Уничтожаем Алгебру

Семенов Михаил, Солонков Денис. 161 группа

12 апреля 2018 г.

Содержание

1 Множества с бинарной операцией, полугруппы, моноиды и группы. Коммутативные группы. Порядок группы. Примеры групп.

Множество M с заданной функцией $\circ : M \times M \to M$. Называется множеством с бинарной операцией, обозначается как $(M, \circ)$. Для этой конструкции полезно выделить следующие свойства:

1. Ассоциативность — $\forall a, b, c \in M : a \circ (b \circ c) = (a \circ b) \circ c$.
2. Существование нейтрального элемента(единицы) — $\exists e \in M : \forall a \in m, a \circ e = e \circ a = a$.
3. Существование обратного элемента — $\forall a \in M, \exists b \in M : ab = ba = e$, где e – обратный элемент. Для элемента a обратный принято обозначать a^{-1}.
4. Коммутативность — $\forall a, b \in M : ab = ba$.

Множество удовлетворяющее условию 1 называют полугруппой.
Множество удовлетворяющее условиям 1-2 называют моноидом.
Множество удовлетворяющее условиям 1-3 называют группой.
Множество удовлетворяющее условиям 1-4 называют абелевой группой(или коммутативной).
Интересные факты про эти множества:

1. В моноиде существует не более одного нейтрального элемента. Пруф: пусть их хотя бы 2 : e_1, e_2. Тогда $e_1 = e_1 \circ e_2 = e_2$.
2. В группе существует не более одного обратного элемента. Пруф: пусть у элемента a их 2 : b, c, но тогда $b = be = bac = ec = c$, ч.т.д.

Теперь нужно сделать несколько вещей:

1. Забыть про полугруппы и моноиды (если не хотите, то можете почитать книжку Винберга).
2. Допустим некоторую халяву и в группе будем писать ab подразумевая $a \circ b$.
3. Если понятно о какой операции в группе идет речь, то тоже будем её опускать при написании и писать не $(G, \circ)$, а G.
4. В группе вместо $\circ$ отныне будем юзать $\cdot$, а в абелевой $+$.
5. $g^1 = g, \forall n > 1 : g^n = g^{n-1} \cdot g, \forall n < -1 : g^n = g^{-1} \cdot g^{n+1}$

Порядком группы называется число элементов в ней, обозначается как $|G|$.
Примечание: $|(\mathbb{Z}, +)| = \infty$.
Примеры групп: $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q} \setminus \{0\}, \cdot), (Z_p, +)$. *последнее это остатки по модулю p.*
Некоторые специальные группы:

1. $\mathbb{GL}_n(\mathbb{R})$ — группа матриц с ненулевым определителем.
2. $\mathbb{SL}_n(\mathbb{R})$ — группа матриц с единичным определителем.
3. S_n — группа подстановок длины n.

2 Подгруппы. Циклические подгруппы. Порядок элемента. Циклические группы.

Определение 2.1. Подмножество H группы G называется подгруппой, если:

1. $e \in H$
2. $\forall a, b \in H : ab \in H$
3. $\forall a \in H : a^{-1} \in H$

Все три условия выше можно переписать, как: H непусто и $\forall a, b \in H : ab^{-1} \in H$

Иногда может оказаться так, что подгруппа порождается одним элементом. Например, множество всех четных чисел в $\mathbb{Z}$ порождается числом 2. Более формально:

Определение 2.2. Пусть G группа и $g \in G$. Циклической подгруппой, порожденной элементом g называется подмножество: $\{g^n | n \in \mathbb{Z}\}$. Такая подгруппа обозначается, как $\langle g \rangle$.

В качестве примера возьмем множество всех четных чисел в $\mathbb{Z}$, то есть $2\mathbb{Z}$. В качестве порождающего элемента можно взять -2 или же 2. То есть $2\mathbb{Z} = \langle -2 \rangle = \langle 2 \rangle$.

Определение 2.3. Порядком элемента g называется такое минимальное натуральное число m, что $g^m = e$. Если такого числа не существует, то порядок элемента равен бесконечности. Порядок элемента обозначается, как $ord(g)$

Так как и у группы и у элемента есть понятие порядок, хотелось бы как то их между собой связать.

Теорема 2.1. Пусть G группа и $g \in G$. Тогда $ord(g) = |\langle g \rangle|$.

Доказательство. Самое важное наблюдение, которое необходимо сделать, это то, что если $g^a = g^b$, то $g^{a-b} = e$. Если $ord(g)$ равен бесконечности, то из описанных выше соображений, в цепочке $g^1, g^2, \ldots$ нет одинаковых элементов, а значит размер $\langle g \rangle$ также равен бесконечности.

Если же $ord(g) = m$, то так как число m минимально возможное, то в цепочке $e, g, \ldots, g^{m-1}$ нет одинаковых элементов. А теперь заметим, что:

$$i = qm + r, r \in [0, m-1]$$
$$g^i = (g^m)^q g^r = e^q g^r = g^r$$

Значит $|\langle g \rangle| = m$, что и требовалось доказать. □

Мы уже определили понятие циклической подгруппы, так что давайте пойдем дальше и определим циклическую группу/

Определение 2.4. Группа G называется циклической, если $\exists g \in G : G = \langle g \rangle$.

3 Смежные классы. Индекс подгруппы. Теорема Лагранжа.

Определение 3.1. Пусть G - группа, $H \subseteq G$ подгруппа и $g \in G$. Левым смежным классом элемента g группы G по подгруппе H называется подмножество:

$$gH = \{gh | h \in H\}$$

Существует также правый смежный класс, который определяется весьма похожим образом, но мы не будем ударяться в политику и просто будем пользоваться левым смежным классом.

Хоть это и не совсем очевидно, но понятие левого смежного класса весьма полезно. Например, для двух разных элементов их левые смежные классы по одной и той же подгруппе H либо совпадают, либо не пересекаются. Докажем это сильное утверждение.

Лемма 3.1. Пусть G - группа, $H \subseteq G$ - подгруппа и $g_1, g_2 \in G$. Тогда либо $g_1H = g_2H$, либо $g_1H \cap g_2H = \varnothing$

Доказательство. Предположим, что $g_1H \cap g_2H \neq \varnothing$, то $\exists h_1, h_2 \in H : g_1h_1 = g_2h_2$. Докажем, что тогда $g_1H = g_2H$, то:

$$\begin{aligned}
&g_1h_1 = g_2h_2 \\
&g_1 = g_2h_2h_1^{-1} \\
&g_1H = g_2h_2h_1^{-1}H \subseteq g_2H \\
&g_1h_1 = g_2h_2 \\
&g_2 = g_1h_1h_2^{-1} \\
&g_2H = g_1h_1h_2^{-1}H \subseteq g_1H
\end{aligned}$$

Из чего следует, что $g_1H = g_2H$, что и требовалось доказать. □

Также, мы можем даже сказать интересные вещи о размере получившегося левого смежного класса.

Лемма 3.2. Пусть G группа и $H \subseteq G$ - конечная подгруппа. Тогда $\forall g \in G : |gH| = |H|$

Доказательство. Из определения левого смежного класса $|gH| \leq |H|$. Также заметим, что если:

$$\begin{aligned}
&gh_1 = gh_2 \\
&g^{-1}gh_1 = g^{-1}gh_2 \\
&h_1 = h_2
\end{aligned}$$

Значит $|gH| = |H|$ что и требовалось доказать. □

Теперь, когда мы доказали, что для любых двух элементов левые смежные классы либо равны, либо пересекаются, то мы можем ввести определения индекса подгруппы.

Определение 3.2. Пусть G группа и $H \subseteq G$ - подгруппа. Индексом подгруппы H в группе G называется число левых смежных классов G по H и обозначается он, как: $[G : H]$.

И теперь, мы наконец подошли к первой серьезной теореме: теореме Лагранжа

Теорема 3.3. Пусть G - конечная группа и $H \subseteq G$ подгруппа. Тогда $|G| = |H| \cdot [G : H]$.

