элемент $g\in G$ представим в виде их конечного произведения: $g=g_{\alpha_1}\cdots g_{\alpha_n}$, $\alpha_i\in J$. Группа называется конечно порожденной, если у нее есть конечная система образующих.

6^0 Задача. Для любой конечно порожденной абелевой группы G существует число r и эпиморфизм $\varphi: \overbrace{\mathbb{Z}\oplus\ldots\oplus\mathbb{Z}}^{r}\to G$ ◀

7^0 В этой лекции будут рассказаны структурные теоремы, описывающие все конечные абелевы и все конечно- порожденные абелевы группы.

8^0 Пусть $p^n m$, где p простое и не делит m, а группа G - конечна (не обязательно абелева). Тогда в G существует подгруппа порядка p^n ◀* , называемая силовской. Любые две силовские подгруппы $H_1, H_2\subset G$ сопряжены, т.е. для некоторого элемента $g\in G$ имеем $gH_1g^{-1}=H_2$ ◀*

9^0 Любая конечная абелева группа является прямой суммой своих силовских подгрупп ◀* Каждая из этих подгрупп является p-группой, т.е. порядок любого ее элемента - степень простого числа p ◀

10^0 Любая конечная абелева p-группа - прямая сумма циклических ◀*

11^0 Разложение из тезиса 10^0 единственно в том смысле, что число слагаемых в двух таких разложениях одинаково, и порядки слагаемых тоже одинаковы (при надлежащем упорядочении этих слагаемых)◀*

12^0 Множество элементов конечного порядка в любой конечно порожденной абелевой группе G является конечной подгруппой $T\subset G$ ◀ (Указание: сперва доказать, что T - конечно порождена ◀)

13^0 В обозначениях предыдущего тезиса, G/T - свободная абелева группа некоторого ранга r ◀. Более того, в G найдется подгруппа $S\subset G$, изоморфная G/T, такая, что $G\cong S\oplus T$ ◀ т.е. любая конечно порожденная абелева группа является прямой суммой конечной (абелевой) группы и свободной (абалевой) группы некоторого ранга $r<\infty$.

14^0 Специальной таблицей назовем набор чисел:

$$\begin{array}{lll}
r \geqslant 0 & p_1 & r_1^{(1)} \geqslant r_2^{(1)} \geqslant \ldots \geqslant r_{k_1}^{(1)} \geqslant 1 \\
& \vee & \\
& p_2 & r_1^{(2)} \geqslant r_2^{(2)} \geqslant \ldots \geqslant r_{k_2}^{(2)} \geqslant 1 \\
& \vee & \\
& \vdots & \ldots \qquad\qquad \ldots \\
& \vee & \\
& p_s & r_1^{(s)} \geqslant r_2^{(s)} \geqslant \ldots \geqslant r_{k_s}^{(s)} \geqslant 1
\end{array}$$

где $p_1, \ldots, p_s$ – простые, $r, r_1^{(1)}, \ldots, r_{k_s}^{(s)}$ – целые, $K_i \geqslant 1$. Каждой специальной таблице отвечает следующая группа

$$[\underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}^{r}] \oplus [\mathbb{Z}_{p_1^{r_1^{(1)}}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{r_{k_1}^{(1)}}}] \oplus \ldots \oplus [\mathbb{Z}_{p_s^{r_1^{(s)}}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{r_{k_s}^{(s)}}}] \quad (*)$$

15^0 Итог этой лекции подводит следующая теорема

Для любой конечно порожденной абелевой группы G существует ровно одна специальная таблица такая, что G изоморфна прямой сумме (*), отвечающей этой таблице.

16^0 Аналогично можно сформулировать теорему о классификации конечных абелевых групп (из таблицы убрать число r, из формулы (*) – первую квадратную скобку). ◀

17^0 Доказательства тезисов 8^0–11^0 – см. К 333-343, тезисов 12^0–15^0–в книге С.Ленга "Алгебра" или Ван дер Вардена "Современная алгебра".

Лекция IУ: ОПРЕДЕЛЕНИЕ И ПРИМЕРЫ ПОЛЕЙ И КОЛЕЦ

1^0 Определение поля: множество F с двумя коммутативными операциями $+, \cdot$ (называемыми сложением и умножением) такими что умножение дистрибутивно относительно сложения и $(F, +)$, $(F \setminus 0, \cdot)$ – (абелевы) группы. Здесь 0 – нуль (нейтральный элемент относительно сложения), а нейтральный элемент относительно умножения называется единицей : 1. Простейшие примеры: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ (см. ниже тезис 9^0), $\mathbb{A}$ (алгебраические числа).

