Конспект вопросов по компьютерной алгебре. Первый семестр. 2010.

Преподаватель: Васильев Николай Николаевич

Конспект писали: Смолов Виктор, Зенцев Федор (группа 3057/2)

Содержание

1 Группа, подгруппа, гомоморфизм групп. Ядро и образ гомоморфизма.

Определение. $< G, *, e >$ - группа, $* : G \times G \to G, e \in G$

1. $\forall a, b, c \in G \ (ab)c = a(bc)$
2. $\forall g \in G \ eg = ge = g$
3. $\forall g \in G \ \exists g^{-1} \in G \ gg^{-1} = g^{-1}g = e$

Если $\forall a, b \in G \ ab = ba$ то группу называют *абелевой*

Теорема. $\exists ! e \in G \ eg = ge = g$

Определение. G - группа, тогда $H \subset G$ называют *подгруппой*, если

1. $e \in H$
2. $\forall h_1, h_2 \in H \ h_1 h_2 \in H \mid HH \subset H$
3. $\forall h \in H \ h^{-1} \in H \mid H^{-1} \subset H$

Определение. G, W - группы.
$f : G \to W$ называют *гомоморфизмом (групп)*, если $\forall g_1, g_2 \in G \ f(g_1 g_2) = f(g_1) * f(g_2)$

Теорема. *$f : G \to W$ - гомоморфизм*
$f(e_G) = e_W$

Определение. $f : G \to W$ - гомоморфизм, тогда
$ker f = \{g \in G | f(g) = e_W\}$ - называют *ядром гомоморфизма f*

Теорема. *$ker f$ - подгруппа G*

Определение. $f : G \to W$ - гомоморфизм, тогда
$Im f = \{w \in W | \exists g \in G \ f(g) = w\}$ - называют *образом гомоморфизма f*

2 Мономорфизмы, эпиморфизмы и изоморфизмы. Понятие нормального делителя (нормальной подгруппы). Факторгруппа.

Определение. Сюръективный гомоморфизм - *эпиморфизм.*
Инъективный гомоморфизм - *мономорфизм.*
Биективный гомоморфизм - *изоморфизм.*
Изоморфизм $f : G \to G$ - *автоморфизм.*

Пусть $H \subset G$. Введем отношение эквивалентности $\sim$ соответствующее подгруппе. $g_1, g_2 \in G$. $g_1 \sim g_2$, если $g_1 g_2^{-1} \in H$

Определение. $\widetilde{g} = \{k \in G | k \sim g\}$ - *класс эквивалентности элемента, левый смежный класс g*
Обозначение: Hg

Определение. G/H - *фактормножество*, множество смежных классов.
$G/H = \{\widetilde{g} \mid \widetilde{g} = Hg\}$

Заметим, что в случае некоммутативной группы можно ввести правые смежные классы gH.

Теорема. *Если $gH = Hg$, то G/H - группа и называется факторгруппой.*

Доказательство. Введем умножение: $\forall g_1H, g_2H \in G/H$ $(g_1H)(g_2H) \overset{def}{=} g_1g_2H$. Проверим корректность умножения: пусть $g_1' \sim g_1, g_2' \sim g_2$. Тогда $g_1' = g_1h_1, g_2' = g_2h_2$, а значит $g_1'g_2' = g_1h_1g_2h_2 = g_1g_2h_1h_2$. То есть $g_1'g_2' = g_1g_2H$. Теперь проверим свойства умножения:

1. $eHgH = gH$
2. $g_1Hg_2Hg_3H = g_1g_2g_3H$
3. $gHg^{-1}H = eH$

□

Определение. $H \subset G$ назовем *нормальной подгруппой*, если $\forall g \in G$ $gH = Hg$ или $gHg^{-1} = H$ или $ghg^{-1} \in H$
Обозначение: $H \triangleleft G$

Теорема. *G - абелева группа, тогда $\forall H \subset G$ - нормальная.*

Теорема. *Ядра гомоморфизмов и только они суть нормальные подгруппы.*

Доказательство. Сперва докажем, что если $f : G \to W$ - гомоморфизм, то $kerf \triangleleft G$. $g \in G, h \in kerf$, тогда $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)f(g)^{-1} = e_W$.
Теперь покажем, что $\forall H \triangleleft G$ $\exists f$ - гомоморфизм и $kerf = H$. Введем $\pi_H : G \to G/H$ - канонической гомоморфизм. Пусть $g \in G, h \in H$ тогда $\pi_H(g) = gH, \pi_H(h) = hH = H$. Следовательно $ker\pi_H = H$. □

Порой пишут: $\{e\} \subset H \triangleleft G \overset{\pi_H}{\to} G/H$

3 Характеризация мономорфизмов в терминах ядра. Основная теорема о гомоморфизме.

Теорема. ϕ - *мономорфизм* $\Leftrightarrow ker\phi = \{e\}$

Доказательство. $[\Rightarrow]$ Пусть $\exists g \neq e$ $\phi(g) = e$. Но $\phi(e) = e$. Таким образом $g \neq e, \phi(g) = \phi(e)$. Противоречие инъективности.
$[\Leftarrow]$ Пусть $\exists g_1 \neq g_2, \phi(g_1) = \phi(g_2)$. Тогда $\phi(g_1)\phi(g_2)^{-1} = e$, а это значит, что $g_1 g_2^{-1} \neq e$ и $g_1 g_2^{-1} \in kerf$. Противоречие тривиальности ядра. □

Теорема. $G/kerf \overset{\sim}{=} Imf$

Доказательство. Пусть $\phi : X \to Y$. Введем отношение эквивалентности: $x_1 \sim x_2$, если $\phi(x_1) = \phi(x_2)$. Рассмотрим $\tau : X/\sim \to Im\,\phi$, $\tau(\tilde{x}) = \phi(x)$.
τ - инъекция. Действительно, если $\overset{\sim}{x_1} \neq \overset{\sim}{x_2}$, то x_1 не эквивалентно x_2 и значит $\phi(x_1) \neq \phi(x_2)$.
τ - сюръекция. Действительно $\forall y \in Im\,\phi$ $\exists x$ $\phi(x) = y$ и $\tilde{x} : \tau(\tilde{x}) = y$. Таким образом изоморфизм установлен.
Теперь пусть $f : G \to W$ - гомоморфизм. $g_1 \sim g_2$, если $f(g_1) = f(g_2)$, или $f(g_1)f(g_2)^{-1} = e, f(g_1 g_2^{-1}) = e$ это означает, что $g_1 g_2^{-1} \in kerf$. То есть отношение $\sim$ совпадает с отношением эквивалентности порождаемым $kerf \triangleleft G$. Можно записать $G/kerf \overset{\sim}{=} Imf$. □

4 Группа подстановок (симметрическая группа). Четные и нечетные подстановки. Теорема о том, что всякая группа есть подгруппа симметричской группы (для конечных групп).

Определение. *Симметрической группой* S_X множества X называется группа автоморфизмов $X \to X$ относительно операции композиции и нейтрального элемента $id_X : \forall x \in X, id_X(x) = x$.
Если $X = \{1, 2, \cdots, n\}$, то симметричскую группу называют группой подстановок и обозначают S_n.

Группа подстановок S_n допускает следующее копредставление:

Образующие:
$\sigma_1, \sigma_2, \cdots, \sigma_{n-1}$

Соотношения:
$\sigma_i^2 = 1$
$\sigma_i \sigma_j = \sigma_j \sigma_i$, если $|i - j| > 1$
$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$

Вообще, образующие в указанном копредставлении являются *транспозициями*, то есть это такие подстановки, которые меняют два соседних элемента местами, а остальные элементы оставляют на месте.

Определение. Подстановка называется *четной*, если она представляется в виде произведения четного числа транспозиций и *нечетной* в противном случае.

Нечетные подстановки группы не образуют. Четные же образуют нормальную подгруппу группы S_n.

Теорема. *Любая группа - подгруппа симметрической группы.*

Доказательство. Необходимо сопоставить каждому элементу $g \in G$ некоторую биекцию $G \to G$, тем самым получив вложение $G \subset S_G$. Рассмотрим $i_g : G \to G, \forall s \in G \ i_G(s) = gs$. Осталось проверить свойства: $i_a \circ i_b = a(bs) = (ab)s = i_{ab}$, $i_g \circ i_{g^{-1}} = g(g^{-1}s) = es = i_e$. □

5 Левые классы смежности по подгруппе (см. вопрос 2). Индекс подгруппы. Теорема об индексе.

Определение. $H \subset G$
$[G : H] = \#(G/H)$ - *индекс* подгруппы. То есть индекс подгруппы это количество смежных классов.
$\#G$ - *порядок*, *мощность* группы.

Замечание: индекс тривиальной подгруппы - порядок группы.

