Общая Алгебра
IV семестр

Адамович Ольга Маратовна

22 мая 2020 г.

Содержание

Лекция №1

1 Линейный оператор простого типа

V – линейное пространство над полем K
$A \in L(V,V)$ – линейный оператор в пространстве V

Опр. $v \in V$ называется собственным вектором A с собственным значением $\lambda \in K \Leftrightarrow$
$\begin{cases} 1)\ v \neq \overline{0} \\ 2)\ Av = \lambda v \end{cases} \Leftrightarrow \begin{cases} 1)\ v \neq 0 \\ 2)\ (A - \lambda\varepsilon)v = \overline{0} \end{cases}$

Если $dim\, V = n < \infty$,
$e =< e_1, ..., e_n >$ – базис V,
то $A \longmapsto A_e \in \mathbb{R}^{n\times n}$ матрица оператора A в базисе e
Если $f - < f_1, ..., f_n >$ – другой базис, то
$A_f = T^{-1}_{e\longmapsto f} A_e T_{e\longmapsto f}, \quad (det\ T \neq 0, T_{e\longmapsto f} -$ матрица перехода $)$
$A_f \sim A_e$

Опр. f – собственный базис оператора A - базис пр-ва V, состоящий из собственных векторов оператора A.

Опр. A - оператор простого типа, если существует собственный базис оператора A.

$$f \text{ - собственный базис} \Leftrightarrow A_f = \begin{pmatrix} \lambda_1 & ... & 0 \\ \vdots & \ddots & \vdots \\ 0 & ... & \lambda_k \end{pmatrix} = diag(\lambda_1, ..., \lambda_n)$$

λ - собственное значение - корень характеристического многочлена
$f_A(t) = det(A - t\varepsilon) = det(A_e - tE)\ \ \forall$ базиса с пр-ва V

$$v \text{ - собственный вектор с собственным значением } \lambda \ \Leftrightarrow \begin{cases} v = eX \\ x \neq 0 \\ (A_e - \lambda E)X = 0 \end{cases}$$

V_λ - собственное подпространство, отвечающее корню λ характеристиче-

ского уравнения
$V_\lambda = \{v \in V : Av = \lambda v\} = Ker(A - \lambda\varepsilon)$
$dim\, V_\lambda = dim\, Ker(A - \lambda\varepsilon) = det(A - \lambda\varepsilon) = dim\, V - rk(A - \lambda\varepsilon) =$
$= n - rk(A_e - \lambda E) = k_\lambda$ - геометрическая кратность корня λ.

A_e называется диагонализуемой, если она подобна диагональной.
A_e диагонализуема $\Leftrightarrow A -$ оператор простого типа.

Теорема 1.
Критерий того, что A$\in L(V,V)$, $dim\, V = n < \infty$ является оператором простого типа.

$$\begin{cases} 1)\ f_A(t) = det(A - \lambda\varepsilon) = (t - \lambda_1)^{S_1}(t - \lambda_2)^{S_2}...(t - \lambda_k)^{S_k} \\ \text{расскладывается над } K \text{ на линейные множители } \lambda_i \in K, \\ s_i - \text{кратность корня, } \lambda_i \quad i = \overline{1,k} \\ 2)\ dim\, Ker(A - \lambda_1\varepsilon) = s_{\lambda_i} \quad \forall i = \overline{1,k} \end{cases}$$

Если $\left.\begin{matrix} 1) \\ 2) \end{matrix}\right\}$ выполняется, то $\exists$ собственный базис $f -$ объединение базисов пространств $V_{\lambda_i} \quad i = \overline{1,k}$

$$A_f = \begin{pmatrix} \lambda_1 & ... & 0 \\ \vdots & \ddots & \vdots \\ 0 & ... & \lambda_k \end{pmatrix}$$

Note. Если не выполняется условие 1), то можно расширить поле.

Например, $\mathbb{R} \subset \mathbb{C}$

Если не выполняется 2), найти собственный базис невозможно $\Rightarrow$ невозможно диагонализовать матрицу оператора.

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & ... & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & ... & \lambda & 1 \\ 0 & ... & ... & \lambda \end{pmatrix} \in \mathbb{R}^{n\times n} \text{ - жорданова клетка}$$

$$det(J_n(\lambda) - tE) = \begin{vmatrix} \lambda - t & ... & 0 \\ \vdots & \ddots & \vdots \\ 0 & ... & \lambda - t \end{vmatrix} = (\lambda - t)^n$$

$t = \lambda, \;\; s_{t=\lambda} = n$

$$\begin{cases} X \neq 0 \\ (J_n(\lambda) - \lambda E)X = 0 \end{cases}$$

$$J_n(\lambda) - \lambda E = \begin{pmatrix} 0 & 1 & ... & 0 \\ \vdots & 0 & \ddots & \vdots \\ \vdots & \ddots & 0 & 1 \\ 0 & ... & ... & 0 \end{pmatrix} = J_n(0) \;\; rk\, J_n(0) = n - 1 \Rightarrow$$

$\Rightarrow k_{t=\lambda} = dim\, V_\lambda = 1 < s_{t=\lambda} = n$, при $n > 1$

$$\begin{cases} X_2 = 0 \\ \quad \vdots \\ X_n = 0 \end{cases}$$

$$X_{oo} = \begin{pmatrix} c \\ 0 \\ \vdots \\ 0 \end{pmatrix} = c \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \qquad \text{ФСР} =< \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} >, \; v_{t=\lambda} = c \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \; c \neq 0$$

$n > 1 \Rightarrow dim\, V_\lambda = 1 < S_\lambda = n$

$J_n(\lambda)$ диагонализовать невозможно.

Мы докажем, что в случае выполнения условия 1, матрица оператора подобна квазидиагональной матрице с клетками Жордана на диагонали.

$$A_e \sim \begin{pmatrix} J(\lambda_1) & ... & 0 \\ \vdots & \ddots & \vdots \\ 0 & ... & J(\lambda_k) \end{pmatrix}$$

2 Корневое подпространство

Опр. $v \in V$ называется корневым вектором оператора A, соответствующим $\lambda \in K$, если $\exists\, m \in \mathbb{Z}_+ = \mathbb{N} \cup \{0\} : (A - \lambda\varepsilon)^m v = 0$.
$min\,\{m \in \mathbb{Z}_+ : (A - \lambda\varepsilon)^m v = 0\}$ называется высотой вектора v и обозначается $ht_\lambda(v)$
v - собственный вектор оператора A с собственым значением $\lambda \Rightarrow$
v - корневой вектор $ht_\lambda(v) = 1$,
$\overline{0}$ - корневой вектор $ht_\lambda(0) = 0 \;\; \forall\, \lambda$

Пример.
$P_n = \{p(t) \in \mathbb{R}[t] : deg\, p(t) \leqslant n\}$
$A = \dfrac{d}{dt}, \quad \lambda = 0.$ − единственное собственное значение
$ht_0(1) = 1$
$ht_0(t) = 2$
$ht_0(t^l) = l + 1, \;\; l = \overline{0, n}$

Утв. 1. Если v − корневой вектор оператора A высоты $ht_\lambda(v) = m$, то $(A - \lambda\varepsilon)^{m-1} v$ − собственный вектор A

Доказательство:
1) $(A - \lambda\varepsilon)^{m-1} v \neq \overline{0}$
2) $(A - \lambda\varepsilon)(A - \lambda\varepsilon)^{m-1} v = (A - \lambda\varepsilon)^m v = \overline{0}$

Следствие.
λ − собственное значение вектора $(A - \lambda\varepsilon)^{m-1} v$ оператора A − корень характеристического уравнения оператора A

Утв. 2.
Пусть λ - корень характеристичекого уравнения оператора A,
$V^\lambda = \{v \in V \,:\, \exists m \in \mathbb{Z}_+ : (A - \lambda\varepsilon)^m v = \overline{0}\} \Rightarrow$
V^λ − линейное подпространство пространства V.

Док-во:
0) $V^\lambda \neq \varnothing$, так как $\overline{0} \in V^\lambda$

1) $v_1, v_2 \in V^\lambda$, то есть $\begin{cases} \exists\, m_1 \in \mathbb{Z}_+ : (A-\lambda\varepsilon)^{m_1} v_1 = \overline{0} \\ \exists\, m_2 \in \mathbb{Z}_+ : (A-\lambda\varepsilon)^{m_2} v_2 = 0 \end{cases} \Rightarrow$

для $\Rightarrow m = max\{m_1, m_2\}$

$(A-\lambda\varepsilon)^m(v_1+v_2) = (A-\lambda\varepsilon)^m v_1 + (A-\lambda\varepsilon)^m v_2 = \overline{0}+\overline{0} = \overline{0} \Rightarrow v_1+v_2 \in V^\lambda$

2) $v \in V^\lambda$, то есть $\exists\, m \in \mathbb{Z}_+ : (A-\lambda\varepsilon)^m v = 0 \Rightarrow$

$\forall\, \alpha \in k : (A-\lambda\varepsilon)^m(\alpha v) = \alpha(A-\lambda\varepsilon)^m v = \alpha \cdot \overline{0} = \overline{0} \Rightarrow \alpha v \in V^\lambda$

0)
1)
2)
$\Rightarrow V^\lambda$ - линейное подпространство V

Опр. V^λ называется корневым подпространством пространства V, отвечающим собственному значению λ.

Note: 1) $V_\lambda \subset V^\lambda$

2) $V_\lambda = Ker(A-\lambda\varepsilon) \subset Ker(A-\lambda\varepsilon)^2 \subset ... \subset Ker(A-\lambda\varepsilon)^l \subset ...$

$Ker(A-\lambda\varepsilon)^l = \{v \in V^\lambda : ht_\lambda(v) \leqslant l\}$

3) $V^\lambda = \bigcup\limits_{l=1}^{\infty} Ker(A-\lambda\varepsilon)^l$

Утв. 3. Если $dim\, V = n < \infty$, то $\exists q \in \mathbb{Z}_+ \ : \ V^\lambda = Ker(A-\lambda\varepsilon)^q$

Опр. $A \in L(V,V)$,

U – линейное подпространство пространства V

U – называется инвариантным подпространством относительно действия оператора A, если $\forall v \in U \quad Av \in U$.

Утв. 4. Пусть $A \in L(V,V),\ \alpha \in K$, тогда

U – инвариантное относительно A подпространство. $\Leftrightarrow$

U – инвариантное относительно $A - \alpha\varepsilon$ подпространство

Док-во:

$\Downarrow v \in U, Av \in U$

$(A-\alpha\varepsilon)v = Av - \alpha v \in U \Rightarrow U$ – инвариантное относительно $A - \alpha\varepsilon$

$\Uparrow v \in U \quad (A-\alpha\varepsilon)v = Av - \alpha\varepsilon \in U \Rightarrow Av \in U$

Утв. 5. $v \in V^\lambda \ : \ ht_\lambda(v) = m \Rightarrow$
$w = (A - \lambda\varepsilon)v \in V^\lambda, ht_\lambda(w) = m - 1$
Док-во очевидно.