Доказательство. Мы доказали, что наша группа разобьется на непересекающееся множество левых смежных классов и их количество равно $[G : H]$. Мы доказали, что размер каждого из них равен $|H|$. Значит $|G| = |H| \cdot [G : H]$. □

4 Пять следствий из теоремы Лагранжа.

4.1 Первое следствие.

Пусть G - конечная группа и $H \subseteq G$ - подгруппа. Тогда $|H|$ делит $|G|$.

4.2 Второе следствие.

Пусть G - конечная группа и $g \in G$, тогда $ord(G)$ делит $|G|$. Это следует из того, что $|\langle g \rangle| = ord(g)$.

4.3 Третье следствие.

Пусть G - конечная группа и $g \in G$. Тогда $g^{|G|} = e$. Это напрямую следует из второго следствия.

4.4 Четвертое следствие

Пусть a - ненулевой вычет по простому модулю p. Тогда $a^{p-1} = 1$. Для этого возьмем группу $\mathbb{Z}_p / \{0\}$ и воспользуемся третьим следствие.

4.5 Пятое следствие

Пусть G - группа, причем $|G| = p$, где p - простое число. Тогда G циклическая группа, порождаемся любым своим неединичным элементом.

Доказательство. Пусть $g \in G$ неединичный элемент. Тогда $|\langle g \rangle| > 1$ и оно делит G. Так как $|G|$ простое число, то $\langle g \rangle| = |G|$, что и требовалось доказать. □

5 Нормальные подгруппы и факторгруппы.

Определение 5.1. Подгруппа $H \subseteq G$ называется нормальной, если $\forall g \in G : gH = Hg$.

Хотелось бы определить какие-то критерии нормальности, ибо пока проверять подгруппу на нормальность весьма не удобно

Теорема 5.1. Для подгруппы $H \subseteq G$ следующие условия эквивалентны:

1. H нормальна
2. $\forall g \in G : gHg^{-1} \subset H$.
3. $\forall g \in G : gHg^{-1} = H$

Второе условие кажется весьма бессмысленным, но именно через него проще всего проверять подгруппу на нормальность.

Доказательство. Докажем, что (1) $\Rightarrow$ (2). Так как $gH = Hg$, то $\forall g \in G, h \in H, \exists h' \in H : gh = h'g$. Исходя из этого:

$$\forall g \in G : \forall h \in G : ghg^{-1} = h'gg^{-1} = h' \in H$$
$$gHg^{-1} \subseteq H$$

Теперь докажем, что (2) $\Rightarrow$ (3). По факту нам просто остается доказать обратное включение, то есть, что $H \subseteq gHg^{-1}$. Ну:

$$h = g^{-1}ghg^{-1}g = g^{-1}(ghg^{-1})g$$
$$ghg^{-1} \in H \Rightarrow ghg^{-1} = h'$$
$$h = g^{-1}(ghg^{-1})g = g^{-1}h'g \in gHg^{-1}$$

Что и требовалось доказать. Остается только доказать, что (3) $\Rightarrow$ (1)

$$gH = gHg^{-1}g \subseteq Hg$$
$$Hg = gg^{-1}Hg \subseteq gH$$

Что и требовалось доказать. □

Теперь мы неожиданно захотим воспользоваться левыми смежными классами, а именно - определить на них группу. Обозначим через G/H множество левых смежных классов группы G по нормальной подгруппе H. Определим на G/H бинарную операцию следующим образом:

$$(g_1H)(g_2H) = (g_1g_2H)$$

Где g_1, g_2 являются представителями соответствующих классов. Чтобы эта операция была корректна, нам нужно показать, что результат операции не меняется, если вместо g_1 и g_2 взять других представителей этого класса, то есть, нам надо доказать, что:

$$g_1g_2H = g_1h_1g_2h_2H$$
$$g_1h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2 = g_1g_2h'h_2$$

Что и требовалось доказать. Очевидно, что наша операция ассоциативна, имеет нейтральный элемент и для каждого элемента определен обратный. Значит G/H является валидной группой.

Определение 5.2. Множество G/H с указанной выше операцией называется факторгруппой группы G по нормальной подгруппе H.

Например: $G = (\mathbb{Z}, +), H = n\mathbb{Z}, G/H = (\mathbb{Z}_n, +)$.

6 Гомоморфизмы и изоморфизмы групп. Классификация циклических групп.

Не один раздел математики не является топовым, пока мы не введем в нем что-нибудь, называющееся изоморфизмом. Так что приступим к этому.

Определение 6.1. Пусть G, F - группы. Отображение $\varphi : G \to F$ называется гомоморфизмом, если $\varphi(ab) = \varphi(a)\varphi(b)$.

Лемма 6.1. Пусть $\varphi : G \to F$ - гомоморфизм групп. Тогда:

1. $\varphi(e) = e$
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$

Доказательство.

$$\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$$
$$e = \varphi(e)$$

$$\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e) = e$$

□

Определение 6.2. Гоморфизм $\varphi : G \to F$ называется изоморфизмом, если отображение φ биективно.

Определение 6.3. Группы G, F называются изоморфными, если между ними существует изоморфизм. Обозначение: $G \cong F$.

Все, мы ввели определение изоморфизма, можно расходиться. Однако, наш экзаменатор считает обратное, так что нам придется продолжить. В алгебре изоморфные группы считают ну прям совсем равными, так что пора вернутся к введенным ранее определениям и построить там изоморфизм с чем-нибудь.

Теорема 6.2. Всякая бесконечная циклическая группа G изоморфна группе $(\mathbb{Z}, +)$. Всякая циклическая группа порядка n изоморфна $(\mathbb{Z}_n, +)$.

Доказательство. В первом случае скажем, что $g^k \to k$. Во втором случае, скажем, что $g^k \to k(\ mod\ n)$. □

7 Ядро и образ гомоморфизма групп.Теорема о гомоморфизме.

Определение 7.1. Пусть у нас есть гомоморфизм $\varphi : G \to F$. С ним связано понятие ядра и образа.

$$Ker(\varphi) = \{g \in G | \varphi(g) = e\}$$
$$Im(\varphi) = \{a \in F | \exists g \in G : \varphi(g) = a\}$$

Очевидно, что ядро и образ представляют из себя подгруппы.

Лемма 7.1. Гомоморфизм групп $\varphi : G \to F$ инъективен тогда и только тогда, когда $Ker(\varphi) = \{e\}$

Доказательство. Очевидно, что это условие необходимое. Докажем, что оно является достаточным. Предположим обратное:

$$\varphi(a) = \varphi(b)$$
$$\varphi(a)\varphi(b)^{-1} = e$$
$$\varphi(ab^{-1}) = \varphi(e)$$
$$ab^{-1} \in Ker(\varphi)$$

Противоречие. □

Лемма 7.2. Пусть $\varphi : G \to F$ - гомоморфизм. Тогда $Ker(\varphi)$ нормальна в G

Доказательство. Достаточно проверить, что $g^{-1}hg \in Ker(\varphi)$ для любых $g \in G$ и $h \in Ker(\varphi)$. Докажим это:

$$\varphi(g^{-1}hg) = \varphi(g^{-1})\varphi(h)\varphi(g) = \varphi(g^{-1})\varphi(g) = \varphi(e) = e$$

Что и требовалось доказать. □

Вернемся назад к определению факторгруппы. Это весьма упоротая концепция и зачастую определить, чему равна факторгруппа очень и очень сложно. Но специально для вас есть великая теорема, которая помогает решить эту проблему:

Теорема 7.3. Пусть $\varphi : G \to F$. Тогда группа $Im(\varphi)$ изоморфна $G/Ker(\varphi)$.

Доказательство. Рассмотрим отображение $\psi : G/Ker(\varphi) \to Im(\varphi)$, заданное формулой $\psi(gKer(\varphi)) = \varphi(g)$. Для начала надо проверить, что выбор разных представителей ничего не меняет:

$$\psi(gh) = \psi(g)\psi(h) = \psi(g)$$

По своему построению отображение сюръективно и инъективно в силу того, что $Ker(\psi) = \{0\}$. Остается проверить, что ψ является гомоморфизмом и мы получим изоморфизм:

$$\psi((gKer(\varphi))(g'Ker(\varphi))) = \psi(gg'Ker(\varphi)) = \varphi(gg') = \varphi(g)\varphi(g') = \psi(gKer(\varphi))\psi(g'Ker(\varphi))$$

□

Теперь, чтобы найти, чему равна факторгруппа G/H, достаточно просто найти такой гомоморфизм φ, что $Ker(\varphi) = H$. Тогда $G/H \cong Im(\varphi)$.