Теорема (Теорема об индексе). *$K \subset H \subset G$,
тогда $[G : K] = [G : H][H : K]$*

Доказательство. $G = \bigcup\limits_{i=1}^{[G:H]} g_iH$ при этом $g_iH \neq g_jH, i \neq j$. Аналогично $H = \bigcup\limits_{j=1}^{[H:K]} h_jK$ при этом $h_iK \neq h_jK, i \neq j$. Запишем $G = \bigcup\limits_{i,j} g_ih_jK$.
Теперь достаточно проверить, что g_ih_jK представляют все различные классы смежности по K. Пусть $g_ih_jK = g_lh_mK$. Умножим на H, получим $g_ih_jKH = g_lh_mKH$, и далее $g_ih_jH = g_lh_mH \Rightarrow g_iH = g_lH \Rightarrow i = l$. Вернемся к исходному равенству $g_ih_jK = g_ih_mK \Rightarrow h_jK = h_mK \Rightarrow j = m$. То есть все классы различны.
Возьмем gK. Ясно, что $g = g_ih, h \in H$ и $h = h_mk, k \in K$. Имеем $g = g_ih_mk, g \in g_ih_mK$. Теперь понятно, что исходное представление G представляло все классы смежности по K. $\square$

Следствия:

1. Порядок подгруппы всегда делитель порядка группы.
   Пусть $K = \{e\}$, по теореме об индексе $\#G = \#(G/H)\#H$
2. $\forall G : \#G = p, p \in \mathbb{P}$ - циклическая группа порядка p
   Рассмотрим $G : \#G = p, p \in \mathbb{P}$. Рассмотрим $H \subset G$ - циклическая подгруппа, порожденная $g \neq e$. Ясно, что $\#H \geq 2$. Но $\#H$ делитель $\#G = p$, а значит $\#H = p = \#G$. Также из этого следует $\forall G : \#G = p, p \in \mathbb{P} \quad G \overset{\sim}{=} \mathbb{Z}/p\mathbb{Z}$
3. Будем называть $d_g = min\{d \mid g^d = e\}$ - *порядком* элемента g. Ясно, что порядок элемента равен порядку циклической подгруппы, порождаемой этим элементом, а по первому следствию это означает, что порядок элемента всегда делитель порядка группы и из этого следует $g^{\#G} = g^{d(\frac{\#G}{d})} = e$.

6 Действие группы на множестве. Орбиты. Разбиение множества на орбиты и формула орбит. Стабилизатор.

Определение. Под действием группы G на множестве X понимается: $s : G \times X \to X$ со свойствами:

1. $s(g_1, s(g_2, x)) = s(g_1 g_2, x)$
2. $s(e, x)) = x$

$x \mapsto s(g, x)$ обозначим как i_g. Обратное действие - $s^{-1}(g, x) = s(g^{-1}, x)$.

Обозначим $s(g, x) = g \cdot x$, т.е.:

1. $g_1(g_2 x) = (g_1 g_2)x$
2. $ex = x$

Определение. Орбитой точки $x \in X$ назовем множество $Gx = \{s(g, x) | g \in G\}$

Лемма. *Множество орбит - разбиение множества X. Орбиты либо совпадают, либо не пересекаются.*

Доказательство. Пусть $y \in Gx_1 \bigcap Gx_2$. Это значит, что $\exists g_1, g_2 : y = g_1 x_1 = g_2 x_2$. Рассмотрим элемент $\widetilde{y} = gx_1$ из орбиты Gx_1. Но $\widetilde{y} = gg_1^{-1}y = gg_1^{-1}g_2 x_2$. Значит $\widetilde{y}$ из орбиты Gx_2. Следовательно орбиты совпадают. □

Определение. Назовем стабилизатором точки $x \in X$ множество $S_x \subset G : S_x = \{g \in G | gx = x\}$.

Лемма. *Стабилизаторы различных точек сопряжены в одной. x и x_1 - точки одной орбиты, тогда $\exists g : S_x = gS_{x_1}g^{-1}$.*

Доказательство. $x_1 = gx$ - т.к. они с одной орбиты. $x = g^{-1}x_1$. Рассмотрим $w \in S_x : wx = x$.

$$wg^{-1}x_1 = g^{-1}x_1$$
$$gwg^{-1}x_1 = x_1$$
$$gwg^{-1} \in S_{x_1}$$

□

Орбиты будем обозначать $O_x = Gx$.

Теорема. $|O_x| = \#(O_x) = [G : S_x], \forall x \in X$

Доказательство. Введем эквивалентность: $g_1 \sim g_2 \overset{def}{\Leftrightarrow} g_1 x = g_2 x \Leftrightarrow g_1^{-1} g_2 x = x \Leftrightarrow g_1^{-1} g_2 \in S_x$. Таким образом, 2 элемента эквивалентны, если они переводят элемент x в один и тот же элемент орбиты. 2 элемента из разных классов эквивалентности переводят элемент x в разные элементы орбиты. Разобьем всю группу на классы эквивалентности G/S_x. Отсюда $\#(O_x) = [G : S_x]$. □

Теорема (Формула орбит)**.** $X = \bigcup\limits_{x \in Orb(X)} O_x$, *($x \in Orb(x)$ - берем по одному представителю со всех орбит)*
$|X| = \sum\limits_{x \in Orb(X)} |O_x| = \sum\limits_{x \in Orb(X)} [G : S_x]$

7 Действие группы на себе сопряжениями. Сопряженные элементы. Классы сопряженности. Формула классов.

Для всякого $x \in G$ определим отображение $\sigma_x : G \to G$ формулой $\sigma_x(y) = x^{-1}yx$. Отображение определяет действие группы на себе, называемое *сопряжением.* В действительности каждое σ_x является автоморфизмом G, т.е. для всех $y, z \in G$ имеем:

$$\sigma_x(yz) = \sigma_x(y)\sigma_x(z)$$

и σ_x обладает обратным $\sigma_{x^{-1}}$.

Орбиты данного действия суть *классы сопряженности.*

Определение. Централизатором элемента $g \in G$ называется множество $C_x = \{g_1 \in G | g_1^{-1}gg_1 = g, \text{ т.е. } gg_1 = g_1g\}$

Видим, что отображение $x \mapsto \sigma_x$ есть гомоморфизм группы G в ее группу автоморфизмов. Ядро этого гомоморфизма - нормальная подгруппа в G, состоящая из всех таких $x \in G$, что $x^{-1}yx = y$ для каждого $y \in G$, т.е. из пересечения(наверное) всех централизаторов.

Отметим, что посредством сопряжений G действует также на множестве своих подмножеств. Действительно, пусть S - множество всех подмножеств в G и пусть $A \in S$ - одно из них. Тогда $x^{-1}Ax$ тоже подмножество G, которое можно обозначить через $\sigma_x(A)$, и легко проверяется, что σ_x определяет действие группы G на S. Отметим, кроме того, что если A - подгруппа G, то $x^{-1}Ax$ тоже подгруппа, так что G действует посредством сопряжений и на множестве своих подгрупп.

Определение. Пусть A, B - два подмножеста в G. Говорим, что они *сопряжены*, если $\exists x \in G : B = x^{-1}Ax$.

Пусть x, y - элементы группы G. Они называются коммутирующими, если $xy = yx$. Множество всех элементов $x \in G$, коммутирующих со всеми элементами группы G, есть подгруппа G. Назовем её *центром* группы G. Пусть G действует на себе посредством сопряжений. Тогда элемент x лежит в центре в том и только в том случае, если орбита этого элемента совпадает с ним самим и, таким образом, состоит из одного элемента. Вообще, индекс орбиты (класса сопряженности) элемента x равен индексу его централизатора. Следовательно, если G - конечная группа, то формула орбит принимает вид:

$$[G:1] = \sum_{x \in CS(X)} [G:C_x],$$

где $CS(X)$ - множество различных представителей всех классов сопряженности

8 Свободная группа. Теорема о том, что всякая группа есть факторгруппа свободной группы.

Пусть $S = \{a, b, c \cdots\}$, $S^{-1} = \{a^{-1}, b^{-1}, c^{-1}, \cdots\}$. Будем называть $A = S \cup S^{-1}$ *алфавитом*, а A^* - множеством всевозможных слов над алфавитом A. *Пустым* словом будем называть $aa^{-1} = \emptyset$. Введем отношение эквивалентности на A^*. $w \sim v$, если w можно получить из v с помощью правил сокращения. Также введем операцию *конкатенации* на A^*.

Определение. $F_S = (A^* \cup \emptyset)/\!\sim$ - группа по конкатенации. F_S - *свободная группа*, порожденная S.

Теорема (Категорное свойство свободной группы)**.** *Существует единственный гомоморфизм, делающий диаграмму коммутативной. То есть* $\forall f : S \to G \;\; \exists! \phi_f : F_S \to G, \;\; f = \phi_f \circ i.$

$$\begin{tikzcd}
S \arrow[rr, "i"] \arrow[dr, "f"'] & & F_S \arrow[dl, "\phi_f"] \\
& G &
\end{tikzcd}$$

Доказательство. Пусть $S = \{s_1, \cdots, s_n\}$. Тогда $Imf = \{f(s_1), \cdots, f(s_n)\} = \{g_1, \cdots, g_n\}$. Теперь введем $\phi_f(s_1^{n_1} s_2^{n_2} \cdots s_i^{n_i}) = g_2^{n_1} g_2^{n_2} \cdots g_i^{n_i}$. Единственность очевидна по построению. □

Теорема. *Приведенное выше свойство может быть принято за определение свободной группы с точностью до изоморфизма.*

Доказательство. Пусть существуют две свободные группы, порожденные S : F_1 и F_2. Тогда по свойству существуют единственные гомоморфизмы $\phi_i : F_1 \to F_2$ и $\phi_j : F_2 \to F_1$. А это значит, что $F_1 \cong F_2$.

$$\begin{tikzcd}
S \arrow[rr, "i"] \arrow[dr, "j"'] & & F_1 \arrow[dl, shift left, "\phi_i"] \\
& F_2 \arrow[ur, shift left, "\phi_j"] &
\end{tikzcd}$$

□

Теорема. *Любая группа есть факторгруппа некоторой свободной группы.*

Доказательство. Пусть G - группа. Забудем о её груповых свойствах и рассмотрим как множество. Рассмотрим F_G - свободную группу, порожденную G. Теперь вспомним о том, что G - группа. Тогда $\exists \phi : F_G \to G$ - естественный эпиморфизм групп, то есть $Im\,\phi = G$. По основной теореме о гомоморфизме $F_G/ker\phi \overset{\sim}{=} Im\,\phi = G$. □

Пример:
$F_{\{a,b\}} \overset{\sim}{=} \mathbb{Z} \times \mathbb{Z}$, если введены следующие правила $aba^{-1}b^{-1} = e, ab = ba$.