Следствие. V^λ - инвариантное относительно A подпространство V

Док-во: V^λ инвариантно относительно $A - \lambda\varepsilon \Rightarrow V^\lambda$ инвариантно относительно A

3 Прямая сумма линейных подпространств

Опр. (Внутр.) прямой суммы линейных пространств
V - линейное пространство
$V_1, V_2, ..., V_k$ - его линейные подпространства
$V = V_1 \oplus V_2 \oplus ... \oplus V_k$, если любой элемент $v \in V$ единственным образом представляется в виде суммы элементов $V_i, \ i = \overline{1,k}$, т.е.
$\begin{cases} 1) \ \forall\, v \in V \ \exists\, v_i \in V_i \ \ i = \overline{1,k} : v = v_1 + ... + v_k \\ 2) \ v = v_1 + ... + v_k = v_1' + ... + v_k', \ v_i, v_i' \in V_i \ \ i = \overline{1,k} \Rightarrow v_i = v_i' \ \forall\, i = \overline{1,k} \end{cases}$

Утв. 6. $V -$ линейное пространство,
$V_1, V_2 -$ его подпространства
$V = V_1 \oplus V_2 \Leftrightarrow$
$\begin{cases} 1) \ V = V_1 + V_2 \ (\forall v \ \exists v_1 \in V_1, v_2 \in V_2 : v = v_1 + v_2) \\ 2) \ V_1 \bigcap V_2 = \{0\} \end{cases}$

Док-во:
$\Downarrow 1) = 1)$
$V = V_1 + V_2$ единственным образом $\Rightarrow V_1 \bigcap V_2 = \{0\}$
Пусть $v \in V_1 \bigcap V_2 \qquad v = v \in V_1 + 0 \in V_2 = 0 \in V_1 + v \in V_2$ одно пр.
$\Leftrightarrow v = 0 \Rightarrow V_1 \bigcap V_2 = \{0\}$
$\Uparrow 1) = 1)$
Пусть $v = v_1 + v_2 = v_1' + v_2'$
Пусть $V_1 \bigcap V_2 = \{0\}$
$V_1 \ni v_1 - v_1' = v_2' - v_2 \in V_2$
$v_1 - v_1' = v_2' - v_2 \in V_1 \bigcap V_2 = \{0\}$

$$\begin{cases} v_1 - v_1' = 0 \\ v_2' - v_2 = 0 \end{cases} \Rightarrow \begin{cases} v_1 = v_1' \\ v_2' = v_2 \end{cases}$$

Утв. 7.

V - линейное пространство.

$V_1, ..., V_k$ - его подпространства

$V = V_1 \oplus ... \oplus V_k$

$$\Updownarrow$$

$$\begin{cases} 1) \forall\, v \in V \;\; \exists\, v_i \in V_i, \;\; i = \overline{1,k} : v = v_1 + ... + v_k \\ 2') v_1 + ... + v_k = \overline{0}, \;\; v_i \in V_i \;\; i = \overline{1,k} \Rightarrow v_i = \overline{0} \end{cases}$$

Док-во:

$1) = 1)$

$2) \Rightarrow 2')$

$\overline{0}$ представляется единственным образом $\Rightarrow v_i = \overline{0} \quad \forall i = \overline{1,k}$

$2') \Rightarrow 2)$

Пусть $v = v_1 + ... + v_k = v_1' + ... + v_k' \Rightarrow$

$\Rightarrow (v_1 - v_1') + (v_2 - v_2') + ... + (v_k - v_k') = \overline{0}$

$v_i - v_i' \in V_i \;\; \forall\, i = \overline{1,k}$

$\Rightarrow v_i - v_i' = \overline{0} \Rightarrow v_i = v_i'$

Лекция №2

Утв. 1. V - линейное пространство, $dim\, V = n < \infty$
V_i - его подпространства, $i = \overline{1,k}$
e_i - базис V_i, $e_i =< e_{i1}, ..., e_{im} >$, $dim\, V_i = n_i$,
$e = e_1 \cup e_2 \cup ... \cup e_k$,
$e =< e_{11}, ..., e_{1n_1}, e_{21}, ..., e_{2n_2}, ..., e_{k1}, ..., e_{kn_k} >$,
тогда $V = V_1 \oplus V_2 \oplus ... \oplus V_k$
$\Updownarrow$
e - базис пространства V

Док-во:

$$V = V_1 \oplus V_2 \oplus ... \oplus V_k \Leftrightarrow \left\{ \begin{array}{l} 1)\ \forall\, v \in V\ \exists\, v_i \in V_i, i = \overline{1,k}\ :\ v = v_1 + ... + v_k \\ 2')\ v_1 + ... + v_k = \overline{0},\ v_i \in V_i, \quad i = \overline{1,k} \Rightarrow v_i = 0 \end{array} \right.$$

$$\left\{ \begin{array}{l} 1) \Leftrightarrow \text{полнота системы } e \\ 2') \Leftrightarrow \text{линейная независимость системы } e \end{array} \right\} \text{доказать самим.}$$

Утв. 2. $V -$ линейное пространство, $dim\, V = n < \infty$,
$V_i -$ его подпространства, $i = \overline{1,k}$

$$\text{тогда } V = V_1 \oplus ... \oplus V_k \Leftrightarrow \left\{ \begin{array}{l} 1')\ dim\, V = \sum\limits_{i=1}^{k} dim\, V_i \\ 2')\ v_1 + ...v_k = 0 \Rightarrow v_i = 0\ \forall i = \overline{1,k} \end{array} \right.$$

Док-во:

Рассмотрим $e_i -$ базис V_i, $dim\, V_i = n_i$, $e_i =< e_{i\,1}, ..., e_{i\,ni} >$
$e = e_1 \cup ... \cup e_k$, количество векторов в e - $\sum\limits_{i=1}^{n} dim V_i$,
$V = V_1 \oplus ... \oplus V_k \Leftrightarrow e -$ базис $V \Leftrightarrow e$ - максимальная линейно независимая

$$\text{система векторов} \Leftrightarrow \left\{ \begin{array}{l} 1')\ dim\, V = \sum\limits_{i=1}^{n} dim V_i \\ 2')\ v_1 + ...v_k = 0 \Rightarrow v_i = 0\ \forall i = \overline{1,k} \end{array} \right.$$

Утв. 3. Пусть $V -$ линейное пространство, $dim\, V = n < \infty$,
$A \in L(V, V)$
$V_i -$ его инвариантные относительно A подпространства, $i = \overline{1,k}$
$V = V_1 \oplus ... \oplus V_k$
$e_i -$ базис V_i

$e = e_1 \cup ... \cup e_k$ – базис V
тогда A_e – блочно-диагональная (квазидиагональная матрица)

Док-во:

Т.к. $e =< e_{i1}, ..., e_{in_i} >$ - базис инвариантного пространства V_i,
$Ae_{ij} \in L[e_{i1}, ..., e_{in_i}]$

$$A_e = \begin{array}{c} \begin{array}{cccc} e_1 & e_2 & & e_k \end{array} \\ \left(\begin{array}{cccc} n_1 \times n_1 & 0 & \cdot & 0 \\ 0 & n_2 \times n_2 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & n_k \times n_k \end{array} \right) \end{array}$$

Вдоль диагонали стоят матрицы $A|_{V_i e_i} \in K^{n_j \times n_i}$, $i = \overline{1,k}$.

1 Характерестический многочлен оператора A, ограниченного на корневом подпространстве

Утв. 4.

Пусть V - линейное пространство, $dim\, V = n < \infty$, $A \in L(V, V)$,
λ - корень характеристического многочлена $f_A(t) = det\,(A - t\varepsilon)$
V^λ - корневое подпространство, соответсвтвующее λ,
$dim\, V^\lambda = p$,
тогда $f_{A|_{V^\lambda}}(t) = det(A|_{V^\lambda} - \lambda\varepsilon) = (\lambda - t)^p$

Док-во:

$V^\lambda = \bigcup\limits_{i=1}^{\infty} Ker(A - \lambda\varepsilon)$
$dim\, V = n < \infty \Rightarrow$
$V_\lambda = Ker(A - \lambda\varepsilon) \subset Ker(A - \lambda\varepsilon)^2 \subset ... \subset Ker(A - \lambda\varepsilon)^q = V^\lambda$,
q – минимальная такая степень m, что $Ker(A - \lambda\varepsilon)^m = V^\lambda$
$dim\, V^\lambda = p = dim\, Ker(A - \lambda\varepsilon)^q$
Пусть f_1 – базис $Ker(A - \lambda\varepsilon) = V_\lambda$
$\exists f_2$ – дополняет f_1 до базиса $Ker(A - \lambda\varepsilon)^2 \Rightarrow f_1 \cup f_2$ – базис $Ker(A - \lambda\varepsilon)^2$

$f = f_1 \cup f_2 \cup ... \cup f_q -$ базис $Ker(A - \lambda\varepsilon)^q = V^\lambda$
$V^\lambda -$ инвариантное относительно $A -$ подпространство$\Rightarrow$ инвариантное относительно $A - \lambda\varepsilon$ подпространство
$(A - \lambda\varepsilon)|_{V_f^\lambda}$
$v -$ собственный вектор
$(A - \lambda\varepsilon)v = 0$
$(A - \lambda\varepsilon)f_1 \subset \{0\}$
$(A - \lambda\varepsilon)f_i \subset L[f_1 \cup ... \cup f_{i-1}]$

$$(A-\lambda\varepsilon)|_{V_f^\lambda} = \begin{array}{c} \begin{matrix} f_1 & f_2 & f_3 & & f_i \end{matrix} \\ \begin{pmatrix} 0_1 & & & \cdot & \\ \cdot & 0_2 & & \cdot & \\ \cdot & \cdot & 0_3 & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \\ 0 & \cdot & \cdot & \cdot & 0_p \end{pmatrix} \end{array}$$

- верхняя треугольная матрица с нулями на диагонали
(на диагонали стоят нулевые матрицы $o_i \in K^{r_i \times r_i}$,
где $r_i = rk\, f_i = dim\, L[f_i],\ i = \overline{1,p}$).

$$A|_{V_f^\lambda} = \begin{array}{c} \begin{matrix} f_1 & f_2 & f_3 & & f_p \end{matrix} \\ \begin{pmatrix} \lambda E_1 & & & \cdot & \\ \cdot & \lambda E_2 & & \cdot & \\ \cdot & \cdot & \lambda E_3 & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \\ 0 & \cdot & \cdot & \cdot & \lambda E_p \end{pmatrix} \end{array} \in K^{p\times p},\ \ \lambda E^i \in K^{r_i \times r_i}$$