2^0 Определение кольца : множество К, с двумя операциями $+, \cdot$, называемыми сложением и умножением, такими, что умножение дистрибутивно слева и справа относительно сложения и $(K,+)$ –абелева группа. Примеры: $\mathbb{Z}$, (кольца вычетов : $\mathbb{Z}/m\mathbb{Z}$ (см. тезис 9^0), кольца многочленов $F[x]$ над лданным полем F ◀ ,кольца функций ◀

Типы колец: ассоциативные, с единицей, коммутитивные, целостные (К 183-185).

3° Обычные свойства операций $+$ и $\cdot$, например $(-a)(-b)=ab$, легко следуют из аксиом (К 175). ◀

4° Делители нуля в кольце: это такие отличные от нуля элементы, произведение которых - нуль. В кольце они могут быть (8°), в поле - нет ◀.

5° Очевидным образом определяется понятие подкольца и подполя ◀. Если E подполе F, то говорят еще, что F расширение E; эта терминология имеет важное психологическое и историческое значение (ибо $\mathbb{R}$ и $\mathbb{C}$ получились последовательным расширением $\mathbb{Q}$).

6° Также как понятие подгруппы, понятие подкольца не адекватно для факторизации ◀. Для этой цели нужен идеал : подкольцо $J\subset K$ такое, что $\forall a\in J\ \forall b\in K\ ab\in J, ba\in J$ (если выполнено только первое включение, говорят, что J - левый идеал, если второе - правый; при выполнении обоих вместо "идеал" говорят иногда двусторонний идеал). Если J идеал кольца K, то K разбивается на смежные классы отношением эквивалентности $a\sim b \Leftrightarrow ab^{-1}\in J$ ◀, в полученное множество кдассов вводится естественная структура кольца ◀ ; это кольцо называется фактор-кольцом кольца K по идеалу J ; обозначение K/J.

7° Множество $3\mathbb{Z}$ чисел, кратных 3, образует идеал в кольце $\mathbb{Z}$ ◀ Фактор-кольцо "вычетов по модулю 3" $\mathbb{Z}/3\mathbb{Z}=\{\bar 0,\bar 1,\bar 2=-1\}$ является полем ◀.

8° Множество $4\mathbb{Z}$ -идеал в $\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ кольцо, но не поле, т.к. содержит делитель нуля: $\bar 2\cdot\bar 2=\bar 0$.

9° Теоремка. $\mathbb{Z}/m\mathbb{Z}$ поле $\Leftrightarrow$ m -простое.

10° ($\Rightarrow$) Если $m=kl$, то $\bar k\cdot\bar l=\overline{kl}=\bar m=\bar 0$ делители нуля!

11° ($\Leftarrow$) Ограничимся доказательством существования обратного элемента для $\bar k\in\mathbb{Z}/m\mathbb{Z}$. Имеет место равенство множеств

$$\{\bar 1\,\bar k, \bar 2\,\bar k, \dots, \overline{(m-1)}\,\bar k\}=\{\bar 1,\bar 2,\dots,\overline{m-1}\}$$ ◀

Но в них столько же элементов, поэтому для некоторого $l<m$ будет $\bar 1=\bar l\,\bar k$, значит $\bar l=\bar k^{-1}$. Остальные аксиомы тривиальны. ◀

12° Задача. Доказать, что из теоремки 9° следует Малая теорема Ферма. Если простое число p не делит $m\in\mathbb{N}$, то m^{p-1} есть единица по модулю p.

13^0 Теоремка 9^0 наводит на мысль, что число элементов в конечном поле – простое. Это неверно – существует поле из 4 элементов: $GF(4)=\{0,1,i,1+i\}$ где $i^2=1+i$ ◀

14^0 Идеал $\mathcal{J}\subset\mathcal{K}$ называется максимальным, если он не содержится ни в каком другом идеале (отличном от К). Например, $3\mathbb{Z}\subset\mathbb{Z}$ – максимальный идеал, $6\mathbb{Z}$ – нет ◀. Любой отличный от К идеал содержится в максимальном идеале (отличном от К) ◀.

15^0 Пример: $m\mathbb{Z}\subset\mathbb{Z}$ максимален $\Leftrightarrow m$ – простой ◀. Из этого факта и следующего тезиса получается новое доказательство 9^0 ◀.