9 Прямое произведение групп. Свойства прямого произведения групп.

Определение. Прямым произведением групп G_1, G_2 назовём
$G_1 \times G_2 = \{(g_1, g_2) | g_1 \in G_1, g_2 \in G_2\}$

Введем произведение на $G_1 \times G_2$:
$(g_1, g_2), (w_1, w_2) \in G_1 \times G_2; (g_1, g_2)(w_1, w_2) = (g_1 w_1, g_2 w_2)$

Теорема. $G_1 \times G_2$ *- группа.*

Естественным образом определяются проекции на сомножители
$h_1(g_1, g_2) = g_1$, $ker\, h_1 = \{(e_1, g) \mid g \in G_2\} \overset{\sim}{=} G_2$
$h_2(g_1, g_2) = g_2$, $ker\, h_2 = \{(g, e_2) \mid g \in G_1\} \overset{\sim}{=} G_1$

Из основной теоремы о гомоморфизме следует также
$(G_1 \times G_2)/G_2 = G_1, (G_1 \times G_2)/G_1 = G_2$

Теорема (Категорное свойство прямого произведения)**.** W *- некоторая группа.*
$\exists ! \phi$ *- гомоморфизм, делающий диаграмму коммутативной.*

$$\begin{tikzcd}
 & G_1 \times G_2 \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\
G_1 & & G_2 \\
 & W \arrow[ul, "f_1"] \arrow[ur, "f_2"'] \arrow[uu, "\phi"] &
\end{tikzcd}$$

Теорема. *Приведенное выше свойство может быть принято за определение прямого произведения с точностью до изоморфизма.*

10 Коммутативные кольца. Гомоморфизмы колец. Моно- и эпиморфизмы. Характеризация мономорфизмов.

Определение. Кольцом $A, +, *$ называется множество с 2-мя бин. операциям: $+ : A \times A \to A$ и $* : A \times A \to A$ и удовлетворяющее следующим условиям:

1. $\{A, +\}$ - Абелева группа.
    (a) $a + b = b + a$
    (b) $(a + b) + c = a + (b + c)$
    (c) $\exists 0 : a + 0 = a$
    (d) $\forall a \exists - a : a + (-a) = 0$
2. $(ab)c = a(bc)$
   $\exists e : ea = ae = a$
3. * $ab = ba$ (коммутативное кольцо)
4. $a(b + c) = ab + ac$

Пример: Z/nZ - коммутативное кольцо, $M_n(Z)$ - некоммутативное кольцо.

Определение. A, B - кольца.
$f : A \to B$ - гомоморфизм колец, если:

1. $f(a * b) = f(a) * f(b)$
2. $f(a + b) = f(a) + f(b)$
3. $f(0_A) = 0_B$
4. $f(1_A) = 1_B$

Инъективный гомоморфизм - мономорфизм.
Сюрьективный гомоморфизм - эпиморфизм.
Биективный гомоморфизм - изоморфизм.

Мы будем рассматривать коммутативные кольца!

Теорема. *ϕ - мономорфизм* $\Leftrightarrow ker\phi = \{0\}$

Доказательство. [$\Rightarrow$] Пусть $\exists a \neq 0 \ \phi(a) = 0$. Но $\phi(0) = 0$. Таким образом $a \neq 0, \phi(a) = \phi(0)$. Противоречие инъективности.
[$\Leftarrow$] Пусть $\exists a \neq b, \phi(a) = \phi(b)$. Тогда $\phi(a) - \phi(b) = 0$, а это значит, что $a - b \neq 0$ и $a - b \in ker\phi$. Противоречие тривиальности ядра. ☐

Определение. f - гомоморфизм колец.
$Ker(f) = \{a \in A | f(a) = 0_B\}$ - ядро гомоморфизма.

Свойства ядра:

1. $a_1, a_2 \in Ker(f) \Rightarrow a_1 + a_2 \in Ker(f)$
2. $0_A \in Ker(f)$
3. $a \in Ker(f), b \in A \Rightarrow ba \in Ker(f) \ \& \ ab \in Ker(f)$

11 Идеалы и факторкольца. Определение простого и максимального идеала.

Определение. A - кольцо; $\mathfrak{a} \subset A$
$\mathfrak{a}$ - идеал, если:

1. $\mathfrak{a}$ - абелева подгруппа
   $\mathfrak{a} + \mathfrak{a} = \mathfrak{a}, -\mathfrak{a} = \mathfrak{a}$
2. $A \cdot \mathfrak{a} \subset \mathfrak{a}; \forall c \in A, a \in \mathfrak{a} \Rightarrow ca \in \mathfrak{a}$

Ядра гомоморфизмов (см. пред. вопрос) колец - идеалы.
Введем отношение эквивалентности на A:

$$a_1 \sim a_2 \ (a_1 \equiv a_2 \mod \mathfrak{a}) \overset{def}{\Leftrightarrow} a_1 - a_2 \in \mathfrak{a}$$

Будем обозначать: $\overline{a}$ - класс эквивалентности. $\overline{a} = a + \mathfrak{a}$. $\overline{0} = \mathfrak{a}$.

Пусть $\mathfrak{a}$ - идеал в A. Построим факторкольцо $A/\mathfrak{a}$ следующим образом. Рассматривая A и $\mathfrak{a}$ как аддитивные группы, образуем факторгруппу $A/\mathfrak{a}$. Определим теперь в $A/\mathfrak{a}$ умножение: $\overline{a} \cdot \overline{b} = \overline{ab}$. Проверим, что такое умножение является правильным, т.е. $\overline{a_1} = \overline{a}$ & $\overline{b_1} = \overline{b} \Rightarrow \overline{a_1 b_1} = \overline{ab}$.

Доказательство. Нужно показать, что если $a_1 \sim a$ и $b_1 \sim b$, то $a_1 b_1 \sim ab$.

$$a_1 = a + a_2, \ a_2 \in \mathfrak{a}$$
$$b_1 = b + b_2, \ b_2 \in \mathfrak{a}$$
$$a_1 b_1 = (a + a_2)(b + b_2) = ab + a_2 b + b_2 a + a_2 b_2$$
$$a_1 b_1 - ab = a_2 b + b_2 a + a_2 b_2 \in \mathfrak{a}$$
$$a_1 b_1 \sim ab$$

□

Таким образом, имеем факторкольцо $A/\mathfrak{a}$.
Будем предполагать, что $\mathfrak{a}$ - собственный идеал, т.е. $\mathfrak{a} \neq A$.

Теорема. $\phi : A \to A/\mathfrak{a}$
$\phi(a) = \overline{a}$; $\phi(ab) = \phi(a)\phi(b)$
ϕ *- канонический гомоморфизм колец.* $Ker(\phi) = \mathfrak{a}$

Теорема. *Ядра гомоморфизмов и только они являются идеалами.*

Определение. Идеал $\mathfrak{P} \subset A$ называется простым, если: $a_1 a_2 \in \mathfrak{P} \Rightarrow (a_1 \in \mathfrak{P}) \vee (a_2 \in \mathfrak{P})$

Определение. Идеал $\mathfrak{M} \subset A$ называется максимальным, если: $\mathfrak{M} \neq A$ и если $\mathfrak{B} \supset \mathfrak{M}$ и $\mathfrak{B}$ - идеал, то $\mathfrak{B} = A$.

12 Поля и области целостности. Характеризация простого и максимального идеалов в терминах факторкольца.

Определение. Кольцо называтся областью целостности, если в нем нет делителей нуля:

$$\forall x \neq 0, y \neq 0 \Rightarrow xy \neq 0$$

Пример: Z - область целостности.

Определение. Поле - кольцо, в котором:

$$\forall x \in A, x \neq 0 \quad \exists x^{-1} : xx^{-1} = 1$$

Теорема. *Идеал $\mathfrak{P}$ прост тогда и только тогда, когда $A/\mathfrak{P}$ - область целостности*

Доказательство. $[\Rightarrow]$ $\mathfrak{P}$ прост.

$$\overline{0} \neq \overline{x} \in A/\mathfrak{P}$$

$$\overline{0} \neq \overline{y} \in A/\mathfrak{P}$$

Покажем, что $\overline{x} \cdot \overline{y} \neq \overline{0}$.

$$x \notin \mathfrak{P}, y \notin \mathfrak{P} \Rightarrow xy \notin \mathfrak{P} \Leftrightarrow \overline{xy} \neq \overline{0} \Leftrightarrow \overline{x} \cdot \overline{y} \neq \overline{0}$$

$[\Leftarrow]$ $A/\mathfrak{P}$ - область целостности. Пусть $\mathfrak{P}$ - не прост. Тогда $\exists a_1, a_2 : a_1a_2 \in \mathfrak{P}$, но $a_1 \notin \mathfrak{P}$ & $a_2 \notin \mathfrak{P}$. Рассмотрим соответствующие классы эквивалентности:

$$\overline{a_1} \neq \overline{0} \ \& \ \overline{a_2} \neq \overline{0}$$

$$\overline{a_1a_2} = \overline{a_1} \cdot \overline{a_2} = \overline{0}$$

Но $A/\mathfrak{P}$ - область целостности. Получили противоречие. ☐

ЗАМЕЧАНИЕ: $1 \in \mathfrak{B} \Leftrightarrow \mathfrak{B} = A$.