- верхняя треугольная матрица с λ на диагонали
$f_{A|_{V^\lambda}}(t) = det(A|_{V^\lambda} - t\mathcal{E}) = det(A|_{V_f^\lambda} - tE) = (\lambda - t)^p$

Следствие:
$\mu \in K$
$(A-\mu\mathcal{E})|_{V^\lambda}$ невырожденный оператор $\Leftrightarrow \mu \neq \lambda$

Док-во:
V^λ - инвариантное подпространство относительно $A - \mu\mathcal{E}$
$det(A-\mu\mathcal{E})|_{V^\lambda} = det(A|_{V^\lambda} - \mu\mathcal{E}) = f_{A|_{V^\lambda}}(\mu) = (\lambda-\mu)^p \neq 0 \quad \Leftrightarrow \quad \lambda \neq \mu.$

2 Размерность корневого подпространства

Теорема 1. Если V – линейное пространство, $dim\, V = n < \infty$,
$A \in L(V,V),\ \ \lambda -$ корень $f_A(t)$ кратности s,

то $dim\ V^\lambda = s$

Док-во:

V^λ – инвариантное относительно A подпространство, $dim\ V^\lambda = p$

Пусть e_1 – его базис, $rk\, e_1 = p$

Базис e_1 можно дополнить до базиса всего пространства V системой e_2

$rk\, e_2 = n - p$

$e = e_1 \cup e_2$ – базис V

Если $W = L[e_2] = L[e_{p+1}, ..., e_n]$

$V' = V^\lambda \oplus W \Rightarrow V^\lambda \cap W = \{\overline{0}\}$

$$A_e = \left(\begin{array}{c|c} A_{V^\lambda e_1} & D \\ \hline 0 & C \end{array}\right)$$

$f_A(t) = det(A_e - tE) = det(A|_{V^\lambda} - tE)det(C - tE) = (\lambda - t)^p det(C - tE) \Rightarrow$

$\Rightarrow p \leqslant s$

Пусть $p \leqslant s$, то есть λ является корнем $det(C - \lambda E)$

Рассмотрим линейный оператор $C \in L(W, W)$,

матрица которого в базисе e_2 C

$$\exists\, w \in W : \begin{cases} w \neq \overline{0} \\ Cw = \lambda w \end{cases}$$

$Aw = u + \lambda w$, где $u \in V^\lambda$

$u = Aw - \lambda w = (A - \lambda\mathcal{E})w \in V^\lambda \ \Rightarrow\ w \in V^\lambda \Rightarrow$

$\Rightarrow \overline{0} \neq w \in V^\lambda \cap W$ ↯ $\Rightarrow\ p = s$

3 Сумма корневых подпространств

Теорема 2. Пусть V – линейное пространство, $dim\ V = n < \infty$,

$A \in L(V, V)$,

V_i – корневое подпространство, соответсвующее корню λ_i характеристичего многочлена $f_A(t)$,

$\lambda_i \neq \lambda_j,\ i \neq j,\ i, j = \overline{1, k}$.

Тогда $v_1 + ... + v_k = \overline{0},\ \ v_i \in V_i \Rightarrow v_i = \overline{0}, \quad i = \overline{1, k}$,

(т.е. $V_1 + ... + V_k = V_1 \oplus ... \oplus V_k$).

Док-во:

Индукция по k.

Для $k = 1$, очевидно,

$v_1 = \overline{0} \Rightarrow v_1 = \overline{0}$

Пусть утверждение теоремы верно для $k-1$ пространства, т.е.

$v_1 + ... + v_{k-1} = \overline{0} \Rightarrow v_i = \overline{0} \;\; i = \overline{1, k-1}$

Докажем, что утверждение верно для k пространств.

Рассмотрим

$v_1 + v_2 + ... + v_k = \overline{0} \;\; (*)$,

$v_k \in V^{\lambda_k}, \;\; ht_{\lambda_k}(v_k) = m$

Применим к $(*)$ $(A - \lambda_k \mathcal{E})^m$

$(A - \lambda_k \mathcal{E})^m v_1 + (A - \lambda_k \mathcal{E})^m v_2 + ... + (A - \lambda_k \mathcal{E})^m v_{k-1} + (A - \lambda_k \mathcal{E})^m v_k = \overline{0}$

$(A - \lambda_k \mathcal{E})^m v_k = \overline{0} \Rightarrow$

$\Rightarrow \sum\limits_{i=1}^{k-1} (A - \lambda_k \varepsilon)^m v_i = 0, \;\; (A - \lambda_k \varepsilon)^m v_i \in V \Rightarrow$

$\Rightarrow$ по предположению индукции

$(A - \lambda_k \varepsilon)^m v_i = \overline{0} \quad \forall i = \overline{1, k-1}$

$A - \lambda_k \varepsilon$ невырожденный оператор на $V_i = V^{\lambda_i} \;\; i = \overline{1, k-1} \Rightarrow$

$\Rightarrow v_i = 0 \quad \forall i = \overline{1, k-1}$

$$\left.\begin{array}{l} v_i = \overline{0} \quad i = \overline{1, k-1} \\ v_1 + ... + v_k = \overline{0} \end{array}\right\} \Rightarrow v_k = \overline{0} \Rightarrow v_i = \overline{0} \;\; \forall i = \overline{1, k}$$

Теорема 3.

Пусть V – линейное пространство, $dim\, V = n < \infty, \;\; A \in L(V, V)$

$f_A(t) = (t - \lambda_1)^{s_1} ... (t - \lambda_k)^{s_k}$,

$\lambda_i \in K, \;\; \lambda_i \neq \lambda_j, \; i \neq j, \; i, j = \overline{1, k}.$

Тогда $V = V^{\lambda_1} \oplus V^{\lambda_2} \oplus ... \oplus V^{\lambda_k}$

Док-во:

$1') \;\; dim\, V = n = \sum\limits_{i=1}^{k} s_i = \sum\limits_{i=1}^{k} dim\, V^{\lambda_i}$

$2') \;\; v_1 + v_2 + ... + v_k = \overline{0}, \; v_i \in V^{\lambda_i} \;\Rightarrow\; v_i = \overline{0} \; \forall \, i = \overline{1, k}$

$$\begin{cases} 1') \\ 2') \end{cases} \Leftrightarrow V = V^{\lambda_1} \oplus ... \oplus V^{\lambda_k}$$

Следствие: Если V - линейное пространтсво, $dim\, V = n < \infty$,
$A \in L(V, V)$,
$f_A(t) = \prod_{i=1}^{k}(t - \lambda_i)^{s_i}$, $\lambda_i \in k$, $\lambda_i \neq \lambda_j$, $i \neq j$, $i, j = \overline{1, k}$,
e_i - базис V^{λ_i},
$e = e_1 \cup ... \cup e_k$,
тогда e - базис V и матрица A_e - квазидиагональная (блочно диагональная).

Док-во:
$V = V^{\lambda_1} \oplus ... \oplus V^{\lambda_k} \Rightarrow$ e - базис V
V^{λ_i} - инвариантные пространства $i = \overline{1, k}$

$A_e = \begin{pmatrix} \square & \cdot & \cdot & 0 \\ \cdot & \square & \cdot & \cdot \\ \cdot & \cdot & \square & \cdot \\ 0 & \cdot & \cdot & \square \end{pmatrix}$ - квазидиагональная.

На диагонали стоят матрицы $A|_{V^{\lambda_i}_{e_i}}$

4 Циклическое пространство, порождаемое корневым вектором

Опр. $v \in V^{\lambda}$ $-$ корневой вектор оператора A, отвечающий $\lambda \in K$, $ht_{\lambda}(t) = m$
Рассмотрим оператор $(A - \lambda\mathcal{E}) = B$
$< v, Bv, B^2v, ..., B^{m-1}v >$
$L[v, Bv, ..., B^{m-1}v]$ $-$ циклическое подпространство корневого вектора v высоты m.

Утв. 5. $L[v, Bv, ..., B^{m-1}v]$ $-$ инвариантное относительно A линейное подпростарнство V.

Док-во: очевидно $L[v, Bv, ..., B^{m-1}v]$ инвариантное подпространство относительно $B \Rightarrow$ и относительно A.
$w = \alpha_0 v + \alpha_1 Bv + ... + \alpha_{m-1}B^{m-1}v$

$Bw = \alpha_0 Bw + \alpha_1 B^2 v + ... + \alpha_{m-1}\overline{0} \in L[v, Bv, ..., B^{m-1}v]$

Лекция №3

1 Канонический базис циклического пространства

Утв. 1. Пусть V – линейное пространство, $A \in L(V,V)$,
λ – собственное значение A, $v \in V^{\lambda}$, $ht_{\lambda}(v) = m$
$B = A - \lambda\varepsilon$
Тогда $v, Bv, B^2v, ..., B^{m-1}v$ – линейно независимы.

Док-во:
Пусть $\alpha_1 v + \alpha_2 Bv + ... + \alpha_m B^{m-1}v = \overline{0}$ $(*)$
$ht_{\lambda}(t) = m \Rightarrow B^m v = \overline{0}$, а $B^{m-1}v \neq \overline{0}$
Подействуем на $(*)$ B^{m-1}
$(*) \Rightarrow \alpha_1 B^{m-1}v = \overline{0} \Rightarrow \alpha_1 = 0$
Действуем на $(*)$ B^{m-k}, $k = \overline{2, m-1} \Rightarrow \alpha_2 = \alpha_3 = ... = \alpha_{m-1} = 0$
$\alpha_m B^{m-1}v = \overline{0} \Rightarrow \alpha_m = 0 \Rightarrow \alpha_i = 0 \quad i = \overline{1, m}$

Следствие. $< B^{m-1}v, ..., Bv, v > = e$ - канонический базис циклического пространства, порождённого вектором v,
$L_v = L[v, Bv, ..., B^{m-1}v]$

Утв. 2. Пусть V - линейное пространство,
$A \in L(V,V)$,
λ - собственное значение A,
$v \in V^{\lambda}$, $ht_{\lambda}(v) = m$.

Тогда $A|_{L_{v_e}} = J_m(\lambda) = \begin{pmatrix} \lambda & 1 & ... & 0 \\ \vdots & \lambda & \ddots & \vdots \\ \vdots & \ddots & \lambda & 1 \\ 0 & ... & ... & \lambda \end{pmatrix}$

Док-во:
Рассмотрим $B|_{L_v} = (A - \lambda\varepsilon)|_{L_v}$.
Далее ограничение $B|_{L_v}$ обозначается B.

$$B(B^{m-1}v) = B^m v = \overline{0} = e \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

. . . . . .

$$B(B^{m-k}v) = B^{m-(k-1)}v = e \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}^{k-1}, \quad k = \overline{2, m}$$

. . . . . .

$$Bv = Bv = e \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}^{m-1}$$

$$B|_{L_{v_e}} = \begin{pmatrix} 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 1 & ... & 0 \\ ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & 1 \\ 0 & 0 & 0 & ... & 0 \end{pmatrix} = J_m(0)$$

$A|_{L_{v_e}} = B|_{L_{v_e}} + \lambda E = J_m(\lambda).$

2 Жорданов базис

Опр. Базис конечномерного линейного пространства V называется жордановым базисом линейного оператора, действующего в этом пространстве, если матрица оператора в этом базисе квазидиагональна (блочно-диагональная), на диагонали стоят клетки Жордана $J_l(\lambda_k)$, где λ_k – собственное значение оператора.