16^0 Теоремка 9^0 наводит на следующую (правильную!) мысль: Фактор-кольцо по максимальному идеалу – поле ◀. Обратно, если $K/\mathcal{J}$ – поле, то идеал $\mathcal{J}$ – максимальный. ◀

К-комм. кольцо с 1

17^0 Если $f(x)\in P[x]$ неприводимый многочлен[1], то он порождает максимальный идеал ◀, и значит фактор

$$P[x]/(f(x))$$

– поле. Например $\mathbb{C}=\mathbb{R}[x]/(x^2+1)$, $GF(4)=\mathbb{Z}_2[x]/(x^2+x+1)$ ◀

Лекция V: КОНЕЧНЫЕ ПОЛЯ, АЛГЕБРАИЧЕСКИЕ РАСШИРЕНИЯ

1^0 Характеристика поля. В (произвольном) поле F рассмотрим цепочку $1,\ 1+1,\ 1+1+1, \ldots\ldots$ $(*)$

Тогда возможны два случая: либо в цепочке все элементы не нулевые, либо для некоторого m имеем $\overbrace{1+\ldots+1}^{m}=0$.

2^0 Если все элементы цепочки $(*)$ отличны от нуля, то поле F называется полем нулевой характеристики (обозн. $\mathrm{char}\,F=0$; примеры: $\mathbb{R},\mathbb{Q},\mathbb{C}$); в этом случае F содержит в качестве подполя поле, изоморфное $\mathbb{Q}$ ◀.

3^0 Если $\bar{m}=\overbrace{1+\ldots+1}^{m}$ первый равный нулю элемент в цепочке $(*)$, то число $m=p$ – простое ◀. Тогда F называется полем характеристики p ($\mathrm{char}\,F=p$) и содержит в качестве подполя поле, изоморфное $\mathbb{Z}/p\mathbb{Z}$ ◀.

4^0 Построение поля $GF(8)$. Начнем с поля $\mathbb{F}_2=\mathbb{Z}/2\mathbb{Z}=\{\bar{0},\bar{1}\}$ и рассмотрим многочлен $x^3+x+1\in\mathbb{F}_2[x]$. Он неприводим ◀.

Рассмотрим множество из восьми элементов:

$$GF(8)=\{a_0+a_1\alpha+a_2\alpha^2;\ a_i\in\mathbb{F}_2\}.$$

----

1) т.е. многочлен, не представимый в виде произведения многочленов меньших степеней.

Введем операции $+, \cdot$ в множество $GF(8)$, как сложение и умножение многочленов из $\mathbb{F}_2[x]$, сокращая результат по соотношению $\alpha^3+\alpha+1=0$ (т.е. используя равенства $\alpha^3=\alpha+1, \alpha^4=\alpha^2+\alpha$). Так, например, $(1+\alpha+\alpha^2)^{-1}=\alpha^2, (\alpha+\alpha^2)(1+\alpha^2)=?$ Получим поле. ◀

5^0 Конструкция тезиса 4 может быть записана короче

$$GF(8)=\mathbb{F}_2[x]/(x^3+x+1)$$

где (x^3+x+1) идеал, порожденный многочленом x^3+x+1. ◀

6^0 Общая конструкция поля Галуа $GF(p^n)$, где $p,n\in\mathbb{N}$, p – простое

$$GF(p^n)=\mathbb{F}_p[x]/(f_n(x))$$

где $\mathbb{F}_p\cong\mathbb{Z}/p\mathbb{Z}$, $f_n(x)\in\mathbb{F}_p[x]$-неприводимый многочлен степени n ◀

7^0 Задача: для любого простого p и любого $n\in\mathbb{N}$ существует неприводимый многочлен $f(x)\in\mathbb{F}_p[x]$ степени n ◀.

8^0-12^0: Описание конечных полей. Пусть K – конечное поле. Тогда существует простое p, такое, что $\operatorname{char}K=p$ и K – расширение поля $\mathbb{F}_p\cong\mathbb{Z}/p\mathbb{Z}$ ◀ (ср. 2^0).

9^0 Пусть K – конечное поле характеристики p. Тогда для некоторого $n\in\mathbb{N}$, число элементов K равно $q=p^n$. ◀

10^0 Мультипликативная группа конечного поля K характеристики p состоит из $q-1$ элементов ($q=p^n$), поэтому для любого $\alpha\in K\setminus 0$ имеем $\alpha^{q-1}=1$ ◀, откуда любой элемент поля K является корнем многочлена

$$x^{p^n}-x\in\mathbb{F}_p[x] \qquad (**)$$

11^0 Если поле K состоит из всех корней многочлена $(**)$, то это условие его определяет однозначно с точностью до изоморфизма ◀ (К 428).

12^0 Итогом тезисов 6^0-11^0 является следующая структурная теорема:

Теорема. Для любого натурального n и простого p существует поле из p^n элементов; оно называется полем Галуа и обозначается $GF(p^n)$. Любое конечное поле изоморфно одному из полей $GF(p^n)$.

13^0 Задача. Мультипликативная группа конечного поля – циклическая ◀.