Определение. $S \subset A$, тогда (S) - идеал, порожденный множеством S, т.е. пересечение всех идеалов, содержащих S.

Теорема. $\mathfrak{M}$ *- максимальный* $\Leftrightarrow A/\mathfrak{M}$ *- поле*

Доказательство. $[\Rightarrow]$ $\mathfrak{M}$ - максимальный идеал. Покажем, что $A/\mathfrak{M}$ - поле. Возьмем ненулевой элемент и найдем обратный к нему.

$$\overline{x} \in A/\mathfrak{M}, \quad \overline{x} \neq \overline{0} \Leftrightarrow x \notin \mathfrak{M}$$

$$(\mathfrak{M}\bigcup\{x\}) = A \Rightarrow 1 \in (\mathfrak{M}\bigcup\{x\})$$

$$(\mathfrak{M}\bigcup\{x\}) = xA + \mathfrak{M}$$

$$\exists y \in A,\ m_1 \in \mathfrak{M} : 1 = xy + m_1 \Leftrightarrow \overline{1} = \overline{x} \cdot \overline{y} + \overline{0} = \overline{xy}$$

$[\Leftarrow]$ $A/\mathfrak{M}$ - поле. Пусть $\mathfrak{M}$ не максимальный. Тогда $\exists \mathfrak{M}_1 : \mathfrak{M} \subset \mathfrak{M}_1 \subset A$. Возьмем $x \in \mathfrak{M}_1 \setminus \mathfrak{M}$:

$$(\mathfrak{M}\bigcup\{x\}) \subset \mathfrak{M}_1 \Rightarrow 1 \notin (\mathfrak{M}\bigcup\{x\})$$

Рассмотрим $\overline{x} \in A/\mathfrak{M}$. Т.к. $A/\mathfrak{M}$ - поле, то $\exists \overline{y} \in A/\mathfrak{M} :\ \overline{x} \cdot \overline{y} = \overline{1}$.

$\exists m_1, m_2 \in \mathfrak{M} : (x+m_1)(y+m_2) = 1 = xy+m_1y+m_2x+m_1m_2 = 1 \Rightarrow 1 \in (\mathfrak{M}\bigcup\{x\})$

Получили противоречие. □

Теорема. *Максимальный идеал простой.*

Доказательство. Пусть $\mathfrak{M}$ - максимальный идеал, и пусть $x, y \in A$ таковы, что $xy \in \mathfrak{M}$. Предположим, что $x \notin \mathfrak{M}$. Тогда $\mathfrak{M} + Ax$ - идеал, строго содержащий $\mathfrak{M}$ и, стало быть, равный A. Следовательно, мы можем написать

$$1 = u + ax,$$

где $u \in \mathfrak{M}$ и $a \in A$. Умножая на y, получаем $y = yu + axy$, откуда $y \in \mathfrak{M}$ и $\mathfrak{M}$, таким образом, простой. □

13 Кольцо полиномов над полем. Кольца главных идеалов. Алгоритм Евклида в кольце полиномов

Теорема. $\mathbb{Z}$ *- кольцо главных идеалов.*

Доказательство. Пусть $\mathfrak{a} \subset \mathbb{Z}$ - идеал и пусть $d \in \mathfrak{a}, d > 0$
$d = min\{a \in \mathfrak{a}, a > 0\}$. Докажем, что $\mathfrak{a} = (d)$.
$[\mathfrak{a} \subset (d)]$
Возьмем $n \in \mathfrak{a}$ и разделим на d, получим
$n = kd + r,\ 0 \leq r < d - 1$.
Заметим, что $n \in \mathfrak{a}$ и $kd \in \mathfrak{a}$, а значит $(r = n - kd) \in \mathfrak{a}$, но d минимальный элемент принадлежащий идеалу. Таким образом $r = 0$ и из этого следует $n \in (d)$.
$[(d) \subset \mathfrak{a}]$
Возьмем $k \in (d)$. То есть $k = ld$. По определению идеала $k \in \mathfrak{a}$. □

На самом деле любое *евклидово* кольцо является кольцом главных идеалов. Неформально евклидово кольцо это то, в котором существует аналог алгоритма Евклида. Вообще алгоритм Евклида базируется на фундаментальном свойстве натуральных чисел: *любой отрезок натурального ряда имеет минимальный элемент.* Так вот более формально кольцо R называется евклидовым если R - область целостности и $\exists d : R \to \mathbb{N} \cup -\infty$ причем $d(a) = -\infty \Leftrightarrow a = 0$ и возможно деление с остатком, то есть $\forall a, b \neq 0 \in R$ имеется представление $a = bq + r,\ d(r) < d(b)$. В частности $K[x]$ - кольцо полиномов над полем K - является евклидовым с $d = deg(f)$ и является кольцом главных идеалов.

Определение. Пусть $\mathfrak{a} = (f_1, \cdots, f_k) \subset K[x]$ - идеал.
$(f_1, \cdots, f_k) = (g)$. Будем называть g *наибольшим общим делителем многочленов* $f_1, \cdots, f_k$ и обозначать $(f_1, \cdots, f_k)$ (не путать с идеалом).

Алгоритм Евклида позволят найти наибольший общий делитель, получить его линейное представление через образующие исходного идеала.
Вход: $f(x), g(x) \in K[x]$
Выход: $u(x), v(x) : d(x) = u(x)f(x) + v(x)g(x),\ (d) = (f, g)$

Алгоритм Евклида

```
$u_{-2} \leftarrow 1, v_{-2} \leftarrow 0$
$u_{-1} \leftarrow 0, v_{-1} \leftarrow 1$
$p_0 \leftarrow f, q_0 \leftarrow g$
$i \leftarrow 0$
while $q_i \neq 0$
    do Разделить $p_i$ на $q_i$ с остатком.
        ▷ Частное $\phi_i$. Остаток $r_i$.
        $p_{i+1} \leftarrow q_i$
        $q_{i+1} \leftarrow r_i$
        ▷ Соотношения Безу
        $u_i \leftarrow u_{i-2} - \phi_i v_{i-1}$
        $v_i \leftarrow v_{i-2} - \phi_i u_{i-1}$
        $i \leftarrow i + 1$
$d \leftarrow p_i$
$u \leftarrow u_i, v \leftarrow v_i$
```

14 Существование максимального идеала в кольце. Лемма Цорна.

Определение. Частично упорядоченное множество Y называют *цепью* или *линейно упорядоченным множеством*, если $\forall x, y \in Y$ $x \leq y$ или $y \leq y$.

Определение. Пусть Y - цепь, $A \subset Y$. Тогда $y \in Y$ называют *верхней гранью* для A, если $\forall a \in A$ $y \geq a$

Определение. Пусть Y - цепь. Тогда $m \in Y$ называют *максимальным элементом*, если $\forall y \in Y$ $m \geq y$

Лемма (Цорна)**.** *Частично упорядоченное множество, в котором любая цепь имеет верхнюю грань, содержит максимальный элемент.*

Теорема. *В любом кольце существует максимальный идеал.*
$\forall A$ - кольца. $\exists \mathfrak{m} \subset A : \mathfrak{m}$ - максимальный идеал.

Доказательство. Пусть X - упорядоченное по включению множество собственных идеалов в A и пусть $S \subset X$ - цепь идеалов в A. Тогда рассмотрим $\mathfrak{B} = \bigcup\limits_{\mathfrak{m} \subset S} \mathfrak{m}$. Покажем, что $\mathfrak{B}$ - идеал.

$$x, y \in \mathfrak{B} \Rightarrow \begin{matrix} x \in \mathfrak{a}_1 \\ y \in \mathfrak{a}_2 \end{matrix} \; \mathfrak{a}_1 \subset \mathfrak{a}_2 \Rightarrow x + y \in \mathfrak{a}_2 \subset \mathfrak{B}$$

$$x \in \mathfrak{B} \Rightarrow x \in \mathfrak{a}_1 \Rightarrow \forall c \in A \; cx \in \mathfrak{a}_1 \subset \mathfrak{B}$$

К тому же $1 \notin \forall \mathfrak{a} \in S \Rightarrow 1 \notin \mathfrak{B} \Rightarrow \mathfrak{B} \neq A$. Таким образом $\mathfrak{B}$ - верхняя грань для S. Итак для произвольной цепи нашлась верхняя грань, далее по лемме Цорна X содержит максимальный элемент, то есть в A существует максимальный идеал. □

Эквивалентные утверждения:

1. Любое множество может быть вполне упорядочено.
2. Произвольное декартово произведения семейства непустых множеств непусто.
3. *Аксиома выбора.* Для любого семейства непустых непересекающихся множеств существует множество, которое имеет только один элемент в пересечении с каждым множеством семейства
4. В каждом кольце существует максимальный идеал.
5. Лемма Цорна.