Такая матрица называется жордановой(нормальной) формой (матрицы) оператора.

"Привести матрицу оператора к жорданорвой форме" означает найти

жорданов базис и матрицу оператора в этом базисе.

3 Построение жорданова базиса в корневом пространстве

Теорема 1.

Пусть V - линейное пространство, $dim\, V = n < \infty$,
$A \in L(V, V)$,
λ - собственное значение A,
V^λ - корневое подпространство, соответствующее λ.
Тогда $\exists$ жорданов базис в V^λ для оператора $A|_{V^\lambda}$.

Док-во:

Рассмотрим $B = A - \lambda\varepsilon$ и $Ker\, B^k \;\; k = 1, ...$
Пусть $dim\, Ker\, B^k = n_k = n - rk\, B^k = n - r_k, \;\; r_k = rk\, B^k$
$V_\lambda = Ker\, B \subset Ker\, B^2 \subset ... \subset Ker\, B^q = V^\lambda$
$dim\, V^\lambda = s_\lambda$
$q = min\{k \in \mathbb{N} : dim\, Ker\, B^k = s_\lambda$, т.е. $r_k = n - s_\lambda\}$.
Пусть e_k - базис пространства $Ker\, B^k$
Построим жорданов базис оператора $A|_{V^\lambda}$ в пространстве V^λ с помощью "жордановой лестницы".
На k-ом этапе этой лестницы будем располагать векторы $v : ht_\lambda(v) = k$

$ht_\lambda(v)$							
f_q	q	f_q					
f_{q-1}	$q-1$	Bf_q	g_{q-1}				
f_{q-2}	$q-2$	$B^2 f_q$	Bg_{q-1}	g_{q-2}			
$\vdots$	$\vdots$						
f_k	k	$B^{q-k} f_q$	. . . . .	Bg_{k+1}	g_k		
f_{k-1}	$k-1$	$B^{q-(k-1)}$	. . . . .	$B^2 g_{k+1}$	Bg_k	g_{k-1}	
$\vdots$	$\vdots$	$\vdots$					
f_1	1	$B^{q-1} f_q$	. . . . .			Bg_2	g_1

Рассмотрим $f_q =< f_{q_1}, f_{q_2} ... f_{q_{(n_q - n_{q-1})}} >$ – систему линейно-независимых векторов, дополняющих базис e_{q-1} пространства $Ker\ B^{q-1}$ до базиса $Ker\ B^q$

$e_{q-1} \cup f_q$ – базис $Ker\ B^q = V^\lambda$

$ht_\lambda(f_{qj}) = q \quad j = \overline{1, n_q - n_{q-1}}$

$V^\lambda = Ker\ B^q = Ker\ B^{q-1} \oplus L[f_q] \Rightarrow Ker\ B^{q-1} \cap L[f_q] = \{\overline{0}\}$

Поместим f_q на этаже q.

Подействуем на все векторы f_q оператором B, получим систему

$B\, f_q =< Bf_{q1}, ..., Bf_{q(n_q - n_{q-1})} > \subset Ker\, B^{q-1}$,

высота этих векторов равна $q-1$

Рассмотрим $e_{q-2} \cup B\, f_q$ и докажем, что эта система линейно независима.

Пусть $\sum\limits_{j=1}^{n_{q-2}} \alpha_j e_{(q-2)j} + \sum\limits_{j=1}^{n_q - n_{q-1}} \beta_j BF_{qj} = \overline{0} \quad (*)$

Подействуем на $(*)$ $B^{q-2} \Rightarrow$

$\Rightarrow B^{q-1}(\sum\limits_{j=1}^{n_q - n_{q-1}} \beta_j f_{qj}) = \overline{0}$

$\sum\limits_{j=1}^{n_q - n_{q-1}} \beta_j f_{qj} \in Ker\, B^{q-1} \cap L[f_q] = \{\overline{0}\}$

$\sum\limits_{j=1}^{n_q - n_{q-1}} \beta_j f_{qj} = \overline{0} \ \Rightarrow\ \beta_j = 0\ \forall\, j = \overline{1, n_q - n_{q-1}}$, т.к. f_q - линейно независимая система

$(*) \ \Rightarrow\ \sum\limits_{j=1}^{n_{q-2}} \alpha_j e_{(q-2)j} = \overline{0} \ \Rightarrow\ \alpha_j = 0\ \forall\, j = \overline{1, n_{q-2}}$, т.к. e_{q-2} - линейно независимая система $\Rightarrow$

$\Rightarrow$ линейно-независимую систему $e_{q-2} \cup Bf_q$ можно дополнить до базиса всего пространства $Ker\ B^{q-1}$

Пусть g_{q-1} – дополняет линейно-независимую

систему векторов $e_{q-2} \cup Bf_q$,

$e_{q-2} \cup Bf_q \cup g_{q-1}$ – базис $Ker\ B^{q-1}$

g_{q-1} размещаем на этаже $q-1$

Обозначим $Bf_q \cup g_{q-1} = f_{q-1}$

Продолжаем спускаться вниз.
Если f_k – система на этаже k
$e_{k-1} \cup f_k$ – базис $Ker\ B^k \Rightarrow$
$Ker\ B^k = Ker\ B^{k-1} \oplus L[f_k] \Rightarrow Ker\ B^{k-1} \cap L[f_k] = \{0\}$
$\Rightarrow$ $e_{k-2} \cup B\, f_k$ - линейно независимая система (доказываем с помощью действия B^{k-2} на линейную комбинацию векторов этой системы, равную $\overline{0}$).
Линейно независимую систему $e_{k-2} \cup B\, f_k$ дополняем до базиса $Ker\, B^{k-1}$ и т.д. спускаемся вниз.
На этаже 1 получим $B\, f_2 \cup g_1 = f_1$ - базис $Ker\, B = V_\lambda$

$V^\lambda = Ker\, B^q = Ker\, B^{q-1} \oplus L[f_q] = Ker\, B^{q-2} \oplus L[f_{q-1}] \oplus L[f_q] ... =$
$= Ker\, B \oplus L[f_2] \oplus ... \oplus L[f_q] =$
$= L[f_1] \oplus L[f_2] \oplus ... \oplus L[f_q]$, f_k - базис $L[f_k]$ $\Rightarrow$
$\Rightarrow$ $f_1 \cup f_2 \cup ... \cup f_q = f$ - базис V^λ

В каждом столбце жордановой лестницы высоты k расположены векторы, образующие канонический базис циклическоого пространства вектора v, стоящего в этом столбце на последнем этаже k.

Можно перенумеровать векторы системы f, начиная с левого нижнего угла лестницы, двигаясь вверх по столбцу до конца, далее переходя к следующему столбцу на первом этаже.
Мы получим базис j_λ пространства V^λ - объединение канонических базисов циклических подпространства
В каждом из этих базисов матрица ограничения оператора A на соответствующее циклическое подпространство является жордановой клеткой.
Базис j_λ будет жордановым базисом пространства V^λ.

$A|_{V^\lambda j_\lambda}$ – жорданова форма с клетками Жордана $J_k(\lambda)$ на диагонали различного размера, отвечающими λ.

Следствие 1.

Число клеток Жордана в жордановой форме $A|_{V^\lambda}$ равно $k_\lambda = dim\, V_\lambda$.

Док-во:

Это число совпадает с числом столбцов в жордановой лестнице $\Rightarrow$ равно числу векторов на первом этаже.

На первом этаже стоит f_1 - базис $Ker\, B = V_\lambda$,

количество векторов в нём $dim\, Ker\, B = dim\, V_\lambda = k_\lambda$

Следствие 2.

Число жордановых клеток $J_k(\lambda)$, отвечающих λ, размера $k \times k$ в $A|_{V^\lambda j_\lambda}$

$N_{J_k(\lambda)} = r_{k+1} - 2r_k + r_{k-1}$,

где $r_k = rk(A - \lambda\mathcal{E})^k$, $k = \overline{1,q}$

Док-во:

$N_{J_k(\lambda)}$ равно числу столбцов жордановой лестницы для V^λ высоты k, т.е. числу векторов в системе g_k

$f_k = Bf_{k+1} \cup g_k$

Система f_k содержит $n_k - n_{k-1}$ векторов ($n_k = dim\, Ker(A - \lambda\mathcal{E})^k$).

Система Bf_{k+1}, как и f_{k+1}, содержит $n_{k+1} - n_k$ векторов.

$\Rightarrow$ система g_k содержит

$(n_k - nk - 1) - (n_{k+1} - n_k) = -n_{k+1} + 2n_k - n_{k-1} =$

$= -(n - r_{k+1}) + 2(n - r_k) - (n - r_{k-1}) =$

$r_{k+1} - 2r_k + r_{k-1} = N_{J_k(\lambda)}$, $k = \overline{1,q}$

При этом $r_{q+1} = r_q$,

$r_0 = rk(A - \lambda\mathcal{E})^0 = rk\, E = n$.

Лекция №4

1 Жорданова Форма

Теорема 1.

Пусть V – линейное пространство надо полем K,
$dim\, V = n < \infty, \quad A \in L(V, V)$
Если $f_A(t) = (\lambda_1 - t)^{s_1}(\lambda_2 - t)^{s_2}...(\lambda_k - t)^{s_k}$ – раскладывается над K на линейные множители, $\lambda_i \in K \quad i = \overline{1,k}, \quad \lambda_i \neq \lambda_j \quad i,j = \overline{1,k}$,
то $\exists$ жорданов базис j оператора A в пространстве V, в этом базисе матрица оператора A_j квазидиагональная, на диагонали - жордановы клетки $J(\lambda_i) \quad i = \overline{1,k}$ различных размеров.

Док-во:

$V = V^{\lambda_1} \oplus ... \oplus V^{\lambda_k}$
В $\forall \; V^{\lambda_i} \quad \exists$ жорданов базис j_i
$j = j_1 \cup j_2 \cup ... \cup j_k$ - жорданов базис в пространстве V
$A|_{V^{\lambda_i}}$ – квазидиагональная матрица, на диагонали жордановы клетки соответствуют λ_i

Следствие. В условиях теоремы 1
$A_e \sim A_j$ - жордановой форме
(матрица оператора приводится к жордановой форме)

Теорема 2. V - линейное пространство над $\mathbb{C}$, $dim\, V = n < \infty \Rightarrow$
$\Rightarrow \exists$ жорданов базис $\forall\, A \in L(V, V)$ в пространстве V.