8 Центр группы.

Определение 8.1. Центр группы G - это подмножество:

$$Z(G) = \{a \in G | \forall b \in G : ab = ba\}$$

Лемма 8.1. Центр $Z(G)$ является нормальной подгруппой G.

Доказательство. Сначала докажем, что $Z(G)$ является просто подгруппой, а потом займемся нормальностью.

$$\begin{aligned}
&\forall a : ae = ea \Rightarrow e \in Z(G)\\
&a, b \in Z(G) : \forall c \in G, cab = acb = abc \Rightarrow ab \in Z(G)\\
&a \in Z(G) : \forall b \in G :\\
&ag = ga\\
&(ag)^{-1} = (ga)^{-1}\\
&g^{-1}a^{-1} = a^{-1}g^{-1} \Rightarrow a^{-1} \in Z(G)
\end{aligned}$$

Теперь докажем нормальность. Для этого нам надо показать, что $\forall g : gZ(G)g^{-1} \subseteq Z(G)$:

$$\begin{aligned}
&\forall g \in g, a \in Z(G) :\\
&gag^{-1} = gg^{-1}a = a \in Z(G)
\end{aligned}$$

Значит $Z(G)$ является нормальной подгруппой в G. □

9 Прямое произведение групп. Теорема о факторизации по сомножителям.

Определение 9.1. Назовем прямым произведением групп $G_1, \ldots, G_m$ множество:

$$G_1 \times \ldots \times G_m = \{(g_1, \ldots, g_m) | g_1 \in G_1, \ldots, g_m \in G_m\}$$

Определим операцию на этом множестве:

$$(g_1, \ldots, g_m)(g'_1, \ldots, g'_m) = (g_1 g'_1, \ldots, g_m g'_m)$$

Очевидно, что данная операция является валидной и наше множество является группой.

Теорема 9.1. Пусть $G_1, \ldots, G_m$ группы и $H_1, \ldots, H_m$ - нормальные подгруппы соответствующих групп. Тогда:

$$(G_1 \times \ldots \times G_m)/(H_1 \times \ldots \times H_m) \cong G_1/H_1 \times \ldots \times G_m/H_m$$

Доказательство. Очевидно, что $H_1 \times \ldots \times H_m$ является нормальной подгруппой(просто проверка по определению). Построим требуемый изоморфизм следующим образом:

$$(g_1 \ldots g_m)(H_1 \times \ldots \times H_m) \to (g_1 H_1, \ldots, g_m H_m)$$

Проверка выполнения аксиом изоморфизма тривиальна и рассмотрена не будет. □

10 Разложение конечной циклической группы.

Теорема 10.1. Пусть $n = ml$, где m, l - взаимнопростые числа. Тогда $\mathbb{Z}_n \cong \mathbb{Z}_m \times \mathbb{Z}_l$.

Доказательство. Это было в дискретной алгебре. Из КТО мы знаем о существовании требуемого изоморфизма. □

Из этой теоремы следует, что любая $\mathbb{Z}_n$ просто разлагается на произведение, эквивалентное разложению на простые. То есть:

$$n = p_1^{k_1} \times \ldots \times p_n^{k_n}$$
$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_n^{k_n}}$$

11 Конечно порождённая абелева группа. Свободная абелева группа и её ранг. Классификация свободных абелевых групп. Характеризация базисов.

Настало время вспомнить всеми любимый линал.

Определение 11.1. Абелева группа A называется конечно порожденной, если найдутся такие элементы $a_1, \ldots, a_n \in A$, что $\forall a \in A : a = s_1 a_1 + \ldots s_n a_n$. Это почти как базис, но не требуется линейной независимости базисных элементов. Элементы $a_1, \ldots, a_n$ называются порождающими элементами.

Определение 11.2. Абелева группа A называется свободной, если в ней есть базис. Тогда рангом группы называется количество элементов в базисе. $rkA = n$.

Лемма 11.1. Всякая свободная абелева группа ранга n изоморфна группе $\mathbb{Z}^n$

Доказательство. Ну просто заизиморфим элементу его координаты в базисе. □

12 Подгруппа свободной абелевой группы свободна.

Теорема 12.1. Всякая подгруппа N свободной абелевой группы L ранга n является свободной абелевой группой ранга $\leq n$.

Доказательство. Воспользуемся индукцией по n. База: $n = 0$ очевидна.

Переход. Пусть $e_1, \ldots, e_n$ - базис L. Рассмотрим подгруппу:

$$L_1 = \langle e_1, \ldots, e_{n-1} \rangle$$

Теперь рассмотрим $N_1 = N \cap L_1 \subseteq L_1$ и на ней работает наше предположение индукции. Зафиксируем в N_1 базис $f_1, \ldots, f_m$. Рассмотрим отображение:

$$\varphi : N \to Z, s_1 e_1 + \ldots + s_n e_n \to s_n$$

Легко видеть, что φ - гомоморфизм и $Ker(\varphi) = N_1$.

$Im\varphi$ является подгруппой $\mathbb{Z}$ и следовательно, выражается, как kZ. Если $k = 0$, то $N \subseteq L_1$ и $N = N_1$. Если же $k > 0$, то возьмем за f_{m+1} какой-нибудь элемент из N, что $\varphi(f_{m+1}) = k$. Докажем, что полученный набор элементов порождает N:

$$\begin{aligned}
&\forall f \in N : \\
&\varphi(f) = sk, s \in \mathbb{Z} \\
&\varphi(f - sf_{m+1}) = 0 \Rightarrow f - sf_{m+1} \in N_1 \\
&f = sf_{m+1} + s_1 f_1 + \ldots + s_m f_m
\end{aligned}$$

Остается доказать, что полученный набор элементов является базисом. Предположим обратное:

$$\begin{aligned}
&s_1 f_1 + \ldots s_m f_m + s_{m+1} f_{m+1} = s'_1 f_1 + \ldots s'_m f_m + s'_{m+1} f_{m+1} \\
&k s_{m+1} = k s'_{m+1} \\
&s_{m+1} = s'_{m+1} \\
&s_1 f_1 + \ldots s_m f_m = s'_1 f_1 + \ldots + s'_m f_m
\end{aligned}$$

Противоречие с тем, что $f_1, \ldots, f_m$ является базисом. Успех. □

13 Целочисленные элементарные преобразования и алгоритм приведения целочисленной матрицы к диагональному виду.

Слишком просто, так что лениво расписывать. TODO: расписать.

14 Теорема о согласованных базисах.

Слишком просто, так что лениво расписывать. TODO: расписать.

15 Примарные абелевы группы. Классификация конечно порождённых абелевых групп. Разложение конечной абелевой группы в сумму примарных циклических.

Определение 15.1. Конечная абелева группа A называется примарной, если ее порядок равен p^k, где p - простое число.

Теорема 15.1. Пусть A -конечно порожденная абелева группа. Тогда:

$$A \cong Z^m \oplus Z_{p_1^{k_1}} \oplus \ldots \oplus Z_{p_s^{k_s}}$$

Где p_i - простое число, а k_i - простое число. Причем это разложение единственно, с точностью до перестановки.

Доказательство. Для начала мы сделаем подъемное, а именно - докажем существование. Пусть A порождается n элементами a_i. Возьмем и сделаем гомоморфизм:

$$\varphi : \mathbb{Z}^n \to A, (s_1, \ldots, s_n) \to s_1 a_1 + \ldots s_n a_n$$

Очевидно, что φ сюръективен. Применив теорему о гомоморфизме получим, что:

$$\mathbb{Z}^n / Ker(\varphi) \cong A$$

По теореме о согласованном базисе мы можем выбрать такой базис $e_1, \ldots, e_n$ и такие числа $u_1, \ldots, u_m$, что:

$$\begin{aligned}
&\mathbb{Z}^n \cong \langle e_1 \rangle \oplus \ldots \oplus \langle e_n \rangle \\
&Ker(\varphi) \cong \langle u_1 e_1 \rangle \oplus \ldots \oplus \langle u_m e_m \rangle \oplus 0 \oplus \ldots \oplus 0 \\
&A \cong \mathbb{Z}^n / Ker(\varphi) \cong \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m} \oplus \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{n-m}
\end{aligned}$$

Теперь разложим каждый $\mathbb{Z}_{u_1}$ на прямую сумму взаимнопростых чисел и получим искомое.