Теорема. *5 ⇒ 1*

Доказательство. Пусть X - множество. Рассмотрим $Y \subset X$ - цепь в X и будем обозначать $(Y, \leq)$. Введем отношение порядка на множестве $\{(Y_s, \leq_s)\}_s : (Y_1, \leq_1) \prec (Y_2, \leq_2)$, если $Y_1 \subset Y_2$, а $\leq_1$ индуцирован $\leq_2$. Пусть тогда S - цепь пар $(Y_s, \leq_s)$. Рассмотрим $Y = \cup Y_s$. Y - верхняя грань для S. То есть любая цепь в множестве пар имеет верхнюю грань, тогда по лемме Цорна существует максимальный элемент $(M, \leq)$. Предположим, что $M \neq X$, то есть $\exists x \notin M$. Рассмотрим $M_1 = M \cup x$, но тогда $(M, \leq) \prec (M_1, \leq_1)$, а $(M, \leq)$ - максимальный. Получили противоречие. □

Приведем еще теорему об идеалах в кольце целых чисел.

Теорема. *Пусть $p \in \mathbb{P}$. Тогда $p\mathbb{Z}$ - максимальный идеал.*

Доказательство. Пусть $(p) \subset (n)$. Тогда $\exists m \in \mathbb{Z} \ : \ p = nm$, откуда $n = 1$ или $n = p$, что и доказывает максимальность идеала, а значит и его простоту. □

15 Модули и их гомоморфизмы. Моно, эпи и изоморфизмы модулей. Примеры.

Определение. M называется модулем над кольцом A или A-модулем.

1. $\{M, 0, +\}$ - абелева группа
2. $b(am) = (ba)m,\ 0m = 0 \mid a, b \in A, m \in M$
3. $a(m_1 + m_2) = am_1 + am_2 \mid a \in A, m_1, m_2 \in M$

ЗАМЕЧАНИЕ: $+ : M \to M$, но $* : A \times M \to M$

Определение. $\phi : M_1 \to M_2;\ M_1, M_2 - A-$модули
Будем называть ϕ *гомоморфизмом модулей*, если:

1. $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$
2. $\phi(0) = 0$
3. $\phi(am) = a\phi(m), \forall a \in A, m \in M$

Определение. $\phi : M_1 \to M_2$ - гомоморфизм модулей.
$ker\,\phi = \{m \in M_1 \mid \phi(m) = 0\}$ - *ядро* гомоморфизма
$Im\,\phi = \{m \in M_2 \mid \exists m_1 \in M_1\ \phi(m_1) = m\}$ - *образ* гомоморфизма

Определение. *Подмодулем* B A-модуля M будем называть подгруппу группы M, замкнутую относительно умножения на элементы из A, т.е. такую, что

$$\forall b \in B, a \in A\ :\ ab \in B$$

Введем отношение эквивалентности, порождаемое подмодулем M_1 в модуле M_2.

$$\forall s_1, s_2 \in M_2\ s_1 \sim s_2 \Leftrightarrow s_1 - s_2 \in M_1$$

Множество классов эквивалентности по такому отношению будем обозначать M_2/M_1. А класс эквивалентности элемента $m \in M_2$ будем обозначать $\overline{m}$. Заметим, что $\overline{m} = m + M_1$.

Теорема. M_2/M_1 - *модуль.*

Доказательство. 1. Положим $\overline{m_1} + \overline{m_2} = \overline{m_1 + m_2}$, $a\overline{m} = \overline{am}$.

2. Проверим корректность введенных операций, пусть

$$m'_1 \sim m_1, m'_2 \sim m_2$$

$$m'_1 \in m_1 + M_1, m'_2 \in m_2 + M_1$$

$$m'_1 + m'_2 \in m_1 + m_2 + M_1$$

$$\overline{m'_1 + m'_2} = \overline{m_1 + m_2}$$

   Пусть теперь

$$m_1 \sim m$$

$$m_1 \in m + M_1, am_1 \in am + M_1$$

$$\overline{am_1} = \overline{am}$$

☐

Теорема. $\exists \phi : M_2 \to M_2/M_1$, $ker\,\phi = M_1$ *- естественный эпиморфизм.*

Доказательство. Пусть $\phi(m) = \overline{m}$. ϕ - эпиморфизм модулей. Пусть $m \in M_1$, тогда $\phi(m) = \overline{m} = m + M_1 = M_1$, а значит $ker\,\phi = M_1$ ☐

Теорема. $\phi : M_1 \to M_2$ *- гомоморфизм модулей. Тогда* $M_1/ker\,\phi = Im\,\phi$

Примеры:

1. Любое векторное пространство - модуль.
2. A - кольцо $\Rightarrow$ A - модуль.
3. $\mathfrak{a} \subset A$ - идеал. $\Rightarrow$ $\mathfrak{a}$ - A-модуль.
4. $A/\mathfrak{a}$ - A-модуль.
5. Любая абелева группа это $\mathbb{Z}$-модуль.
6. Кольцо многочленов над кольцом - модуль. Кольцо многочленов над полем - векторное пространство.

16 Китайская теорема об остатках. Целочисленный вариант. Использование в модулярной арифметике.

Теорема (Целочисленный вариант китайской теоремы об остатках)**.** *Пусть* $m_1, \ldots, m_k \in \mathbb{Z}$ *- попарно взаимнопростые числа. Тогда*

$$\forall x_1, \ldots, x_k, \quad 0 \leq x_i < m_i$$

$$\exists! x \in \mathbb{Z}_m : x \equiv x_i \mod m_i,\ i = \overline{1, k}.$$

Существует изоморфизм колец:

$$\phi: \quad \mathbb{Z} \Big/ (\prod_{i=1}^{k} m_i)\mathbb{Z} \to \prod_{i=1}^{k} \mathbb{Z}/m_i$$

Доказательство. $m = \prod_{i=1}^{k} m_i$
Построим ϕ - изоморфизм.

$$\phi(x) = (x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_k)$$

ϕ - инъективно. Действительно, пусть ϕ - не инъективно, тогда

$$\exists x, y \in \mathbb{Z}/m\mathbb{Z} : \ \forall i \ \ x - y \vdots m_i \overset{(m_i, m_j)=1}{\Rightarrow} x - y \vdots m$$

Но $\forall x, y \in \mathbb{Z}/m\mathbb{Z}$ $|x - y| < m$, а значит $x = y$.
ϕ - сюръективно. Действительно, заметим, что ϕ действует между равномощными множествами. И далее по принципу Дирихле: любое инъективное отображение между двумя равномощными множествами сюръективно. □

С помощью алгоритма Евклида и целочисленного варианта китайской теоремы об остатках может быть построен конструктивный алгоритм восстановления числа по его остаткам (от деления на взаимнопростые числа).
Например в алгоритме RSA вычисления ведутся по модулю $n = pq$, где p, q - большие простые числа, что делает эти вычисления в $\mathbb{Z}/n\mathbb{Z}$ достаточно долгими. Китайская теорема об остатках позволяет вести эти вычисления в $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.
Вообще *модулярной арифметикой* называют операции сложения, вычитания и умножения, основанные на идеи оперирования не непосредственном с числом, а его остатками, не содержащих общих делителей. Преимущество модулярной арифметики заключается в том, что операции

выполняются просто и быстро, а также вычисления не растут. Отрицательным моментом является невозможность сравнивать числа представленные остатками и соответственно невозможность заметить переполнение.

17 Общий вариант китайской теоремы об остатках. Применение ее к кольцу полиномов.

Определение. Идеалы $\mathfrak{a}, \mathfrak{b}$ взаимнопросты, т.е. $(\mathfrak{a}, \mathfrak{b}) = 1$, если $\mathfrak{a}+\mathfrak{b} = A$

Теорема (Китайская теорема об остатках)**.** *Пусть A - кольцо и $\mathfrak{a}_1, \dots, \mathfrak{a}_k$ - попарно взаимнопростые идеалы. Тогда*

$$\forall x_1, \dots, x_k, \quad x_i \in A$$

$$\exists x \in A : x \equiv x_i \mod \mathfrak{a}_i, \; i = \overline{1, k}.$$

Существует изоморфизм колец:

$$\phi : \quad A \Big/ \bigcap_{i=1}^{k} \mathfrak{a}_i \to \prod_{i=1}^{k} A/\mathfrak{a}_i$$

Доказательство. Доказательство по ММИ.
База: $k = 2$

$$\mathfrak{a}_1 + \mathfrak{a}_2 = A \Rightarrow \exists y_1 \in \mathfrak{a}_1, y_2 \in \mathfrak{a}_2 : \quad y_1 + y_2 = 1.$$

Надо показать, что

$$\exists x \in A : \begin{array}{ll} x & \equiv x_1 \mod \mathfrak{a}_1 \\ x & \equiv x_2 \mod \mathfrak{a}_2 \end{array}$$

Предъявим $x = x_2y_1 + x_1y_2$. Покажем, что это верно:

$$\begin{aligned} x - x_1 = x_2y_1 + x_1y_2 - x_1 = x_2y_1 + x_1(y_2 - 1) = x_2y_1 - x_1y_1 \in \mathfrak{a}_1 \\ x - x_2 = x_2y_1 + x_1y_2 - x_2 = x_1y_2 + x_2(y_1 - 1) = x_1y_2 - x_2y_2 \in \mathfrak{a}_2 \end{aligned}$$