Следствие. $\forall$ комплексная матрица подобна жордановой форме (приводится к жордановой форме).

Note. Если над полем K $f_A(t)$ не раскладывается на линейные множители, то $\exists$ поле $L \supset K$:
$f_A(t)$ раскладывается над L на линейные множители.
Из Т.1. $\Rightarrow$ $\exists$ жорданов базис оператора A в пространстве V над полем

L.
(Если V над $\mathbb{R}$ и $f_A(t)$ имеет комплексные корни, то V нужно рассмотреть над $\mathbb{C} \Rightarrow$ $\exists$ жорданов базис A в V над $\mathbb{C}$.)

2 Действительный аналог жордановой формы

Утв. V – линейное пространство над $\mathbb{R}$ $\quad dim\, V = n < \infty$
$f_A(t)$ имеет корень $\lambda = \alpha + i\beta \in \mathbb{C} \quad \beta \neq 0$
то $f_A(t)$ имеет и корень $\overline{\lambda} = \alpha - i\beta \in \mathbb{C}$
$\forall J_k(\lambda) \longmapsto J_k(\overline{\lambda})$ и

$$C = \left(\begin{array}{c|c} J_k(\lambda)_e & 0 \\ \hline 0 & J_k(\overline{\lambda})_e \end{array}\right) \in \mathbb{C}^{2k\times 2k} \text{ в базисе } e \cup f;$$

то $\exists$ базис b в V над $\mathbb{R}$, в котором матрица C имеет вид:

$$C_b = \left(\begin{array}{cccccc} \boxed{\begin{array}{cc}\alpha & \beta\\ -\beta & \alpha\end{array}} & \boxed{\begin{array}{cc}1 & 0\\ 0 & 1\end{array}} & 0 & \ldots & 0 \\ 0 & \boxed{\begin{array}{cc}\alpha & \beta\\ -\beta & \alpha\end{array}} & \boxed{\begin{array}{cc}1 & 0\\ 0 & 1\end{array}} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & \ldots & \ldots & \boxed{\begin{array}{cc}\alpha & \beta\\ -\beta & \alpha\end{array}} \end{array}\right) \in \mathbb{R}^{2k\times 2k}$$

Док-во:
$\exists\, e = e_1 ... e_k : \begin{cases} Ae_1 = \lambda e_1 \\ Ae_i = \lambda e_i + e_{i-1} \end{cases}$
$\exists\, f = \overline{e} =< f_1 ... f_k >=< \overline{e}_1, ..., \overline{e}_k >$
$\begin{cases} Af_1 = \lambda f_1 \\ Af_i = \overline{\lambda} f_i + f_{i-1} \end{cases}$
$e_j = g_j + ih_j \quad g_j, h_j \in \mathbb{R}^n$
$f = g_j - ih_j \quad < g_1, h_1, g_2, h_2, ..., g_k, h_k >= b$ базис.

Следствие.
$\forall$ матрицу над $\mathbb{R}$ можно привести к квазидиагональному виду, где на диагонали стоят жордановы клетки, отвечающие действительным корням характерестического многочлена $f_A(t)$, и действительные аналоги жордановых клеток, отвечающих парам комплексных сопряженных корней $f_A(t)$.

3 Единственность жордановой формы

Теорема 3. Если $\exists$ жорданова форма матрицы оператора, то она единственна с точностью до перестановки жордановых клеток.

Без доказательства.

4 Минимальный многочлен линейного оператора и его матрицы

$V -$ линейное пространство над полем K,
$dim\, V = n < \infty, \quad A \in L(V,V), \quad f(t) \in K[t], \quad f(A) \in L(V,V)$
Если $e -$ базис V, $\exists \Phi_e : A \longmapsto A_e -$ изоморфизм алгебр $L(V,V)$ и $K^{n\times n}$
$f(A)_e = f(A_e)$...

Опр. $f(t) \in K[t]$ называется аннулирующим многочленом $A \in L(V,V)$ и $A_e \in K^{n\times n}$, если $f(A) = \overline{0} (\Leftrightarrow f(A_e) = \overline{0})$.

Утв. 1. Если $dim\, V = n < \infty, \quad A \in L(V,V)$,
то $\exists$ аннулирующий многочлен для оператора A.

Док-во:
$dim\, V = n < \infty \Rightarrow dim\, L(V,V) = n^2 < \infty$.
$\exists\, k \in \mathbb{N} : A^0 = E, A, ..., A^{k-1}$ - линейно независимы,

а $E, A, ..., A^{k-1}, A^k$ - линейно зависимы.
$A^k = \alpha_1 A^{k-1} + .. + a_k E$
$f(t) = t^k - \alpha_1 t^{n-1} - ... - a_k$ - аннулирующий многочлен оператора A.

Опр. Назовём минимальным многочленом оператора A
$m_A(t) \in K[t]$ - его аннулирующий многочлен минимальной степени.

Утв. 2. $\forall$ аннулирующий многочлен оператора A делится на его минимальный многочлен.
Если $f(t) \in K[t] : f(A) = \overline{0} \Rightarrow f(t) \vdots m_A(t)$

Доказательство:
$K -$ поле $\Rightarrow k[t] -$ евклидово кольцо
$\exists q(t), r(t) : f(t) = m_A(t)q(t) + r(t),$
где $\left[\begin{array}{l} r(t) = 0 \\ deg\ r(t) < deg\ m_A(t) \end{array} \right.$
Пусть $r(t) \neq 0 \Rightarrow f(A) = m_A(A)q(A) + r(A)$
$\overline{0} = \overline{0} + r(A)$
$r(A) = \overline{0}$, но $deg\ r(t) < deg\ m_A(t)$ $\lightning$
$r(t) = 0$

Следствие. Минимальные многочлены одного и того же оператора ассоциированы, т.е. отличаются друг от друга множителем $\alpha \in K^*$.

Док-во:
$m_A^{(1)}(t), m_A^{(2)}(t)$ - минимальные многочлены
$\left\{ \begin{array}{l} m_A^{(1)}(t) \vdots m_A^{(2)}(t) \\ m_A^{(2)}(t) \vdots m_A^{(1)}(t) \end{array} \right. \Leftrightarrow m_A^{(1)}(t) \sim m_A^{(2)}(t)$

Note. Если положить в $m_A(t)$ старший коэффициент равным 1, то $m_A(t)$ будет определён однозначно.

Опр. $m_A(t) \in K[t]$ - минимальный многочлен для A, если:
1) $m_A(A) = 0$,
2) $deg\, m_A(t) = min\{deg\, f(t) : f(t) \in K[t]$ и $f(A) = \overline{0}\}$

3) Старший коэффициент $m_A(t)$ $\alpha_0 = 1$.

Note. $m_A(t) = m_{A_e}(t)$ $\forall$ базиса e пространства V.

Примеры:

1) $A = O$

$m_O(t) = t = m_0(t)$

2) $A = \mathcal{E}$

$m_{\mathcal{E}}(t) = t - 1 = m_E(t)$

Утв. 3.

Если $J_k(\lambda) = \begin{pmatrix} \lambda & 1 & ... & 0 \\ \vdots & \lambda & \ddots & \vdots \\ \vdots & \ddots & \lambda & 1 \\ 0 & ... & ... & \lambda \end{pmatrix} \in K^{k\times k} \Rightarrow m_{J_k(\lambda)} = (t-\lambda)^k$

Док-во:

$J_K(\lambda)$ − матрица оператора A, действующего в циклическом пространстве L_v вектора $v \in V^\lambda$, $ht_\lambda(v) = k$, в каноническом базисе этого пространства $< B^{k-1}v, B^{k-2}v, ..., v >= e$, где $B = (A - \lambda\mathcal{E})$

$B^k w = (A - \lambda\mathcal{E})^k w = \overline{0} \quad \forall w \in L_v \Rightarrow (A - \lambda\mathcal{E})^k = O$ в L_v

и $(A - \lambda\mathcal{E})^l v \neq \overline{0} \quad \forall l = \overline{1, k-1} \Rightarrow (A - \lambda\mathcal{E})^l \neq O$ в L_v

$(t-\lambda)^k = m_{J_k(\lambda)}(t)$

Утв. 4.

Если $V = V_1 \oplus ... \oplus V_k$,

$dim\, V = n < \infty$, V_i - подпространство V, $i = \overline{1, k}$, V_i - инвариантно относительно A,

$A \in L(V, V)$,

то $m_A(t) =$ НОК$\{m_{A|_{V_1}}(t), m_{A|_{V_2}}(t), ..., m_{A|_{V_k}}(t)\}$.

Док-во:

e_i - базис V_i

$e = e_1 \cup e_2 \cup ... \cup e_k$ - базис V

$$A_e = \begin{pmatrix} \boxed{A|_{V_1 e_1}} & & 0 \\ & \ddots & \\ 0 & & \boxed{A|_{V_1 e_k}} \end{pmatrix}$$

$m_A(t)$ - аннулирующий многочлен для $A|_{V_i} \Rightarrow m_A(t) \ : \ m_{A|_{V_i}}(t), \ \ i = \overline{1,k}$
$\Rightarrow m_A(t) =$ НОК$\{m|_{A_{V_1}}, \dots, m|_{A_{V_k}}\}$

Утв. 5. Минимальный многочлен оператора A, действующего в корневом пространстве $V^\lambda, \quad dim\, V^\lambda = s_\lambda$,
$m_{A|_{V^\lambda}}(t) = (t-\lambda)^q$, где $q_\lambda = min\{k \in N \ : \ dim\, Ker(A - \lambda\mathcal{E})^k = s_\lambda\}$
- максимальный размер жордановой клетки, отвечающей λ.

Док-во:
V^λ является прямой суммой циклических пространств.
В каждом из которых в каноническом базисе матрица оператора - жорданова клетка $J_k(\lambda)$
$m_{J_k(\lambda)} = (t-\lambda)^k$
$m_{A|_{V^\lambda}} = (t-\lambda)^{q_\lambda}$, т.к. $q_\lambda -$ максимальный размер соответсвующей жордановой клетки.

Теорема 4.
Если V - линейное пространство над $K, \ \ dim\, V = n < \infty$,
$A \in L(V,V)$,
$f_A(t) = (\lambda_1 - t)^{S_1} \dots (\lambda_k - t)^{S_k}$ раскладывается на линейные множители,
то $m_A(t) = \prod\limits_{i=1}^{k} (t-\lambda_1)^{q_{\lambda_i}}$
Док-во: $\Leftarrow$ утв. 4 и 5.

Следствие 1. Жорданова форма оператора A диагональна $\Leftrightarrow m_A(t)$ не имеет кратных корней.

Док-во:
Жорданова форма оператора A диагональна $\Leftrightarrow$ все жордановы клетки

имеют размер $1 \Leftrightarrow q_i = 1, \quad i = \overline{1,k}$

Следствие 2. Если жорданова форма оператора A диагональна $\Rightarrow$ жорданова форма его ограничения $A|_U$ на $\forall$ инвариантное подпространство $U \subset V$ также диагональна.