А теперь, настало время чудовищной боли, а именно - доказательства единственности такого разложения. Обозначим за $\langle c \rangle_q$ циклическую группу порядка q, порождающую c. Мы будем доказывать единственность в несколько стадий. Для начала докажим, что число $\mathbb{Z}$ в разложении A определяется однозначно. Пусть имеется разложение:

$$A \cong \langle c_1 \rangle_{p_1^{k_1}} \oplus \ldots \oplus \langle c_m \rangle_{p_m^{k_m}} \oplus \langle c_{m+1} \rangle_\infty \oplus \ldots \oplus \langle c_{m+t} \rangle_\infty$$

Рассмотрим подгруппу в A, состоящую из все элементов конечного порядка. Такая подгруппа называется подгруппой кручения и обозначается, как $Tor(A)$.

$$a = r_1 c_1 + \ldots + r_m c_m + r_{m+1} c_{m+1} + \ldots + r_n c_n$$

Очевидно, что $a \in Tor(A)$ тогда и только тогда, когда $r_{m+1} = \ldots = r_n = 0$, из чего следует, что:

$$\begin{aligned}
&Tor(A) \cong \langle c_1 \rangle_{p_1^{k_1}} \oplus \ldots \oplus \langle c_m \rangle_{p_m^{k_m}} \\
&A / Tor(A) = \mathbb{Z}^t
\end{aligned}$$

Так как $Tor(A)$ определяется от группы и не зависит от ее конкретного разложения, то из этого следует, что число t определяется однозначно.

Мы доказали, что количество $\mathbb{Z}$ в разложении определяется однозначно. Теперь остается разобраться с группами конечной размерности в нашем разложении. Для начала докажем, что для каждого простого числа p в нашем разложении, сумма показателей степеней определяется однозначно. Определим для каждого простого числа p подгруппу p-кручения:

$$Tor_pA = \{a \in A | \exists k \in \mathbb{N} : p^k a = 0\}$$

Ясно, что $Tor_pA \subseteq TorA$. Легко видеть, что $\langle c_i \rangle_{p_i^{k_i}} \subseteq Tor_pA$, для всех $p_i = p$. Если же $p_i \neq p$, то так как порядок элемента делится на p_i, то $p^k a \neq 0$. Из этого следует, что Tor_pA однозначно определяет сумму показателей степений числа p в разложении.

Благодаря доказанной выше штуке, нам осталось доказать это для случая, когда $|A| = p^k$, то есть A - примарная группа или же:

$$A \cong \langle c_1 \rangle_{p^{k_1}} \oplus \ldots \oplus \langle c_r \rangle_{p^{k_r}}$$

Докажем единственность такого разложения индукцией по k. База: $k = 1, A \cong \mathbb{Z}_p$. Переход:

Рассмотрим подгруппу pA.

$$pA \cong \langle pc_1 \rangle_p^{k_1 - 1} \oplus \ldots \oplus \langle pc_r \rangle_{p^{k_r - 1}}$$

$|pA| = p^{k-r}$. По предположению индукции pA разлагается единственным образом. Из разложения pA мы можем восстановить разложение A единственным образом, прибавим к ненулевым степеням по единичке, и добавив первых степеней, чтобы размер сошелся. □

16 Экспонента конечной абелевой группы и критерий цикличности.

Забудем произошедшее выше, как страшный сон и вместо этого поймем, что мы можем представлять конечные группы, как гораздо более простые конструкции. Из теоремы о согласованных базисах следует, что $A \cong \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m}$, где u_i делит u_{i+1}, где числа $u_1, \ldots, u_m$ называюься инвариантными множителями.

Определение 16.1. Экспонентной конечной абелевой группы A называется число $expA$, равное наименьшему общему кратному порядок элементов из A.

Из разложения выше очевидно, что $expA = u_m$, то есть наибольшему инвариантному множителю. Если же $expA = |A| = u_m$, то $A = \mathbb{Z}_{u_m}$ и $|A| = u_m$.

17 Криптография с открытым ключом. Задача дискретного логарифмирования. Система Диффи-Хеллмана обмена ключами.

Пусть у нас есть конечная группа G и $g \in G$. Для данного элемента $g \in \langle g \rangle$ найти такое натуральное число k, что $h = g^k$. Данная задача называется дискретным логарифмированием.

Пусть два участника хотят определить секретное число для дальнейшего шифрования, пользуясь открытым каналом. Пусть они выберут какое-то большое число g, после чего первый участник выберет число a и сообщит второму g^a, а второй выберет число b и сообщит первому g^b. Далее первый возведет число второго в степень a и получит g^{ab}, также поступит в второй и получит g^{ab}. Так как задача дискретного логарифмирования трудоемка, то мы победили.

18 Криптосистема Эль-Гамаля.

Первый участник сообщает всем число g^a. Пусть второй участник хочет секретно передать первому элемент h. Тогда он выбирает натуральное k и сообщает всем пару $(g^k, h(g^a)^k)$. Теперь, чтобы восстановить число h, $h = (hg^{ak})(g^k)^{|G|-a}$. Так как только A знает число a, то только он сможет восстановить h.

19 Действие группы на множестве. Орбиты и стабилизаторы. Число элементов в орбите.

Мы все это время вводили какие-то определения, доказывали всякие теоремы, но уже давно хотелось какого-то движения, какого-то действия. Итак:

Определение 19.1. Действием группы G на множество X называется отображение $G \times X \to X$, удовлетворяющее следующим условиям:

1. $\forall x \in X : ex = x$.
2. $\forall a, b \in G, x \in X : g(hx) = (gh)x$.

Заметим, что если мы зафиксируем конкретный элемент $g \in G$, то мы определяем отображение $a_g : X \to X$ по правилу $a_g(x) = gx$. Мало того, это отображение еще и биективно:

$$gx_1 = gx_2$$
$$x_1 = x_2$$

Значит, мы можем сказать, что a_g соответствует перестановка из $S(X)$ и наше действие можно определить, как отображение $a : G \to S(X), g \to a_g$. И даже больше того, это отображение является гомоморфизмом:

$$a_{gh}(x) = (gh)x = g(hx) = ga_h(x) = a_g(a_h(x)) = (a_g a_h)(x)$$

Теперь начнем вводить всякие определения про действие

Определение 19.2. Орбитой точки $x \in X$ называется подмножество:

$$Gx = \{x' \in X | \exists g \in G : x' = gx\}$$

Неожиданно оказывается, что орбиты двух точек либо совпадают, либо не пересекаются. Это утверждение эквивалентно следующему:

Лемма 19.1. Для точек $x, x' \in X$ отношение x' лежит в орбите Gx является отношением эквивалентности.