Переход:
Покажем, что $\mathfrak{a}_1$ взаимнопрост с $\prod\limits_{i=2}^{k} \mathfrak{a}_i$. Т.к. $\mathfrak{a}_1$ взаимнопрост с $\mathfrak{a}_i, \; i = \overline{2, k}$:

$$\begin{aligned} a_1 + b_1 = 1, &\quad a_1 \in \mathfrak{a}_1, b_1 \in \mathfrak{a}_2 \\ a_2 + b_2 = 1, &\quad a_2 \in \mathfrak{a}_1, b_2 \in \mathfrak{a}_3 \\ &\dots \\ a_{k-1} + b_{k-1} = 1, &\quad a_{k-1} \in \mathfrak{a}_1, b_{k-1} \in \mathfrak{a}_k \end{aligned}$$

Рассмотрим произведение:

$$(a_1 + b_1)(a_2 + b_2) \cdots (a_{k-1} + b_{k-1}) = 1 \Leftrightarrow$$

$$(\dots)a + b_1 b_2 \cdots b_{k-1} = 1,$$

где $a \in \mathfrak{a}_1$, а $b_1 b_2 \cdots b_{k-1} \in \prod\limits_{i=2}^{k} \mathfrak{a}_i$. Аналогично получаем, что $\mathfrak{a}_l$ взаимнопрост с $\prod\limits_{i=1, i\neq l}^{k} \mathfrak{a}_i$.

Вернемся к доказательству теоремы. Пусть она верна для семейства из $k-1$ идеалов. Рассмотрим $\mathfrak{a}_1$ и $\mathfrak{b} = \prod\limits_{i=2}^{k} \mathfrak{a}_i$. По КТО:

$$\exists y_1 : \begin{array}{ll} y_1 & \equiv 1 \mod \mathfrak{a}_1 \\ y_1 & \equiv 0 \mod \mathfrak{b} \end{array}$$

Аналогичным образом найдем $y_2, y_3, \dots, y_l$. Получаем:

$$\begin{cases} y_i & \equiv 1 \mod \mathfrak{a}_i \\ y_i & \in \mathfrak{a}_j, \ i \neq j \end{cases}$$

Предъявим $x = \sum\limits_{i=1}^{k} x_i y_i$. Действительно,

$$x - x_i = \sum_{l \neq i} x_l y_l + (x_i y_i - x_i) \in \mathfrak{a}_i,$$

т.к. $\sum\limits_{l \neq i} x_l y_l \in \mathfrak{a}_\mathfrak{i}$ и $x_i(y_i - 1) \in \mathfrak{a}_i$.

Таким образом имеем сюръективное отображение $f : A \to \prod\limits_{i=1}^{k} A/\mathfrak{a}_i$.

Заметим, что ядро данного гомоморфизма есть $\bigcap\limits_{i=1}^{k} \mathfrak{a}_i$. По теореме о гомоморфизме имеем изоморфизм:

$$A \Big/ \bigcap_{i=1}^{k} \mathfrak{a}_i \cong \prod_{i=1}^{k} A/\mathfrak{a}_i$$

□

Рассмотрим применение теоремы к кольцу полиномов.

Теорема. *$K[x]$ - кольцо полиномов над полем K.*
$f_1, \dots, f_k$ - полиномы такие, что $(f_i) + (f_j) = K[x] = (1), i \neq j$. Тогда для любого набора остатков $\forall r_1, \dots, r_k, \ r_i \in K[x]$:

$$\exists f \in K[x] : \quad (f - r_i) \ \vdots \ f_i, \ i = \overline{1, k}.$$

18 Расширения полей. Конечные и алгебраические расширения. Теорема: любое конечное расширение является алгебраическим.

Пусть $\mathbb{K}, k$ - поля.

Определение. $k \subset \mathbb{K}$ - расширение полей.

K является векторным пространством над k

Определение (Степень расширения)**.** $[\mathbb{K} : k]$ - размерность $\mathbb{K}$ над k как векторное пространство.

Если $[\mathbb{K} : k] = n$, то $|\mathbb{K}| = |k|^n$, и если k - простое подполе, то $|K| = p^n = q$.
ЗАМЕЧАНИЕ: $Gal(\mathbb{K} : k)$ - группа Галуа - группа автоморфизмов $\mathbb{K}$, оставляющих k на месте.

Теорема.

$$k \subset \mathbb{K} \subset \mathbb{W}$$

Тогда $[\mathbb{W} : k] = [\mathbb{W} : \mathbb{K}] \cdot [\mathbb{K} : k]$

Доказательство. Будем обозначать: $\mathbb{W}_{\mathbb{K}}$ - про-во, соотв. вложению $\mathbb{K} \subset \mathbb{W}$. Аналагично, $\mathbb{K}_k$.
$[\mathbb{W} : \mathbb{K}] = n \Rightarrow$ есть n базисных векторов $E_1, \ldots, E_n \in \mathbb{W}_{\mathbb{K}}$.
Возьмем $w \in \mathbb{W}$: $w = \sum\limits_{i=1}^{n} \alpha_i E_i, \quad \alpha_i \in \mathbb{K}$.

$[\mathbb{K} : k] = m \Rightarrow$ есть m базисных векторов $e_1, \ldots, e_m \in \mathbb{K}_k$.
Каждый $\alpha_i = \sum\limits_{j=1}^{m} \beta_i j e_j, \quad \beta_{ij} \in k$.
Итого, $w = \sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m} \beta_{ij} e_j E_i, \quad e_j E_i \in \mathbb{W}$.

□

Определение. $k \subset \mathbb{K}$
$\alpha \in \mathbb{K}$ называется алгебраическим над k, если

$$\exists c_0, c_1, \ldots, c_n \in k : \quad \sum_{i=0}^{n} c_i \alpha^i = 0$$

Определение. Расширение $k \subset \mathbb{K}$ называется алгебраическим над k, если $\forall \alpha \in \mathbb{K}$ - алгебраическое над k.

Теорема. *Любое конечное расширение - алгебраическое.*
$[\mathbb{K} : k] < \infty \Rightarrow k \subset \mathbb{K}$ *- алгебраическое.*

Доказательство. Пусть $[\mathbb{K} : k] = n$. Возьмем $\forall \alpha \in \mathbb{K}$. Заметим, что вектора $1 = \alpha^0, \alpha^1, \ldots, \alpha^n$ линейно зависимы (их $n+1$). Значит, $\sum\limits_{i=0}^{n} c_i \alpha^i = 0$. □

19 Неприводимые полиномы над полем. Неразложимые элементы кольца. Понятие факториального кольца. Существование неприводимых полиномов над конечными полями.

Определение. Многочлен $f \in k[x]$ называется неприводимым над полем k, если он имеет положительную степень и равенство $f = gh, g \in k[x], h \in k[x]$ может выполняться только в том случае, когда либо g, либо h является постоянным многочленом.

Определение. A - кольцо.
$a \in A$ - неразложим, если $a = g_1 g_2 \Rightarrow g_1 = 1 \vee g_2 = 1$

Определение. Кольцо A называется факториальным, если для любого элемента существует разложение на неразложимые элементы, и оно единственно с точностью до порядка следования неразложимых сомножителей и единиц кольца.

Теорема. *Над конечным полем существуют неприводимые полиномы любой степени.*

Данная теорема очень важна для построения полей Галуа.

20 Характеристика поля. Простое подполе. Поля конечной характеристики. Конечные поля. Построение полей Галуа F_{p^n}.

Пусть $\mathbb{K}$ - поле. Будем полагать $\underbrace{x+x+x+\cdots+x}_{n} = nx$

Введем понятие характеристики поля:

$$char(\mathbb{K}) = p = \min_k\{k \cdot e = 0\}.$$

p либо $\in \mathbb{N}$, либо $= 0$, если такого k не существует.

Пример: $Z/pZ = F_p$ - поле, т.к. идеал pZ максимальный. Характеристика F_p равна p.

Определение. Конечное поле - поле, состоящее из конечного числа элементов.

Теорема (Свойство)**.** *Любое конечное поле имеет ненулевую характеристику.*

Теорема (Свойство)**.** *Характеристика поля - простое число.*

Доказательство. $]n = pq$
$n \cdot e = 0 \Rightarrow (p \cdot q) \cdot e = 0 \Rightarrow p(q \cdot e) = 0$
Но n - min $\Rightarrow q \cdot e \neq 0, q \cdot e = x$. Итого, $p \cdot x = 0 \Rightarrow p \cdot x \cdot x^{-1} = 0 \Rightarrow p \cdot e = 0$!!! ☐

Определение. Поле называется простым, если оно не содержит собственных подполей.