Док-во:

Пусть U - инвариантное подпространство.

$m_A(A) = \overline{0} \Rightarrow m_A(A|_U) = \overline{0}$

$\Downarrow$

$m_A(t) \vdots m_{A|_U}(t)$

жорданова форма оператора A диагональная $\Rightarrow$

$\Rightarrow m_A(t)$ не имеет кратных корней, т.е.

$m_A(t) = (t - \lambda_1)...(t - \lambda_k) \Rightarrow$

$\Rightarrow m_{A|_U}(t)$ не имеет кратных корней $\Rightarrow$

$\Rightarrow$ жорданова форма $A|_U$ диагональна.

Лекция №5

1 Теорема Гамильтона-Кэли

Если V - линейное пространство над K, $dim\, V = n < \infty$, $A \in L(V,V)$, то $f_A(A) = \overline{0}$.

Док-во:

$\left.\begin{array}{l} m_A(t) = m_{A_e}(t) \\ f_A(t) = f_{A_e}(t) \end{array}\right\}$ $\forall$ базиса e.

1) Пусть $f_A(t)$ раскладывается на линейные множитнли над K.

$f_A(t) = (\lambda_1 - t)^{s_1}...(\lambda_k - t)^{s_k}$

$\Rightarrow m_{A_i}(t) = m_A(t) = (t - \lambda_1)^{q_1}...(t - \lambda_k)^{q_k}$, где $q_i \leqslant s_i$.

$f_A(t) \vdots m_A(t) \Rightarrow f_A(A) = 0$

2) Если $f_A(t)$ не раскладывается на линейные множители над K, то (докажем позже) $\exists$ поле $L \supset K$: над L $f_A(t)$ раскладывается на линейные множители.

Рассмотрим V как линейное пространство над L, A_e как матрицу с элементами из L п.1)$\Rightarrow f_{A_e}(A_e) = \overline{0}$, но $f_{A_e}(t)$ не зависит от того, над L или над K мы рассмотрим A_e.

$f_{A_e}(A_e) = \overline{0} \Rightarrow f_A(A) = 0$

Пример:

$A \in L(V,V), dim\, V = 2$

$A^2 - (tr\, A)A + (det\, A)E = \overline{0}$, т.к $f_A(t) = t^2 - (tr\, A)t + det\, A$

2 Кольца и поля

Опр.

$A -$ множество с двумя операциями оператора $a, b \longmapsto \begin{cases} a+b \in A \\ ab \in A \end{cases}$,
удовлетворяющими аксиомам

1) $a + b = b + a \; \forall \; a, b \in A$

2) $(a + b) + c = a + (b + c) \; \forall \; a, b, c \in A$

3) $\exists \; \overline{0} : a + \overline{0} = \overline{0} + a = a \; \forall a \in A$

4) $\forall a \in A \, \exists (-a) : a + (-a) = (-a) + a = \overline{0}$

5) $\begin{cases} a(b + c) = ab + bc \\ (a + b)c = ac + bc \end{cases} \quad \forall a, b, c \in A \quad$ дистрибутивность

$\underline{1) - 5) \Rightarrow A \text{ - кольцо}}$

6) $ab = ba \quad \forall a, b \in A$

$\underline{1) - 6) \Rightarrow A \text{ - коммутативное кольцо}}$

7) $(ab)c = a(bc) \quad \forall a, b, c \in A$

$\underline{1) - 5), 7) \Rightarrow A \text{ - ассоциативное кольцо}}$

8) $\exists \; 1 \in A : 1a = a1 = a \quad \forall a \in A$

$\underline{1) - 5), 8) \Rightarrow A \text{ - кольцо с 1}}$
$\underline{1) - 8) \Rightarrow A \text{ - коммутативное ассоциативное кольцо с 1}}$ (A - КАК1)

9) $\forall a \in A \setminus \{\overline{0}\} \;\; \exists \; a^{-1} \in A : \quad aa^{-1} = a^{-1}a = 1$

10) $|A| > 1$

$\underline{1) - 10) \Rightarrow A - \text{поле}}$
$\underline{1) \text{ - } 5), 7) \text{ - } 10) \Rightarrow \ A \text{ - тело}}$

Примеры:

1) $(V^3, +, [,])$

1) - 5) выполняются

6) не выполняется

$[a,b] = -[b,a]$ антикоммутативность $\Leftrightarrow \ [a,a] = \overline{0} \quad (*)$

7) не выполняется, но

$\big[[a,b],c\big] + \big[[b,c],a\big] + \big[[c,a],b\big] = \overline{0}$ тождество Якоби $(**)$

8) не выполняется

$\forall\, a \in V^3 \setminus \{\overline{0}\}$

$[a,b] \neq a \ \forall\, b \in V^3$

$(V^3, +, [\,])$ - некоммутативное, неассоциативное кольцо без 1

$\begin{cases} *) \\ **) \end{cases} \Rightarrow$ - кольцо Ли

2) Q_8 - группа кватернионов

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

$\mathbb{H} = \{a + bi + cj + dk, \ a,b,c,d \in \mathbb{R}\}$

$(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) =$

$= (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k$

$(a_1 + b_1 i + c_1 j + d_1 k)\,(a_2 + b_2 i + c_2 j + d_2 k) =$

$= a_1 a_2 + b_1 a_2 i + c_1 a_2 j + d_1 a_2 j + a_1 b_2 i + ... + d_1 d_2 k^2$

$\mathbb{H}$ - тело кватернионов

$1 \mapsto E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \ i \mapsto I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$

$j \mapsto J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \ k \mapsto K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

$$\mathbb{H} = \left\{ \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}, \quad a,b,c,d \in \mathbb{R} \right\} =$$

$$= \left\{ \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}, \quad \alpha = a+ib,\ \beta = c+id \in \mathbb{C} \right\}.$$

1) - 5) выполняются.

6) не выполняется.

$ij = k \ \ ji = -k$

$h = a + bi + cj + dk \neq \overline{0} \ \Leftrightarrow \ a^2 + b^2 + c^2 + d^2 \neq 0.$

$\forall h \in \mathbb{H}\backslash\{\overline{0}\} \quad \exists\, (a+bi+cj+dk)^{-1} =$

$$= \frac{a-bi-cj-dk}{(a+bi+cj+dk)(a-bi-cj-dk)} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2} \in \mathbb{H},$$

т.к. $(a+bi+cj+dk)(a-bi-cj-dk) = a^2 + abi + acj + adk - abi + b^2 +$
$+ bck - bdi - acj - bck + c^2 + cdi - adk + bdj - cdi + d^2 = a^2 + b^2 + c^2 + d^2$

	i	j	k
i	-1	k	-j
j	-k	-1	i
k	j	-i	-1

3 Следствия аксиом

1) $\overline{0}$ - единиственный

2) $\forall\, a \in A \ \ (-a)$ - единственный

3) $\forall\, a,b \in A \ \exists!$ решение $a + x = b$

$x = b + (-a) = b - a$ разность

1)-3) были доказаны в прошлом семестре как следствия аксиом группы.

4) $\overline{0} \cdot a = a \cdot \overline{0} = \overline{0}$

Док-во:

$\overline{0} \cdot a = (\overline{0} + \overline{0})a = \overline{0}a + \overline{0}$

$\exists(-\overline{0} \cdot a) \in A$

$\overline{0} = \overline{0} \cdot a$

Аналогично $a \cdot \overline{0} = \overline{0}$

5) Если $1 \in A$, то она единственная

Док-во:

Пусть e_1, e_2 - единицы,

$e_1 = e_1 e_2 = e_2$.

6) Если $\overline{0} = 1 \Rightarrow A = \{\overline{0}\}$

Док-во:

Пусть $a \neq 0,\ a \in A$

$\overline{0} = \overline{0} \cdot a = 1 \cdot a = a$ ☒

7) (-a)b = a(-b) = -ab

Док-во:

$ab + (-a)b = (a + (-a))b = 0 \cdot b = 0$

$(-a)b + ab = 0 \Rightarrow -ab = (-a)b$

Аналогично $a(-b) = -ab$

8) Если A – ассоциативно-коммутативное кольцо с 1 и $\exists\, a^{-1}$, то a^{-1} единственный.

Док-во:

$a_2^{-1} = 1a_2^{-1} = (a_1^{-1}a)a_2^{-1} = a_1^{-1}(a\ a_2^{-1}) = a_1^{-1}1 = a_1^{-1}$

9) A - тело

$\forall a, b \in A,\ a \neq 0$

$\exists!$ решение $ax = b, \quad x = a^{-1}b$

$\exists!$ решение $xa = b, \quad x = ba^{-1}$

Док-во: доказать самим. (доказывается стандартно)

4 Подкольцо

Опр. Непустое подмножество кольца называется подкольцом, если оно само является кольцом относительно операций, определенных в кольце и ограниченных на это поддмножество.

Note.
Пусть $B -$ подкольцо кольца A, тогда
$A -$ комутативное кольцо $\Rightarrow$ $B -$ комутативное кольцо
$A -$ ассоциативное кольцо $\Rightarrow$ $B -$ ассоциативное кольцо
$A -$ кольцо с $1 \Rightarrow$ в $B -$ может быть $1 \in A$, может быть своя единица, B может вообще не иметь единицы.

Примеры: Пусть $A = \big(\mathbb{R}^{n\times n}, +, \cdot\big) = gl\big(\mathbb{R}, n\big)$ - некоммутативное ассоциативное кольцо с $1 = E$.

1) $B = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \quad a, b, c \in \mathbb{R} \right\}$ -
- некоммутативное ассоциативное кольцо с $1 = E$

2) $B = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \quad a \in \mathbb{R} \right\}$ -
- коммутативное ассоциативное кольцо с $1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq E$.

3) $B = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, \quad a, b \in \mathbb{R} \right\}$ -
- некоммутативное ассоциативное кольцо без 1, т.к.

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad \forall \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in B$$

4.1 Критерий того, что подмножества кольца является подкольцом

Пусть $A -$ кольцо, тогда

$B \subset A$ является подкольцом A

$$\Updownarrow$$

1) $\overline{0} \in B$

2) $b_1,\ b_2 \in B \Rightarrow b_1 + b_2 \in B$

3) $\forall b \in B \Rightarrow (-b) \in B$

4) $\forall b_1,\ b_2 \in B \Rightarrow b_1 b_2 \in B$

Док-во: 1), 2), 3) $\Leftrightarrow B -$ аддитивная подгруппа A (см. III семестр)
Все аксиомы кольца A, выражаемые тождествами, верны в $B \subset A$

Лекция №6

1 Подполе

Опр. Подмножеством поля называется его подполе, если оно само является полем относительно операций, определённых в поле и ограниченных на это подмножество.

Утв. 1. Если A - поле, B - его подкольцо,
$\widetilde{1}$ - единица B, то $\widetilde{1} = 1 \in A$.