Доказательство. Проверим все аксиомы. Рефлексивность очевидна. Симметричность:

$$x' \in Gx$$
$$x' = gx$$
$$g^{-1}x' = x$$
$$x \in Gx'$$

Транзитивность:

$$x \in Gx_1$$
$$x_1 \in Gx_2$$
$$x = g_1 x_1$$
$$g_1^{-1} x = x_1$$
$$x_1 = g_2 x_2$$
$$g_1^{-1} x = g_2 x_2$$
$$x = g_1 g_2 x_2$$
$$x \in Gx_2$$

□

Определение 19.3. Стабилизатором точки $x \in X$ называется подгруппа:

$$St(x) = \{g \in G | gx = x\}$$

Лемма 19.2. Пусть конечная группа G действует на множество X. Тогда для всякого элемента $x \in X$ справедливо равенство:

$$|Gx| = |G|/|St(x)|$$

Доказательство. Возьмем множество $G/St(x)$ левых смежных классов. Важно отметить, что это не факторгруппа, так как $St(x)$ не обязательно нормальная. Определим отображение $\varphi : G/St(x) \to Gx, gSt(x) \to gx$. Докажем, что отображение не зависит от выбранного представителя:

$$g' = gh, h \in St(x)$$
$$g'x = (gh)x = g(hx) = gx$$

□

Это отображение сюръективно исходя из определения орбиты. Проверим инъективность:

$$g_1 x = g_2 x$$
$$g_2^{-1} g_1 x = x$$
$$g_2^{-1} g 1 \in St(x) \Rightarrow g_2 St(x) = g_1 St(x)$$

Ибо они пересекаются. Значит наше отображение инъективно, а значит оно является биекцией. Следовательно:

$$|Gx| = |G/St(x)| = |G : St(x)| = |G|/|St(x)|$$

Последний переход был проведен по теореме Лагранжа.

20 Транзитивные, свободные и эффективные действия групп. Ядро неэффективности.

Чуть чуть обмажемся классификацией действий:

Определение 20.1. Действие G на X называется транзитивным, если все точки множества X образуют одну орбиту, или другими словами: $\forall x, x' \in X : \exists g : x' = gx$

Определение 20.2. Действие G на X называется свободным, если $\forall x \in X : St(x) = \{e\}$.

Определение 20.3. Действие G на X называется эффективным, если для g выполняется: $\forall x : gx = x$, то $g = e$. Иными словами, пересечение стабилизаторов всех точек равно $\{e\}$.

Определение 20.4. Ядром неэффективности действия группы G на множестве X называется подгруппа:

$$K = \{g \in G | \forall x \in X : gx = x\}$$

Очевидно, что $K = Kera$, где $a : G \to S(X)$ - гомоморфизм, который мы определили выше. Отсюда следует, что K - нормальная подгруппа в G, а значит мы можем рассмотреть факторгруппу G/K и даже, во имя сотоны, определить ее действие на множестве X по формуле $(gK)x = gx$. Очевидно, что это действие является корректным.

Лемма 20.1. Выше определенное действие является эффективным.

Доказательство. Пусть $g \in G$ и $\forall x \in X : (gK)x = x$. Тогда $\forall x \in X : gx = x$ и значит, что $g \in K, gK = K$. □

21 Три действия группы на себе. Изоморфизм действий. Описание свободных транзитивных действий.

По факту, никто не мешает нам взять в качестве множества X саму группу G. После такого выбора сразу напрашиваются 3 достаточно интуитивных действия группы самой на себя:

Определение 21.1. Действие G на G: $(g, h) \to gh$ называтеся действием умножением слева.

Определение 21.2. Действие G на G: $(g, h) \to hg^{-1}$ называтеся действием умножением справа.

Определение 21.3. Действие G на G: $(g, h) \to ghg^{-1}$ называтеся действием сопряжениями.

Первые два действия свободны и транзитивны. Орбиты третьего действия называются классами сопряженности группы G. Настало время сделать понятие действия топовым и определить изоморфизм:

Определение 21.4. Два действия группы G на множества X и Y называются изоморфными, если существует такая биекция $\varphi : X \to Y$, такая что:

$$\forall g \in G, x \in X : \varphi(gx) = g\varphi(x)$$

Лемма 21.1. Всякое свободное транзитивное действие группы G на множестве X изоморфно действию G на себя левыми сдвигами.

Доказательство. Зафиксируем произвольный элемент $x \in X$. Построим отображение $\varphi : G \to X, \varphi(h) = hx$. Сюръективность следует из того, что действие является транзитивным. Инъективность же следует из свободности действия. Значит, φ является биекцией. Остается только проверить свойство изоморфизма:

$$\forall g \in G, g' \in G : \varphi(gg') = (gg')x = g(g'x) = g\varphi(g')$$

Что и требовалось доказать. □

22 Теорема Кэли.

Теорема 22.1. Всякая конечная группа G порядка n изоморфна подгруппе симметрической группы S_n

Доказательство. Рассмотрим действие G на себя умножением слева. Так как это действие свободно, то соответствующий гомоморфизм $a : G \to S(G) \cong S_n$ инъективен и $Ker(a) = \{e\}$. По теореме о гомоморфизме:

$$G/\{e\} \cong G \cong Ima \subseteq S_n$$

Что и требовалось доказать. □

23 Кольца. Коммутативные кольца. Обратимые элементы, делители нуля, нильпотенты и идемпотенты. Примеры колец. Поля. Кольца вычетов. Алгебры над полями.

Определение 23.1. Кольцом называется множество R с двумя бинарными операциями $+$ и $\times$, обладающими следующими свойствами:

1. $(R, +)$ является абелевой группой
2. $a(b + c) = ab + ac, (b + c)a = ba + ca.$
3. $a(bc) = (ab)c$
4. $\exists 1 \in R : a1 = 1a = a$

Сразу можно сказать, что:

$$a0 = a(0 + 0) = a0 + a0 \Rightarrow 0 = a0 = 0a$$

Определение 23.2. Кольцо R называется коммутативным, если $ab = ba$.

Определение 23.3. Элемент $a \in R$ называется обратимым, если $\exists b \in R : ab = ba = 1$.

Определение 23.4. Элемент $a \in R$ называется левым делителем нуля, если $a \neq 0, \exists b \neq 0 \in R : ab = 0$.

Сразу можно заметить, что все делители нуля являются необратимыми:

$$ab = 0$$
$$b = 0$$

Противоречие.

Определение 23.5. Элемент $a \in R$ называется нильпотентом, если $a \neq 0, \exists m \in \mathbb{N} : a^m = 0$.

Определение 23.6. Элемент $a \in R$ называется идемпотентом, если $a^2 = a$.

Определение 23.7. Полем назыается коммутативное ассоциативное кольцо K с единицей, в которой всякий ненулевой элемент обратим.

Лемма 23.1. Кольцо вычетов $\mathbb{Z}_n$ является полем тогда и только тогда, когда n - простое число.

Доказательство. Если n составное, то $n = ml$ и тогда $ml = n = 0$, следовательно m является делителем нуля и он не обратим, что противоречит определению поля. □

Определение 23.8. Алгеброй над полем K называется множество A с операциями сложения, умножения и умножения на элементы поля K, обладающими следующими свойствами:

1. A является векторным пространством над полем K
2. A является кольцом.
3. $\forall \lambda \in K, a, b \in A : (\lambda a)b = \lambda(ab)$

Сразу вместе с алгберой определяется ее размерность, как размерность векторного пространства из 1-го пункта.

Определение 23.9. Подалгеброй называется подмножество, замкнутое относительно всех операций и являющееся алгеброй.

Сделаем кольца и алгебры топовыми:

Определение 23.10. Изоморфизмом колец и алгебр называется гомоморфизм, являющийся биекцией.

24 Идеалы колец. Главные идеалы и идеалы, порождённые подмножеством, в коммутативных кольцах.

Хотелось бы определить что-то типа факторгруппы, но на кольцах. Начнем медленно к этому двигаться:

Определение 24.1. Подмножество I кольца R называется идеалом, если оно является подгруппой по сложению и $\forall a \in I, r \in R : ra \in I, ar \in I$.

Пусть R - коммутативное кольцо. Тогда с каждым элементом $a \in R$ можно связать идеал $\{ra | r \in R\}$.

Определение 24.2. Идеал I называется главным, если существует такой элемент $a \in R$, что $I = \langle a \rangle$.

Если же у нас есть подмножество $S \subseteq R$, то с ним связан идеал:

$$(S) = \{r_1 a_1 + \ldots + r_k a_k | a_i \in S, r_i \in R, k \in \mathbb{N}\}$$

25 Факторкольца. Теорема о гомоморфизме для колец.

Теперь пусть у нас есть кольцо R и идеал I. Поскольку I является подгруппой $(R, +)$, то мы можем рассмотреть факторгруппу R/I, и даже ввести на ней умножение:

$$(a + I)(b + I) = ab + I$$

Проверим корректность умножения:

$$a' = a + x, x \in I$$
$$b' = b + y, y \in I$$
$$a'b' + I = (a + x)(b + y) + I = ab + ay + xb + x + I = ab + I$$

Определение 25.1. Кольцо R/I называется факторкольцом кольца R по идеалу I.