] $\mathbb{K}$ - поле, $char(\mathbb{K}) = p$, p - простое.
$\exists k \subset \mathbb{K}$ - простое подполе. k - замкнуто относительно сложения, умножение, взятия обратного.
$k \cong F_p$

$\mathbb{K}$ - конечное поле, $char(K) = p$
$\exists k \cong F_p \subset \mathbb{K}$
Пусть $[\mathbb{K} : k] = n$. Тогда $|K| = q = p^n$. Рассмотрим полином $x^q - x$. Покажем, что $x^q - x \equiv 0, \forall x \in \mathbb{K}$.

$$]x = 0 : \quad 0^q - 0 = 0$$

$$]x \neq 0 : \quad x^{q-1} - 1 \overset{?}{=} 0$$

Рассмотрим $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$. $\mathbb{K}^*$ - группа по умножению. $|\mathbb{K}^*| = q - 1$. По теореме (если $|G| = m$, то $g^m = 1$) получаем, что $x^{q-1} = 1$.
Таким образом, $\forall \alpha \in \mathbb{K}$, α - корень уравнения $x^{p^n} - x$.

$$x^{p^n} - x = \prod_{\alpha \in \mathbb{K}} (x - \alpha)$$

У многочлена p^n корней. В поле $\mathbb{K}$ p^n элементов. Можно построить поле $\mathbb{K}$, найдя все корни этого уравнения. (Важно знать, что существует алгебраическое замыкание, в котором данный многочлен имеет корни!)

Еще один способ построения конечного поля - рассмотреть фактор-колько по максимальному идеалу:
$F_p[x]/(f)$ - является конечным полем из $q = p^n,\ n = deg(f)$ элементов, если f - неприводимый полином над F_p.

21 Алгебраическое замыкание поля. Поле разложения многочлена. Существование поля разложения. Поле Галуа как поле разложения полинома $x^q - x$.

Теорема. *Пусть k - поле и f - многочлен из $k[x]$ степени $\geqslant 1$. Тогда существует расширение $k \subset \mathbb{K}$, в котором f имеет корень.*

Доказательство. Пусть $f = gf_1$, где g - неприводимый сомножитель над k. Тогда $(f) \subset (g)$ и (g) - максимальный идеал.
Рассмотрим гомоморфизмы (вложения):

$$k \to k[x] \to k[x]/(g)$$

Обозначим $\mathbb{K} = k[x]/(g) \supset k$.
Возьмем моном $x \in k[x]$ и рассмотрим элемент $\overline{x} \in K$. Покажем, что g переводит класс $\overline{x}$ в $\overline{0}$, т.е. является корнем g.

$$\overline{x} = x + \phi \cdot g, \text{ где } \ \phi \in k[x]$$

Пусть $g(x) = \sum\limits_{i=0}^{n} a_i x^i$. Тогда

$$g(\overline{x}) = \sum_{i=0}^{n} a_i(\phi g + x)^i = [\text{раскрыв скобки по биному}] = (...)g + \sum_{i=0}^{n} a_i x^i$$

Таким образом, $g(\overline{x}) \equiv 0 \mod g(x)$, т.е. $g(\overline{x}) = \overline{0}$ □

Пусть k - поле, f - многочлен из $k[x]$ степени $\geqslant 1$. Под *полем разложения* $\mathbb{K}$ многочлена f мы будем понимать расширение $k \subset \mathbb{K}$, в котором f разлагается на линейные множители, т.е.

$$f(x) = c(x - a_1)(x - a_2) \cdots (x - a_n)$$

где $a_i \in \mathbb{K}, i = \overline{1, n}$

Теорема. *k - поле. f - произвольный полином из $k[x]$. Существует $\mathbb{K}_f : \quad k \subset \mathbb{K}_f$ и $\mathbb{K}_f$ - поле разложения многочлена f.*

Доказательство. Разложим f на неприводимые сомножители над полем k:

$$f(x) = g_1(x) g_2(x) \cdots g_k(x)$$

Построим поле $\mathbb{K}_1 : \quad k \subset \mathbb{K}_1 = k[x]/(g_1)$.
В поле $\mathbb{K}_1$ $f = (x - \alpha_1) \cdot f_1$, где α_1 - корень g_1.
Аналогично строим $\mathbb{K}_2, \mathbb{K}_3, \ldots, \mathbb{K}_n$.

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \quad \text{в } \mathbb{K}_n$$

Поле, порожденное всеми корнями f: $\mathbb{K}_f = k(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \mathbb{K}_n$ □

Определение. $k \subset \mathbb{K}$ - алгебраическое расширение.
$\mathbb{K}$ - алгебраически замкнуто, если $\forall f \in K[x]$ имеет корень в $\mathbb{K}$.

Теорема. *k - поле.*
$\exists \mathbb{K} : \quad k \in \mathbb{K}$, $\mathbb{K}$ - алгебраично над k и алгебраически замкнуто.
$\mathbb{K}$ единственно с точностью до изоморфизма (без док-ва).

Доказательство. Сначала построим расширение поля k, в котором каждый многочлен степени $\geqslant 1$ имеет корень.
Будем рассматривать неприводимые многочлены f над полем k от своей собственной переменной x_f.
Введем большое кольцо многочленов от многих переменных $k[x_1, x_2, x_3, \ldots]$.
(Для удобства будем вместо x_{f_i} писать x_i)
Рассмотрим идеал $\mathfrak{a} = (f(x_f)$по всем неприводимым $f)$. Этот идеал содержится в каком-то большем идеале $\mathfrak{M} : \ \mathfrak{a} \subset \mathfrak{M}$. Покажем, что $\mathfrak{M} \neq k[x_1, x_2, x_3, \ldots]$, то есть, что $1 \notin \mathfrak{M}$.
Допустим, что $\mathfrak{M}$ содержит 1. Тогда:

$$\sum_{i=1}^{N} g_i(x_1, x_2, x_3, \ldots, x_M) \cdot f_i(x_i) = 1 \quad (*)$$

Пусть $\mathbb{F}$ - конечное расширение, в котором все f_i имеют корень:

$$\left.\begin{array}{l} f_1 \text{ имеет корень } \alpha_1 \\ f_2 \text{ имеет корень } \alpha_2 \\ \vdots \\ f_N \text{ имеет корень } \alpha_N \end{array}\right. \quad \alpha_i \in \mathbb{F}$$

Подставив α_i в ур-ние $(*)$ получаем:

$$\sum_{i=1}^{N} g_i(\ldots) \cdot f_i(\alpha_i) = 0 = 1!!!$$

Пусть $\mathfrak{M}$ оказался максимальным идеалом, содержащий идеал, порожденный всеми многочленами $f(x_f)$ в $k[x_1, x_2, x_3, \ldots]$. Тогда $k[x_1, x_2, x_3, \ldots]/\mathfrak{M}$

- поле. Обозначим его через $\mathbb{K}_1$. Имеем каноническое вложение $k \subset \mathbb{K}_1$. Все полиномы из $k[x]$ имеют корни в $\mathbb{K}_1$.
По индукции строим последовательность $k \subset \mathbb{K}_1 \subset \mathbb{K}_2 \ldots$. Пусть $\mathbb{K} = (\bigcup\limits_i \mathbb{K}_i) \bigcup k$ - объединение полей. Очевидно, $\mathbb{K}$ - поле. И если f - полином над $\mathbb{K}_n$, то его корни лежат в $\mathbb{K}_{n+1}$. $\square$

Про поле Галуа см. пред. вопрос.

22 Определение и свойства автоморфизма Фробениуса

Пусть $\mathbb{K}$ - поле, $\text{char}(\mathbb{K}) = p$, $F_p \subset \mathbb{K}$.

Определение. $\phi_p : \mathbb{K} \to \mathbb{K}$, $\phi_p(x) = x^p$ назовем *автоморфизмом Фробениуса.*

$\mathbb{K}$ - векторное пространство над F_p.

Теорема. *ϕ_p - линейный оператор в $\mathbb{K}$ над F_p.*

Доказательство.

$$\phi_p(xy) = x^p y^p = \phi_p(x)\phi_p(y)$$

$$\phi_p(x+y) = (x+y)^p = \sum_{i=0}^{p} C_p^i x^i y^{p-i}$$

$$\forall i \in [1, \dots, p-1] \;\; C_p^i \,\vdots\, p$$

$$(x+y)^p = x^p + y^p = \phi_p(x) + \phi_p(y)$$

$$\phi_p(ax+by) = a^p x^p + b^p y^p$$

$$a, b \in F_p \Rightarrow a^p = a, b^p = b$$

$$\phi_p(ax+by) = ax^p + by^p$$

□

Также можно рассматривать $\phi : \mathbb{K}[x] \to \mathbb{K}[x]$, в таком случае автоморфизм Фробениуса будет линейным оператором в $\mathbb{K}[x]/(f)$ над F_p, если f - неприводимый многочлен.

Определение. *Алгеброй* называют векторное пространство или модуль с умножением.

Пример:

1. $\mathbb{R}^3$
2. $\mathbb{R}$ - $\mathbb{Z}$-алгебра
3. A, B - кольца. $A \subset B$. B - A-алгебра

23 Факториальные кольца. Задача о разложении полиномов на множители в кольце многочленов. Приведение к случаю полинома свободного от квадратов.

Теорема (Факториальность кольца многочленов). $\forall f \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ $f = f_1 f_2 \ldots f_k$ *с точностью до констант и порядка следования сомножителей, то есть, если* $f = g_1 g_2 \ldots g_m$, *то* $k = m$ *и* $\exists \sigma \in S_k \ : \ f_i = c_i g_{\sigma(i)}$

Пусть F_q - поле. $\mathrm{char}(F_q) = p$.