Док-во: $\widetilde{1} = \widetilde{1} \cdot \widetilde{1}$ $(*)$
т.к. A - поле, $\exists\, \widetilde{1}^{-1}$, умножим $(*)$ на $\widetilde{1}^{-1}$ $\Rightarrow$ $1 = \widetilde{1}$.

1.1 Критерий того, что подмножество поля является подполем

Пусть A - поле, тогда $B \subset A$ является подполем $A \Leftrightarrow$

$$\Leftrightarrow \begin{cases} 1) & \overline{0} \in B \\ 2) & \forall\, b_1, b_2 \in B \Rightarrow b_1 + b_2 \in B \\ 3) & \forall\, b \in B \Rightarrow (-b) \in B \\ 4) & b_1 b_2 \in B \\ 5) & 1 \in B \\ 6) & \forall\, b \in B \setminus \{\overline{0}\} \Rightarrow b^{-1} \in B \end{cases}$$

Док-во:
1), 2), 3) $\Leftrightarrow$ B - аддитивная подгруппа A.
4), 5), 6) $\Leftrightarrow$ $B \setminus \{\overline{0}\}$ - мультипликативная подгруппа $A \setminus \{\overline{0}\}$.
Все аксиомы, выражаемые тождествами верны в $B \subset A$.

2 Целостное кольцо

Напомним

Опр. Областью целостности, или целостным кольцом (ЦК), называется коммутативное ассоциативное кольцо с 1 (КАК1) без делителей нуля.

Note. Подразумевается, что в целостном кольце есть ненулевые элементы, т.е. число его элементов больше 1.

Утв. 2. Конечное целостное кольцо явдяется полем.

Док-во:

Пусть A - ЦК и $|A| = n < \infty$.
Нужно доказать, что $\forall\, a \in A \setminus \{\overline{0}\}\ \ \exists\, a^{-1} \in A : aa^{-1} = a^{-1}a = 1$.
Пусть $A = \{a_1, a_2, ..., a_n\},\ a_i \neq a_j$ при $i \neq j,\ i, j = \overline{1, n}\ \Rightarrow$
$\Rightarrow\ \forall\, a \in A \setminus \{\overline{0}\}\ \ aa_i \neq aa_j$ при $i \neq j,\ i, j = \overline{1, n}$, т.к.
в области целостности A возможно "сокращение". $\Rightarrow$
$\Rightarrow \{aa_1, aa_2, ..., aa_n\} = A \ni 1 \Rightarrow$
$\Rightarrow \exists\, k \in \{1, 2, ..., n\} : aa_k = 1 \Rightarrow a_k = a^{-1}$.

3 Поле отношений целостного кольца

Мы покажем, что любую область целостности A можно вложить в некоторое поле $Quot\, A$ - её поле отношений подобно тому,
как $\mathbb{Z} \subset \mathbb{Q} = Quot\, \mathbb{Z}$.
(В случае конечной области целостности $A = Quot\, A$)

Опр. Пусть A - ЦК, $(a_i, b_i) \in A \times (A \setminus \{\overline{0}\}),\ i = \overline{1, 2}$
Получим $(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 b_2 = b_1 a_2$

Утв. 1. „$\sim$“ является отношением эквивалентности.

Док-во:

1) рефлексивность
$ab = ba \Rightarrow (a, b) \sim (b, a)$
2) симметричность
$(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 b_2 = a_2 b_1 \Leftrightarrow a_2 b_1 = a_1 b_2 \Leftrightarrow (a_2, b_2) \sim (a_1, b_1)$
3) транзитивность
$$\begin{cases} (a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 b_2 = b_1 a_2 \Leftrightarrow a_1 b_2 b_3 = b_1 a_2 b_3 \\ (a_2, b_2) \sim (a_3, b_3) \Leftrightarrow a_2 b_3 = b_2 a_3 \Leftrightarrow a_2 b_3 b_1 = b_2 a_3 b_1 \end{cases} \Rightarrow$$
$\Rightarrow a_1 b_2 b_3 = b_2 a_3 b_1 \Rightarrow a_1 b_3 = a_3 b_1 \Rightarrow (a_1, b_1) \sim (a_3, b_3)$

$$\left.\begin{array}{l} 1) \\ 2) \\ 3) \end{array}\right\} \Rightarrow \text{„}\sim\text{“ - отношение эквивалентности}$$

Следствие. Отношение эквивалетности „$\sim$“ разбивает множество пар $A \times (A \setminus \{\overline{0}\})$ на непересекающиеся классы эквивалентности.

Обозначим $\frac{a}{b}$ класс эквивалентности пары (a, b), а множество всех классов эквивалентности $Quot\, A = \left\{\frac{a}{b}\right\}$.

Утв. 5.

$(a, b) \sim (ca, cb)\ \forall\, c \in A \setminus \{\overline{0}\}$

Док-во:

$ab = ba \Rightarrow cab = cba\ \ \forall\, c \in A \setminus \{\overline{0}\} \Rightarrow (ca, cb) \sim (a, b)\ \forall\, c \in A \setminus \{\overline{0}\}$

Утв. 6.

$(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow (b_2a_1, b_1b_2) \sim (b_1a_2, b_1b_2)$

Док-во:

$(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1b_2 = b_1a_2 \Leftrightarrow a_1b_2(b_1b_2) = b_1a_2(b_1b_2) \Leftrightarrow$
$\Leftrightarrow (a_1b_2, b_1b_2) \sim (b_1a_2, b_1b_2)$

Опр. Введём на множестве пар $A \times (A \setminus \{\overline{0}\})$
операции сложения и умножения:
$(a_1, b_1) + (a_2, b_2) = (a_1b_2 + b_1a_2, b_1b_2)$,
$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$.

Покажем, что введённые операции согласованы с отношением эквивалетности.

Утв. 7.

$$\left\{\begin{array}{l} (a_1, b_1) \sim (a_1', b_1') \\ (a_2, b_2) \sim (a_2', b_2') \end{array}\right. \Rightarrow (a_1, b_1) + (a_2, b_2) \sim (a_1', b_1') + (a_2', b_2')$$

Док-во:

$(a_1, b_1) + (a_2, b_2) = (a_1b_2 + b_1a_2, b_1b_2) \sim \big((a_1b_2 + b_1a_2)b_1', (b_1b_2)b_1'\big) =$

$= (a_1b_2b_1' + b_1a_2b_1', b_1b_2b_1') \overset{\text{т.к. } a_1b_1'=a_1'b_1}{=} (a_1'b_1b_2 + b_1a_2b_1', b_1b_2b_1') =$
$= \big((a_1'b_2 + a_2b_1')b_1, b_1(b_2b_1')\big) \sim (a_1'b_2 + a_2b_1', b_1'b_2) = (a_1', b_1') + (a_2, b_2)$

Т.о., $(a_1, b_1) + (a_2, b_2) \sim (a_1', b_1') + (a_2, b_2)$, т.е. суммы пар будут эквивалентными, если одно из слагаемых заменить на эквивалентное. $\Rightarrow$
$\Rightarrow (a_1, b_1) + (a_2, b_2) \sim (a_1', b_1') + (a_2, b_2) \sim (a_1', b_1') + (a_2', b_2')$

Утв. 8.
$$\begin{cases} (a_1, b_1) \sim (a_1', b_1') \\ (a_2, b_2) \sim (a_2', b_2') \end{cases} \Rightarrow (a_1, b_1)(a_2, b_2) \sim (a_1', b_1')(a_2', b_2')$$
Док-во:
$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2) \sim (a_1a_2b_1', b_1b_2b_1') \overset{a_1b_1'=a_1'b_1}{=}$
$= (a_1'b_1a_2, b_1b_2b_1') \sim (a_1'a_2, b_2b_1') = (a_1', b_1')(a_2, b_2)$

Т.о., $(a_1, b_1)(a_2, b_2) \sim (a_1', b_1')(a_2, b_2)$, т.е. произведения пар будет эквивалентными, если один из сомножителей заменить на эквивалентный.
$\Rightarrow (a_1, b_1)(a_2, b_2) \sim (a_1', b_1')(a_2, b_2) \sim (a_1', b_1')(a_2', b_2')$

Опр. Определим операции сложения и умножения на множестве классов эквивалентности $Quot\ A = \left\{\dfrac{a}{b}\right\}$:
$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1b_2 + b_1a_2}{b_1b_2},$$
$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1a_2}{b_1b_2}$$

Из утверждений 7,8 следует, что это определение корректно.

Утв. 9. *Quot A* с введенными операциями сложения и умножения является полем.

Док-во: Проверим выполнение аксиом поля.

1) $\dfrac{a_1}{b_1} + \dfrac{a_2}{b_2} = \dfrac{a_1b_2 + b_1a_2}{b_1b_2} = \dfrac{a_2}{b_2} + \dfrac{a_1}{b_1}$

2) $\left(\frac{a_1}{b_1}+\frac{a_2}{b_2}\right)+\frac{a_3}{b_3}=\frac{a_1b_2+b_1a_2}{b_1b_2}+\frac{a_3}{b_3}=\frac{a_1b_2b_3+b_1a_2b_3+a_3b_1b_2}{b_1b_2b_3}=$

$=\frac{a_1}{b_1}+\frac{a_2b_3+b_2a_3}{b_2b_3}=\frac{a_1}{b_1}+\left(\frac{a_2}{b_2}+\frac{a_3}{b_3}\right)$

3) $\frac{0}{1}\in Quot\ A: \frac{a}{b}+\frac{0}{1}=\frac{a+0}{1\cdot b}=\frac{0+a}{1\cdot b}=\frac{a}{b}$

4) $\forall\ \frac{a}{b}\in Quot\ A \quad \exists(-\frac{a}{b})=\frac{(-a)}{b}\in Quot\ A:$

$\frac{a}{b}+\frac{(-a)}{b}=\frac{ab+(-a)b}{b\cdot b}=\frac{0\cdot b}{b^2}=\frac{0}{b}=\frac{0}{1}$

5) $\frac{a_1}{b_1}\left(\frac{a_2}{b_2}+\frac{a_3}{b_3}\right)=\frac{a_1}{b_1}\cdot\frac{a_2b_3+b_2a_3}{b_2b_3}=\frac{a_1a_2b_3+a_1a_3b_2}{b_1b_2b_3}=\frac{a_1a_2b_3}{b_1b_2b_3}+\frac{a_1a_3b_2}{b_1b_2b_3}=$

$=\frac{a_1a_2}{b_1b_2}+\frac{a_1a_3}{b_1b_3}=\frac{a_1}{b_1}\cdot\frac{a_2}{b_2}+\frac{a_1}{b_1}\cdot\frac{a_3}{b_3}$