Теперь поймем, что теорема о гомоморфизме все еще работает на кольцах.

Лемма 25.1. Пусть $\varphi : R \to R'$ - гомоморфизм колец. Тогда $Ker(\varphi)$ является идеалом в R.

Доказательство. Нам необходимо показать, что $\forall a \in Ker(\varphi), r \in R : ar \in Ker(\varphi), ra \in Ker(\varphi)$.

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0 \Rightarrow ra \in Ker(\varphi)$$

□

Теорема 25.2. Пусть $\varphi : R \to R'$ - гомоморфизм. Тогда:

$$R/Ker(\varphi) \cong Im(\varphi)$$

Доказательство. Сделаем define $I = R/Ker(\varphi)$. Теперь заведем отображение $\psi : I \to Im(\varphi), (a + I) \to \varphi(a)$. Из доказательства теоремы о гомоморфизме эта операция валидно определена и является биекцией. Остается проверить, что ψ сохраняет операцию умножения:

$$\psi((a + I)(b + I)) = \psi(ab + I) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(a + I)\psi(b + I)$$

Что и требовалось доказать. □

26 Простое кольцо. Простота алгебры матриц.

Определение 26.1. Кольцо R называется простым, если в нем нет собственных идеалов.

Для того, чтобы лучше осознать это определение, докажем простенькую лемму

Лемма 26.1. Поле F является простым кольцом.

Доказательство. Предположим обратное. Пусть в поле есть собственный идеал I. Тогда:

$$\exists a \in I$$
$$\exists a^{-1} \in R : a^{-1}a = 1$$
$$a^{-1}a \in I \Rightarrow 1 \in I$$

Так как идеал образует группу по сложению, то в нем лежит все поле F и он является несобственным. □

Определение 26.2. Центром алгебры A над полем K называется ее подмножество:

$$Z(A) = \{a \in A | \forall b \in A : ab = ba\}$$

Докажем какую-то люто бесполезную и неприятную теорему, которую нам зачем то засунули в билет:

Теорема 26.2. Пусть K - поле, n - натуральное число и $A = Mat(n \times n, K)$ - алгебра квадратных матриц порядка n над полем K. Тогда:

1. $Z(A) = \{\lambda E | \lambda \in K\}$
2. Алгебра A является простой(если смотреть на нее, как на кольцо)

Доказательство. Обозначим за E_{ij} матрицу, в которой на клетке (i,j) стоит 1, а в остальных клетках 0. Тогда, матрицы E_{ij} образуют базис в A и любая матрица $X = \sum_{k,l=1}^{n} x_{kl}E_{kl}$.

Докажем первое утверждение теоремы. Пусть $X \in Z(A)$. Тогда:

$$X = \sum_{k,l=1}^{n} x_{kl}E_{kl}$$
$$XE_{ij} = (\sum_{k,l=1}^{n} x_{kl}E_{kl})E_{ij} = \sum_{k=1}^{n} x_{ki}E_{kj}$$
$$E_{ij}X = E_{ij}(\sum_{k,l=1}^{n} X_{kl}E_{kl}) = \sum_{l=1}^{n} x_{jl}E_{il}$$
$$XE_{ij} = E_{ij}X$$
$$\sum_{k=1}^{n} x_{ki}E_{kj} = \sum_{l=1}^{n} x_{jl}E_{il}$$

Из полученного неравенства следует, что $x_{ii} = x_{jj}$, то есть на главной диагонале она равна, и так как для каждого ij какое-то множество остальных клеток оказывается равным 0, то меняя i и j мы получим, что все, кроме главной диагонали равно 0. Значит $X = \lambda E$.

Теперь докажем второе утверждение. Пусть I - собственный идеал алгебры A и $X \in I$. Тогда рассмотрим разложение X по базису и найдем такие kl, что $x_{kl} \neq 0$. Теперь рассмотрим хитрое произведение:

$$E_{ik}XE_{lj} = E_{ik}(\sum_{p,q=1}^{n} x_{pq}E_{pq})E_{lj} = (\sum_{q=1}^{n} x_{kp}E_{iq})E_{lj} = x_{kl}E_{ij} \in I$$

Меняя i, j доказываем, что все базисные элементы лежат в идеале, а значит и вся алгебра лежит в идеале. Противоречие с тем, что оно собственное. □

27 Центр алгебры матриц.

Смотреть выше.

28 Симметрические многочлены. Степенные суммы и элементарные симметрические многочлены. Формулировка основной теоремы о симметрических многочленах. Примеры.

Определение 28.1. Многочлен $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ называется симметрическим, если $f(x_{r(1)}, \ldots, x_{r(n)}) = f(x_1, \ldots, x_n)$ для всякой перестановки $r \in S_n$.

Если вспомнить то, что любая перестановка представляется в виде композиции замены соседних элементов, то достаточно проверить, что значения многочлена не меняются при замене соседних переменных для того, чтобы сказать, что он является симметрическим.

Определение 28.2. Многочлен $s_k(x_1, \ldots, x_n) = x_1^k + \ldots + x_n^k$ называется степенной суммой.

Определение 28.3.

$$\sigma_1(x_1, \ldots, x_n) = x_1 + \ldots + x_n$$
$$\sigma_2(x_1, \ldots, x_n) = \sum_{1 \le i < j \le n} x_i x_j$$
$$\ldots$$
$$\sigma_k(x_1, \ldots, x_n) = \sum_{1 \le i_1 < \ldots < i_k \le n} x_{i_1} \ldots x_{i_k}$$
$$\ldots$$
$$\sigma_n(x_1, \ldots, x_n) = x_1 \ldots x_n$$

Называются элементарными симметрическими многочленами.

И сразу дадим великую теорему, которую мы будем доказываться следующие 2 билета:

Теорема 28.1. Для любого симметрического многочлена $f(x_1, \ldots, x_n)$ существует и единственнен такой многочлен $F(y_1, \ldots, y_n)$, что:

$$f(x_1, \ldots, x_n) = F(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n))$$

Докажем мы ее на 2 билета позже.

29 Лексикографический порядок и старший член. Лемма о старшем члене.

Представим одночлен в виде $x_1^{i_1} \ldots x_n^{i_n}$, после чего будем сравнивать лексикографически последовательность $i_1, \ldots, i_n$.

Определение 29.1. Старшим членом ненулевого многочлена $f(x_1, \ldots, x_n$ называется наибольший в лексикографическом порядке встречающийся в нем одночлен. Обозначение: $L(f)$.

Докажем очень сильную и мощную лемму(еще чуточку более мощная, и была бы теорема):

Лемма 29.1. Пусть f, g - многочлены. Тогда $L(fg) = L(f)L(g)$.

Доказательство. Пусть u - одночлен в f и v - одночлен в g. Тогда:

$$u \le L(f)$$
$$v \le L(v)$$
$$uv \le L(f)L(v)$$

Заметим, что хотя бы одно из первых двух неравенств является строгим, если $u \ne L(f)$ или $v \ne L(v)$. Тогда, очевидно, что третье неравенство будет также строгим, поэтому $L(f)L(v)$ будет больше всех остальных одночленов.

Остается лишь убедиться в том, что он не сократиться после умножения, но так как он наибольший, то это очевидно. □

Лемма 29.2. Если $ax_1^{k_1}x_2^{k_2} \ldots x_n^{k_n} = L(f)$, где f - симметрический многочлен, то $k_1 \ge k_2 \ge \ldots \ge k_n$.