Постановка задачи о разложении на множители:

Пусть $f \in F_q[x], f = \prod\limits_{i=1}^{m} f_i^{\alpha_i}, (f_i^{\alpha_i}, f_j^{\alpha_j}) = 1$. Требуется найти: m, f_i, α_i

Определение. $f \in F_q[x]$ будем называть *свободным от квадратов*, если $\forall i \ \ \alpha_i = 1$.

Определение. $D : A \to A$ будем называть *дифференциальным оператором*, если

1. $D(\alpha f + \beta g) = \alpha D f + \beta D g$
2. $D(fg) = D(f)g + D(g)f$

Рассмотрим $D : F_q[x] \to F_q[x], D(x^n) = nx^{n-1}, D(x^n x_m) = D(x^n)x^m + D(x^m)x^n$, в частности $D(x^2) = 2xD(x)$. Можно показать,что других дифференциальных операторов нет.

Далее покажем как свести задачу разложения полинома на множители к задаче разложения на множители соответствующего свободного от квадратов полинома.

Пусть

$$f(x) = \phi(x)^2 g(x)$$

тогда

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

Заметим, что $f \,\vdots\, \phi$ и $f' \,\vdots\, \phi$ и значит $(f, f') \,\vdots\, \phi$.

Лемма. $f \in \mathbb{K}[x], char(\mathbb{K}) = p, f' = 0$, *тогда* $\exists g(x) : f(x) = g(x)^p$.

Доказательство.

$$f = \sum_{i=0}^{n} c_i x^i$$

$$f' = \sum_{i=0}^{n} i c_i x^{i-1} = 0$$

Тогда $\forall i \ \ ic_i = 0, c_i \neq 0$, то есть $\forall i \ \ i \vdots p$. Перепишем f с учетом последних наблюдений.

$$\sum_{j=0}^{s} c_{pj} x^{pj}$$

Таким образом, если $f' = 0$, то x входит в f со степенями кратными p. Другими словами $f'(x) = 0 \Rightarrow f(x) = g(x^p)$. Рассмотрим $\phi_p(g(x)) = (\sum a_i x^i)^p = \sum a_i x^{ip} = g(\phi_p(x)) = g(x^p)$, так как ϕ_p - линейный оператор. □

Теперь можно сформулировать алгоритм приведения f к полиному свободному от квадратов. Предыдущая лемма позволяет считать, что $f' \neq 0$, так как если $f' = 0$, то f можно заменить на $g(x)^p$ и искать разложение $g(x)$.

Вход: $f(x) \in F_q[x]$ **Выход**: $\widetilde{f}$ - свободный от квадратов

Освобождение от квадратов

```
$S \leftarrow \emptyset$ ▷ $S$ - хранилище собственных множителей $f(x)$
while true
      do $h(x) \leftarrow (f(x), f'(x))$ ▷ алгоритм Евклида
         if $h(x) = 1$
              do return ▷ $f(x)$ - свободен от квадратов

         if $h(x) \neq 1$
         ▷ Запоминаем $h(x)$
              do $S \leftarrow h(x)$
                  $f(x) \leftarrow f(x)/h(x)$
```

Ясно, что в дальнейшем для получения разложения f на множители необходимо будет разложить на множители соответствующий ему свободный от квадратов полином, а также полиномы $h(x)$ сохраненные в S.

24 Теорема Берлекэмпа

Вообще, идея Берлекэмпа состоит в применении КТО. Если $(c_1, c_2, ..., c_m)$ является произвольным набором чисел из F_p, то из КТО вытекает, что $\exists!\ g(x) \in k[x]$ такой, что

$$\begin{aligned} &g(x) \equiv c_1 \mod f_1 \\ &g(x) \equiv c_2 \mod f_2 \\ &g(x) \equiv c_3 \mod f_3 \\ &\dots \\ &g(x) \equiv c_m \mod f_m \end{aligned}$$

Полином $g(x)$ предоставляет способ получения множителей $f(x)$, так как при $m \geqslant 2$ и $c_1 \neq c_2$ мы получим НОД$(f(x), g(x) - c_1)$, делящийся на $f_1(x)$, но не на $f_2(x)$.

Лемма. $F_p \subset k, char(k) = p$
$\forall x \in k \quad x \in F_p \Leftrightarrow x^p = x$

Доказательство. $[\Rightarrow]$ Непосредственно следует из малой теоремы Ферма.
$[\Leftarrow]$ $x^p = x$ - имеет p корней. Возьмем $\alpha_1 \in F_p$ - очевидно, корень. Так мы можем предъявить все p корней из F_p, и других быть не может. □

Теорема (Берлекэмпа)**.** *$f = f_1 \cdots f_m, f_i \in k[x], char(k) = p, k$ - конечное поле. Тогда:*

$$\begin{matrix} g^p - g \;\vdots\; f \\ (g^p \equiv g \mod f) \end{matrix} \quad \Leftrightarrow \quad \begin{matrix} \exists c_1, c_2, ..., c_m \in F_p : \\ g - c_i \;\vdots\; f_i \end{matrix}$$

Доказательство. $[\Leftarrow]$

$$\begin{aligned} &g - c_1 \vdots f_1 \Leftrightarrow g - c_1 \equiv 0 \mod f_1 \Leftrightarrow g \equiv c_1 \mod f_1 \\ &g^p \equiv c_1^p \equiv [\text{малая т. Ферма}] \equiv c_1 \equiv g \mod f_1 \end{aligned}$$

Таким образом,

$$\left.\begin{aligned} &g^p - g \;\vdots\; f_1 \\ &g^p - g \;\vdots\; f_2 \\ &g^p - g \;\vdots\; f_3 \\ &\vdots \\ &g^p - g \;\vdots\; f_m \end{aligned}\right. \Leftrightarrow g^p - g \;\vdots\; f$$

[⇒] (Альтернативное док-во от Ромы) По КТО существует изоморфизм:

$$\phi: \quad k[x]/(f) \to \prod_{i=1}^{m} k[x]/(f_i)$$

ϕ таков, что переводит g в $(r_1, r_2, \ldots, r_m)$. Итак,

$$\begin{aligned} g^p \equiv g \mod f &\Leftrightarrow g^p \equiv g \mod f_i \\ g \equiv r_i &\mod f_i \\ g^p \equiv r_i^p &\mod f_i \\ \Rightarrow r_i^p \equiv r_i &\mod f_i \overset{\text{по лемме}}{\Rightarrow} r_i \in F_p \end{aligned}$$

□

Пусть теперь мы нашли g, такой, что $g^p \equiv g \mod f$. По теореме, $\exists c \in F_p: \ g - c \,\vdots\, f_1$. Ищем

$$\begin{aligned} &\text{НОД}(g-0, f) \\ &\text{НОД}(g-1, f) \\ &\text{НОД}(g-2, f) \\ &\vdots \\ &\text{НОД}(g-(p-1), f), \end{aligned}$$

и один из делителей будет нетривиальным.

25 Алгоритм Берлекэмпа для разложения полиномов над конечным полем.

Пусть $f \in k[x], char(k) = p$ и $f = f_1 \cdot f_2 \cdot f_3 \cdots f_m$. Т.е. f свободен от квадратов.
Задача стоит в отыскании f_i по заданному f.

Первый шаг - решение уравнения $g^p \equiv g \mod f$.
Заметим, что т.к. $\phi_p(g) = g^p$ - линейный оператор, то задача сводится к нахождению матрицы оператора, а затем к нахождению собственного подпространства оператора.
Итак, для нахожденя матрицы оператора необходимо применить фробениус к базисным векторам, т.е. к мономам $1, x, x^2, \ldots, x^{n-1}$, где $n = deg(f)$.

Например, найдем матрицу фробениуса в F_5-алгебре $F_5[x]/(f = x^4 + x^3 + 2x^2 + x + 1)$. Базисные вектора - $1, x, x^2, x^3$.

$$1^5 = 1 \equiv 1 \mod f$$
$$x^5 \equiv -x^3 + x^2 + 1 \mod f$$
$$x^{10} = (x^5)^2 \equiv x^3 + x - 1 \mod f$$
$$x^{15} = x^5 \cdot x^{10} \equiv x^3 \mod f$$

Таким образом, матрица фробениуса есть:

$$F = \begin{array}{c} \begin{array}{cccc} 1 & x & x^2 & x^3 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & -1 \\ -1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Далее, находим собственное подпространство соответствующее собственному значению 1, решая систему

$$(F - E) \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_n \end{pmatrix} = 0$$

Второй шаг - отщепление множителей. Для этого возьмем вектор $(c_0, c_1, \ldots, c_n)$ из собств. подпространства, составим $g(x) = \sum_{i=0}^{n} c_i x^i$. Далее, следуя теореме Берлекэмпа будем перебирать:

$$\begin{gathered}
\text{НОД}(g-0,f)\\
\text{НОД}(g-1,f)\\
\text{НОД}(g-2,f)\\
\vdots\\
\text{НОД}(g-(p-1),f),
\end{gathered}$$

Если какой-то из делителей нетривиален, то он «отщепляется». И для него рекурсивно запускается алгоритм (очевидно, процесс заканчивается, если для какого-то множителя нельзя отщепить ни один «подмножитель», т.е. множитель неразложим).
Далее из пространства выбирается следующий вектор, линейно-независимый со всеми предыдущими, и процесс повторяется.

Таким образом мы отщепим все множители, и, в свою очередь, раздожим их на множители, тем самым разложив исходный многочлен на неразложимые множители.