14^0-20^0. Построение алгебраически замкнутого расширения произвольного поля K. Поле E называется алгебраически замкнутым, если любой многочлен $f(x)\in E[x]$ имеет корень $\alpha\in E$. (таково $\mathbb{C}$, но не $\mathbb{R}$). Последовательно расширяя K, будем строить алгебраически замкнутое расширение $E \supset K$.

15° <u>Нулевой шаг</u> (ср. 6°). Если $f(x) \in K[x]$ (неприводимый) многочлен, то канонический эпиморфизм (факторизация) ϕ: $K[x] \to K[x]/(f(x))$ порождает мономорфизм полей◄:

$$\sigma : K \to (\phi(K))(\xi) = \widetilde{F},$$

где поле $\widetilde{F}$ получается из подполя ϕ(K) присоединением элемента (ср. IУ, 13°) $\xi = \phi(x)$ (здесь x рассматривается как многочлен $x \in K[x]$), притом многочлен (вернее, класс многочленов) σf имеет корень $\xi \in \widetilde{F}$ ◄

I 16° <u>Первый шаг. Для любого поля К и многочлена $f(x) \in K[x]$ существует расширение $F \supset K$, в котором $f(x)$ имеет корень.</u> Действительно, не нарушая общность, можно считать, что f - неприводим ◄ ; далее, пользуясь 15°, в множество $F = K \cup S$ (где S - множество символов, биективно отображающееся на $\widetilde{F} \setminus \sigma$(K)) легко внести (пользуясь естественной биекцией $\tilde{\sigma} : F \to \widetilde{F}$) структуру поля ◄ , притом $f(\alpha)=0$, где $\alpha = \tilde{\sigma}^{-1}(\xi)$ ◄

17° <u>Второй шаг</u> . ("конструкция Артина"). Рассмотрим множество символов

$$\mathcal{S} = \{ x_f , f \in K[x] \}$$

и кольцо $K[\mathcal{S}]$ многочленов от многих переменных $x_f \in \mathcal{S}$ с коэффициентами в К (хотя $\mathcal{S}$ - бесконечно, в каждый $\varphi \in K[\mathcal{S}]$ входит лишь конечное число переменных x_f).

18° Идеал, порожденный многочленами вида $f(x_f)$, $f \in K[x]$ (индекс f <u>тот же</u>, что сам многочлен!) не содержит 1. Действительно, в противном случае для некоторых $f_i \in K[x]$ и $g_i \in K[\mathcal{S}]$, мы имели бы $\sum_{i=1}^{N} g_i f_i(x_{f_i}) = 1$; расширив К последовательно с помощью $f_1, \dots, f_N$ (см. 16°) до поля F_N , в котором $f_1, \dots, f_N$ имеют корни $\alpha_1, \dots, \alpha_N$, и подставив вместо x_{f_i} числа α_i (и нули вместо остальных x'ов), мы получили бы 0=1 в поле F_N ◄

19° Пусть J максимальный идеал в $K[\mathcal{S}]$, порожденный многочленами $f(x_f)$, $f \in K[x]$; тогда $\widetilde{E}_1 = K[\mathcal{S}]/J$ - поле ◄ , содержащее изоморфный образ К ◄ . Применяя трюк из 16°, легко построить расширение $E_1 \supset K$, в котором любой многочлен $f \in K[x]$ имеет корень $\alpha \in E_1$ ~~$\alpha \in K_1$~~ ◄

20° <u>Последний шаг</u>. Построим последовательность расширений (по 19°)

$$K \subset E_1 \subset E_2 \subset \dots \subset E_n \subset \dots$$

в которой любой многочлен из $E_i[x]$ имеет корень в E_{i+1} . Положим

$$E = \bigcup_{i=1}^{\infty} E_i$$

.

и введем в E структуру поля, порожденную E_i -ыми ◀ . Тогда $K \subset E$ и любой многочлен из $E[x]$ имеет в E корень ◀ . Нами доказана

Теорема. Любое поле имеет алгебраическое замкнутое расширение.

21⁰ Задача. Докажите теорему из тезиса 20⁰ для случая конечных полей, пользуясь естественной цепочкой включений $GF(p^n) \subset GF(p^{n!}) \subset GF(p^{(n+1)!}) \subset \ldots \subset GF(p^{(n+k)!}) \subset \ldots$ ◀

22⁰ Задача. Докажите теорему единственности (тезис 12⁰), взяв алгебраически замкнутое расширение E поля $\mathbb{F}_p$, где p - характеристика данного поля K, и доказав, что поле, изоморфное K, лежит в E и описывается как множество неподвижных элементов гомоморфизма $E \to E$ заданного правилом $E \ni x \mapsto x^{p^n} \in E$. (Указание: $x^{p^n} - x$ не имеет кратных корней, как показывает подсчет его производной ◀)◀.