Доказательство. Предположим обратное. Так как многочлен симметрический, то он равен многочлену, где мы поменяли x_i и x_j переменную местами, значит если в нем существует наш максимальный одночлен, то и существует одночлен, где мы изменили порядок k_i, k_j из чего и следует наше условие. □

Лемма 29.3. Пусть $k_1, \ldots, k_n$ - целые неотрицательные числа. Если $k_1 \geq k_2 \geq \ldots \geq k_n$, то существуют и единственны такие числа $l_1, \ldots, l_n$, что:

$$x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} = L(\sigma_1(x_1, \ldots, x_n)^{l_1} \ldots \sigma_n(x_1, \ldots, x_n)^{l_n})$$

Доказательство. По доказанной выше лемме мы получаем следующую систему уравнений:

$$\begin{cases} k_1 = l_1 + \ldots + l_n \\ k_2 = l_2 + \ldots + l_n \\ \ldots \\ k_n = l_n \end{cases}$$

А у этой системы единственное решение. □

30 Доказательство основной теоремыо симметрических многочленах.

Настало время обмазываться. Напомним нашу теорему и докажем ее(наверное)

Теорема 30.1. Для любого симметрического многочлена $f(x_1, \ldots, x_n)$ существует и единственнен такой многочлен $F(y_1, \ldots, y_n)$, что:

$$f(x_1, \ldots, x_n) = F(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n))$$

Доказательство. Сначала докажем существование искомого многочлена. Если f - нулевой многочлен, то возьмем за F нулевой многочлен. Иначе по лемме 2 найдем одночлен от элементарных симметрических, который равен $L(f)$: $\sigma_1^{l_1} \ldots \sigma_n^{l_n}$. Возьмем $f' = f - \sigma_1^{l_1} \ldots \sigma_n^{l_n}$. Если $f' = 0$, то мы нашли f. Иначе повторим описанный выше процесс.

Остается доказать, что описанный выше процесс обязательно закончится. Для начала заметим, что последовательность старших многочленов будет убывать. Это очевидно следует из того, что после того, как мы вычтем симметрический одночлен из нашего, то самый старший одночлен будет уничтожен, а появятся только меньшие его.

Ну а теперь замечаем, что с учетом второй леммы таких многочленов конечное число, значит мы остановимся. Существование доказано.

Докажем единственность. Предположим обратное. Пусть:

$$f(x_1, \ldots, x_n) = F(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)) = G(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n))$$
$$H(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)) = F - G$$

H является ненулевым многочленом, однако во всех точках принимает значение, равное нулю. А дальше я не осилил(((

□

31 Теорема Виета. Дискриминант многочлена.

Теорема 31.1. Пусть $\alpha_1, \ldots, \alpha_n$ - корни многочлена $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$. Тогда:

$$\sigma_k(\alpha_1, \ldots, \alpha_n) = (-1)^k a_{n-k}$$

Доказательство.

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = (x - \alpha_1)\ldots(x - \alpha_n)$$

Просто раскрыть скобки справа и посмотреть на соответствующие показатели степени. □

Определение 31.1. Дискриминантом многочлена $h(x) = a_nx^n + \ldots + a_1x + a_0$ с корнями $\alpha_1, \ldots, \alpha_n$ называется выражение:

$$D(h) = a_n^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

32 Примеры полей. Характеристика поля и простое подполе.

Примеры полей: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$, где p - простое. Также, можно взять поле рациональных дробей над полем K, элементами которого являются $f(x)/g(x)$, где f, g многочлены и $g \neq 0$.

Определение 32.1. Пусть K - поле. Характеристикой поля K назовем такое число p, что $\underbrace{1 + 1 + \ldots + 1}_{p} = 0$. Если такого числа нет, то скажем, что характеристика равна 0. Обозначение: $char(K)$.

Лемма 32.1. Характеристика поля K либо 0, либо простое число.

Доказательство. Пусть $p = char(K) = ml$. Тогда:

$$0 = (\underbrace{1 + \ldots + 1}_{m})(\underbrace{1 + \ldots + 1}_{l})$$
$$a = \underbrace{1 + \ldots + 1}_{m}$$
$$b = \underbrace{1 + \ldots + 1}_{l}$$
$$ab = 0$$

Противоречие, так как в поле нет делителей нуля. □

Для любого множества $S \subset K$ существует такое наименьшее по включению подполе в K, содержащее S. Мы знаем, что любое подполе содержит в себе 0. Значит, если взять в качестве $S = \{0\}$, то мы получим самое малое по включению подполе в K. Такое подполе называется простым.

33 Расширение полей. Конечное расширение и его степень. Степень композиции расширений.

Определение 33.1. Если K - подполе поля F, то говорят, что F - расширение поля K.

Определение 33.2. Степенью расширения полей $K \subseteq F$ называется размерность поля F, как векторного пространства над полем K, что обозначается, как $[F : K]$.

Определение 33.3. Пусть F - расширение поля K. Это расширение называется конечным, если $[F : K] < \infty$.

Лемма 33.1. Пусть $K \subseteq F$ и $F \subseteq L$ - конечные расширения полей. Тогда: $[L : K] = [L : F][F : K]$.

Доказательство. Пусть $e_1, \ldots, e_n$ базис F над K и $f_1, \ldots, f_m$ - базис L над F. Докажем, что следующее множество элементов является базисом:

$$\{e_i f_j | i \in [1, n], j \in [1, m]\}$$
$$a \in F : a = \alpha_1 f_1 + \alpha_2 f_2 + \ldots + \alpha_n f_n = \sum_{i,j=1}^{n} \beta_{ij} e_i f_j$$

Теперь осталось доказать, что это базис. Предположим обратное:

$$\sum_{i,j=1} \beta_{ij} e_i f_j = 0$$
$$\sum_{i=1}^{n} (\sum_{j=1}^{n} \beta_{ij} e_j) f_i) = 0$$

Так как f_i базис, то:

$$\sum_{j=1}^{n} \beta_{ij} e_j = 0$$

Так как e_j базис, то $\beta_{ij} = 0$, что и требовалось доказать. □

34 Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента и его свойства.

Определение 34.1. Элемент $a \in F$ называется алгебраическим над подполем K, если существует ненулевой многочлен $f(x) \in K[x]$, для которого $f(a) = 0$. В противном случае a называется трансцендентным элементом над K.

Определение 34.2. Минимальным многочленом алгебраического элемента $a \in F$ над подполем K называется ненулевой многочлен $h_a(x)$ наименьшей степени, для которой $h_a(a) = 0$.

Лемма 34.1. Пусть $a \in F$ - алгебраический элемент над K и $h_a(x)$ - его минимальный многочлен. Тогда:

1. $h_a(x)$ - определен однозначно с точностью до пропорциональности
2. $h_a(x)$ - является неприводимым многочленом над полем K.
3. Любой аннулирующий многочлен $f(x)$ делится на $h_a(x)$.

Доказательство. Докажем сначала (3) пункт. Предположим обратное.

$$f = qh_a + r$$
$$f(a) = r(a)$$
$$r(a) = 0$$

Противоречие с тем, что у h_a минимальная степень. Теперь из (3) очевидно следует (1). Остается доказать (2). Предположим обратное:

$$h_a = fg$$

Из чего следует, что либо $f(a) = 0$, либо $g(a) = 0$, что опять же противоречит. □

35 Минимальное подполе, порождённое алгебраическим элементом.

Пусть $a \in F$ поле, а K подполе. Обозначим за $K(a)$ минимальное подполе, которое включает в себя K и a.

Лемма 35.1. Пусть $a \in F$ - алгебраический элемент над K и n - степень его минимального многочлена над K. Тогда:

$$K(a) = \{\beta_0 + \beta_1 a + \ldots + \beta_{n-1}a^{n-1} | \beta_0, \ldots, \beta_{n-1} \in K\}$$

Кроме того: $1, a, \ldots, a^{n-1}$ линейно независимы над K и $[K(a) : K] = n$.

Доказательство. Заметим, что какое-бы поле, содержащее K и a мы не взяли, то в них всегда лежат следующие элементы:

$$\left\{ \frac{f(a)}{g(a)} \mid f \in K[x], g \in K[x], g(a) \neq 0 \right\}$$

Легко видеть, что описанная выше штука является полем и при этом она еще и является минимальным полем. Остается показать, что это поле представимо в виде, описанном выше и мы победили. Для начала заметим, что:

$$(g(x), h_a(x)) = 1$$
$$\exists v, u : v(x)g(x) + u(x)h_a(x) = 1$$
$$v(x)g(x) = 1 - u(x)h_a(x)$$

Утверждение про то, что нод равен 1 следует из того, что $h_a(x)$ является неприводимым. А теперь вжух:

$$\frac{f(a)}{g(a)} = \frac{f(a)v(a)}{1 - u(a)h_a(a)} = \frac{f(a)v(a)}{1 - u(a)0} = f(a)v(a)$$

И мы перешли из дроби к нормальному многочлену. А теперь возьмем остаток по $h_a(a)$ и:

$$f(a)v(a) = q(a)h_a(a) + r(a) = r(a)$$

И так как $r(a)$ имеет степень не большее, чем $n - 1$, то:

$$r(a) = \beta_0 + \ldots + \beta_{n-1}a^{n-1}$$

Чтд. □

36 Присоединение корня неприводимого многочлена. Поле разложения многочлена.

Теорема 36.1. Пусть K - произвольное поле, а $f(x) \in K[x]$ - многочлен. Тогда существует конечное расширение $K \subseteq F$ в котором f имеет корень.

Доказательство. Заметим, что если $f(x)$ не является неприводимым, то мы можем решить эту задачу для одного из его делителей $p(x)$. Возьмем факторкольцо $K[x]/(p(x))$, что представляет из себя все остатки от деления на $p(x)$. Докажем, что сие является полем, для чего достаточно показать, что всякий элемент обратим. Пусть $g(x) \in K[x]$ не делится на $p(x)$(то есть не является нулевым элементом), то тогда $(g(x), p(x)) = 1$, так как $p(x)$ неприводимый. Значит:

$$\exists v, u : v(x)g(x) + u(x)p(x) = 1$$
$$v(x)g(x) = 1 - u(x)p(x)$$
$$(g(x) + p(x)) \cdot (v(x) + p(x)) = (1 + p(x)) + (0 + u(x)p(x)) = (1 + p(x))$$

Что и доказывает, что наше факторкольцо является полем. Теперь покажем, что если мы возьмем $F = K[x]/(p(x))$, то расширение будет конечным. Ну это очевидно так, причем размерность будет равна степени $p(x)$. В качестве базиса тупо возьмем:

$$(1 + p(x)), (x + p(x)), \ldots, (x^{n-1} + p(x))$$

Единственное, что осталось показать - это то, что в поле F и многочлена $p(x)$ есть корень. Возьмем в качестве $x = (x + p(x))$. Важно отметить, что мы берем не сумму, а именно элемент нашего факторкольца. То есть, по факту мы просто взяли остаток от деления $p(x)$ по $p(x)$, так как мы начали рассматривать x, как своеобразный "вычет"по модулю $p(x)$. И тогда очевидно, что $p(x + p(x)) = 0$, что и требовалось доказать. □

Определение 36.1. Пусть K - поле и $f(x) \in K[x]$ - многочлен положительной степени. Полем разложения многочлена $f(x)$ называют такое расширение F поля K, что выполняются следующие свойства:

1. Многочлен $f(x)$ разлагается над F на линейные множители.
2. F является минимальным по включению полем, содержащим в себе K и удовлетворяющим первому свойству.

Если говорить проще, то это то, насколько надо дополнить поле, чтобы у многочлена n-ой степени появилось n корней.

Теорема 36.2. Поле разложения любого многочлена существует и единственно с точностью до изоморфизма, тождественного к K.

Доказательство этой теоремы не входит в курс.

37 Порядок конечного поля.

И мы на финальном рывке. Щас будет череда мощных теорем и мы победили.

Теорема 37.1. Число элементов конечно поля равна p^n, где p - простое.

Доказательство. Пусть K - конечное поле характеристики p и пусть размерность K над простым подполем $(1) \cong \mathbb{Z}^p$ равна n. Выберем в K базис $e_1, \ldots, e_n$ над $\mathbb{Z}_p$. Тогда исходя из того, что каждый элемент представляется через базис однозначно, мы получаем, что элементов p^n, что и требовалось доказать. □

38 Автоморфизм Фробениуса.

Возьмем конечное поле K характеристики p и рассмотрим отображение:

$$\varphi : K \to K, a \to a^p$$

Докажем, что φ - гомоморфизм. Он очевидно сохраняет операцию умножения, покажем, что он сохраняет сложение:

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \ldots + \binom{p}{p-1}ab^{p-1} + b^p$$

Заметим, что так как p простое, то $\binom{p}{i}$ делится на p, чисто исходя из его определения через факториалы и следовательно: $\binom{p}{i}k = \binom{p}{i}q1 = 0$, так как p - характеристика поля. Итого: $(a+b)^p = a^p + b^p$ и значит наше отображение является гомоморфизмом. Ядро гомоморфизма является идеалом, но в поле нет собственных идеалов и $\varphi(1) \neq 0$, значит $Ker(\varphi) = \{0\}$, то есть φ - инъективно. Ну а инъективное отображение из конечного множества в само себя очевидно является биекцией.

Определение 38.1. Определенная выше биекция φ называется автоморфизмом Фробениуса поля K.

39 Теорема существования и единственности для конечных полей.

Щас мы перейдем к теореме, но пока скажем про одну штуку, которая всплывет в доказательстве:

Лемма 39.1. Пусть K - произвольное поле, а $\varphi : K \to K$ - изоморфизм. Множество неподвижных точек $\{a \in K \mid \varphi(a) = a\}$ является подполем в K.

Доказательство. Ну вы проверите все аксиомы, я в вас верю. □

А теперь крайне и крайне сильная теорема. Если бы мне не нужно былоы бы вводить для этого отдельную команду в заголовке, то я бы написал «Теорема» капсом.

Теорема 39.2. Для всякого простого числа p и натурального числа n существует и единственно с точностью до изоморфизма поле из p^n элементов.

Доказательство. Пусть $q = p^n$. Докажем единственность. Пусть поле K содержит q элементов. Тогда мультипликативная группа $K^\times$ имеет порядок $q-1$. Из теоремы Лагранжа мы знаем, что $\forall a \neq 0 : a^{q-1} = 1$, а значит $a^q - a = 0$ для вообще всех a, включая 0. Тогда, все элементы нашей группы являются корнями многочлена $x^q - x \in \mathbb{Z}_p[x]$. Из этого следует, что K является полем разложения многочлена, а такое поле единственно.

Докажем существование. Возьмем за K - поле разложения многочлена $f(x) = x^q - x, f \in \mathbb{Z}_p[x]$. Тогда: $f'(x) = qx^{q-1} - 1 = -1$, так как q делится на характеристику поля. Заметим, что у f не может быть кратных корней. В самом деле, предположим обратное. Тогда:

$$f(x) = (x-\alpha)^2 g(x)$$
$$f'(x) = (x-\alpha)g(x) + (x-\alpha)^2 g'(x)$$

Из чего следует, что $f'(x)$ делится на $(x-\alpha)$, но мы показали, что $f'(x) = -1$. Противоречие.

Значит у $f(x)$ нет кратных корней. А теперь заметим, что:

$$x^{p^n} - a = 0$$
$$x^{p^n} = a$$
$$\varphi^n(x) = a$$

Где φ - автоморфизм Фробениуса, а значит все корни являются его неподвижными точками. А про них мы знаем, что множество неподвижных точек образует поле. Так как K является полем разложения, то в нем не существует собственного подполя, который содержит все корни нашего многочлена, а значит K равно множеству неподвижных точек и его размер равен q, что и требовалось доказать. □

40 Цикличность мультипликативной группы конечного поля.

Теорема 40.1. Мультипликативная группа конечного поля F_q является циклической.

Доказательство. Обозначим за $A = (F_q, \times)$ - нашу мультипликативную группу. Ее размер будет равен $q - 1$, то есть A - конечная абелева группа. Вспомним определение экспоненты, как НОК от порядков всех элементов нашей группы и обозначим это число за m. Если $m = q - 1$, то мы доказали наше утверждение. Предположим обратное, что $m < q - 1$. Из определения экспоненты следует, что $\forall a \in A : a^m = 1$, то есть если мы возьмем многочлен $x^m - 1$, то все элементы нашей группы будут являться его корнями, но их больше, чем его степень. Противоречие. □