Аналогично, $\left(\frac{a_1}{b_1}+\frac{a_2}{b_2}\right)\cdot\frac{a_3}{b_3}=\frac{a_1}{b_1}\cdot\frac{a_3}{b_3}+\frac{a_2}{b_2}\cdot\frac{a_3}{b_3}$

6) $\frac{a_1}{b_1}\cdot\frac{a_2}{b_2}=\frac{a_1a_2}{b_1b_2}=\frac{a_2}{b_2}\cdot\frac{a_1}{b_1}$

7) $\left(\frac{a_1}{b_1}\cdot\frac{a_2}{b_2}\right)\cdot\frac{a_3}{b_3}=\frac{a_1a_2}{b_1b_2}\cdot\frac{a_3}{b_3}=\frac{a_1a_2a_3}{b_1b_2b_3}=\frac{a_1}{b_1}\cdot\frac{a_2a_3}{b_2b_3}=\frac{a_1}{b_1}\cdot\left(\frac{a_2}{b_2}\cdot\frac{a_3}{b_3}\right)$

8) $\frac{1}{1}\in Quot\ A: \frac{a}{b}\cdot\frac{1}{1}=\frac{1}{1}\cdot\frac{a}{b}=\frac{a}{b}$

9) $\forall\ \frac{a}{b}\in Quot\ A\setminus\left\{\frac{0}{1}\right\} \quad \exists\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}\in Quot\ A$, т.к.
$\frac{a}{b}\neq\frac{0}{1}\Leftrightarrow a\neq 0$, поскольку $\frac{a}{b}=\frac{0}{1}\Leftrightarrow(a,b)=(0,1)\Leftrightarrow(a,b)=(0,1)\Leftrightarrow$

$\Leftrightarrow a\cdot 1=b\cdot 0\Leftrightarrow a=0$ и $\frac{a}{b}\cdot\frac{b}{a}=\frac{b}{a}\cdot\frac{a}{b}=\frac{ab}{ab}=\frac{1}{1}$

10) $\frac{0}{1}\neq\frac{1}{1}$, т.к. $(0,1)\sim(1,1)\Leftrightarrow 0\cdot 1=1\cdot 1\Leftrightarrow 0=1,\Rightarrow |Quot\ A|>1$

Утв. 10. Отображение $\varphi: A\to Quot\ A: \varphi(a)=\frac{a}{1}\in Quot\ A \quad \forall a\in A$ является мономорфизмом колец.

Док-во:

$$\varphi(a_1 + a_2) = \frac{a_1 + a_2}{1} = \frac{a_1 \cdot 1 + a_2 \cdot 1}{1 \cdot 1} = \frac{a_1}{1} + \frac{a_2}{1} = \varphi(a_1) + \varphi(a_2)$$

$$\varphi(a_1 a_2) = \frac{a_1 a_2}{1} = \frac{a_1 a_2}{1 \cdot 1} = \frac{a_1}{1} \cdot \frac{a_2}{1} = \varphi(a_1) \cdot \varphi(a_2)$$

$$Ker\ \varphi = \left\{ a \in A :\ \varphi(a) = \frac{0}{1} \Leftrightarrow \frac{a}{1} = \frac{0}{1} \Leftrightarrow a = 0 \right\} = \{0\}$$

Note:

φ является вложением A в $Quot\ A$, можно отождествить $a \in A$ с $\frac{a}{1} \in Quot\ A$. Тогда уравнение $xb = a$ может быть переписано в поле $x\frac{b}{1} = \frac{a}{1} \Rightarrow$ в поле $Quot\ A$ оно имеет единственное решение $x = \frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1} = \frac{a}{1} \cdot \frac{1}{b} = \frac{a}{b}$,
аналогично и $bx = a$ имеет единственное решение $\frac{a}{b}$.

Утв. 11. *$Quot\ A$ – наименьшее по включению поле, содержащее A.*

Док-во:

Пусть F – поле : $F \supset A$

$$\left.\begin{array}{l} \forall\, a \in A \Rightarrow \frac{a}{1} \in F \\ \forall b \in A \setminus \{0\} \Rightarrow \frac{b}{1} \in F \Rightarrow \frac{1}{b} \in F \end{array}\right\} \Rightarrow \frac{a}{1} \cdot \frac{1}{b} = \frac{a}{b} \in F \Rightarrow Quot\ A \subset F$$

Примеры:

1) $\mathbb{Z}$ – ЦК $\Rightarrow Quot\ \mathbb{Z} = \mathbb{Q}$ – поле рациональных чисел

2) K – поле $\Rightarrow K[x]$ – ЦК $\Rightarrow Quot\ K[x] = K(x)$ – поле рациональных функций.

Лекция №7

1 Евклидово кольцо

Вспомним:

Опр. Целостное кольцо(ЦК) A называется евклидовым(ЕК), если $\exists$ функция, называемая нормой (высотой): $N : A \setminus \{\overline{0}\} \to \mathbb{Z}_+ = \mathbb{N} \cup \{0\}$:
1) $N(ab) \geqslant N(a) \quad \forall\, a, b \in A$, причём $N(ab) = N(a) \;\Leftrightarrow\; b \in A^*$
2) $\forall\, a, b \in A, \quad b \neq 0$

$\exists\, q, r \in A : \quad a = qb + r$, где $\left[\begin{array}{c} r = \overline{0} \\ N(r) < N(b) \end{array} \right.$

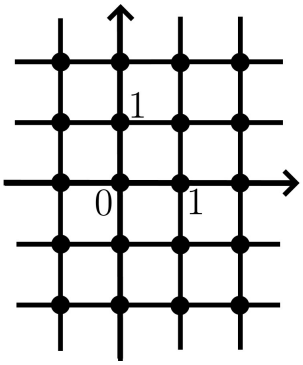
Нам хорошо известны примеры евклидовых колец:
1) $\mathbb{Z} -$ ЕК с $N(a) = |a| \quad \forall a \in \mathbb{Z} \setminus \{\overline{0}\}$,
2) $K -$ поле, $K[x] -$ ЕК с $N(p(x)) = deg\ p(x) \quad \forall p(x) \in K[x] \setminus \{\overline{0}\}$
Ещё один интересный пример ЕК представляют.

2 Целые гауссовы числа

Рассмотрим множество целых гауссовых чисел

$\mathbb{Z}[\,i\,] = \{a + ib : \; a, b \in \mathbb{Z}\} \subset \mathbb{C}$

На комплексной плоскости они располагаются в узлах сетки квадратов со стороной 1.



Легко видеть, что $\mathbb{Z}[\,i\,] \subset \mathbb{C}$ удовлетворяет критерию подкольца и содержит $1 = 1 + 0i$

$\mathbb{C} -$ поле $\Rightarrow \mathbb{Z}[\,i\,] -$ ЦК

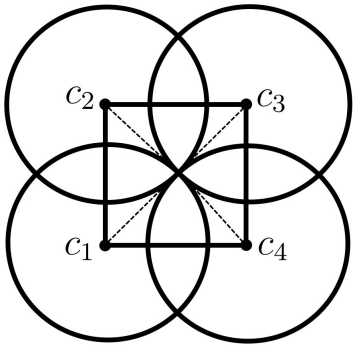
Найдём $(\mathbb{Z}[\,i\,])^*$.
Пусть $z \in \mathbb{Z}[\,i\,] \setminus \{0\} \; : \exists\, z^{-1} \in \mathbb{Z}[\,i\,] : z \cdot z^{-1} = 1 \Rightarrow$
$\Rightarrow |z| \cdot |z^{-1}| = 1$, но $|z|, |z^{-1}| \geqslant 1 \Rightarrow |z| = 1 \Rightarrow z \in \{1, -1, i, -i\}$

Очевидно, $1, -1, i, -i$ являются обратимыми в $\mathbb{Z}[\,i\,]$ $\Rightarrow$
$\Rightarrow (\mathbb{Z}[\,i\,])^* = \{1, -1, i, -i\}$

Рассмотрим функцию нормы
$z = a + ib \longmapsto N(z) = N(a + ib) = a^2 + b^2 = |z|^2$
Будем считать, что $N(z)$ определена на $\mathbb{Z}[\,i\,]\setminus\{0\}$
$N : \mathbb{Z}[\,i\,]\setminus\{0\} \to \mathbb{Z}_+$
$(\forall\, z \in \mathbb{Z}[\,i\,]\setminus\{0\} \;\; N(z) \geqslant 1)$
Проверим условия для $N(z)$ из определения ЕК:
1) $N(z_1 z_2) = |z_1 z_2|^2 = |z_1|^2 \cdot |z_2|^2 = N(z_1)N(z_2) \geqslant N(z_1)$,
причём $N(z_1 z_2) = N(z_1)N(z_2) = N(z_1) \Leftrightarrow$
$\Leftrightarrow N(z_2) = |z_2|^2 = 1 \Leftrightarrow z_2 \in (\mathbb{Z}[\,i\,])^*$
2) Покажем, что

$$\forall\, z_1, z_2 \in \mathbb{Z}[\,i\,], z_2 \neq 0 \;\; \exists\, q, r \in \mathbb{Z}[\,i\,] : z_1 = qz_2 + r, \left[\begin{array}{l} r = 0 \\ N(r) < N(z_2) \end{array}\right.$$

Пусть $\dfrac{z_1}{z_2} = z \in \mathbb{C}$.
Точка z находится в каком-то квадрате $c_1c_2c_3c_4$ со стороной 1,
$c_j \in \mathbb{Z}[\,i\,],\; j = \overline{1,4}$.



Диагональ квадрата имеет длину $\sqrt{2}$. $\Rightarrow$ 4 круга радиуса $\dfrac{\sqrt{2}}{2}$ с центрами в вершинах полностью покрывают квадрат. $\Rightarrow$ Среди вершин квадрата есть хотя бы одна, расстояние от которой до точки z не превосходит $\dfrac{\sqrt{2}}{2}$. Назовём эту вершину $q \in \mathbb{Z}[\,i\,]$.

$$|z - q| \leqslant \frac{\sqrt{2}}{2} \Leftrightarrow \left|\frac{z_1}{z_2} - q\right|^2 \leqslant \frac{1}{2}$$

$r = z_1 - qz_2 \in \mathbb{Z}[\,i\,]$

Если $r \neq 0$, то $N(r) = |r|^2 = |z_1 - qz_2|^2 = \left| z_2\left(\frac{z_1}{z_2} - q\right)\right|^2 =$

$= |z_2|^2\left|\frac{z_1}{z_2} - q\right|^2 \leqslant |z_2|^2\frac{1}{2} = \frac{N(z_2)}{2} < N(z)$

T.o., $\mathbb{Z}[\,i\,]$ – ЕК

Чтобы найти q : $\left|\frac{z_1}{z_2} - q\right| \leqslant \frac{1}{2}$, для $\frac{z_1}{z_2} = z = x + iy$, $x, y \in \mathbb{R}$,

рассмотрим x_1 – ближайшее к x целое число,
y_1 – ближайшее к y целое число,

тогда $\begin{cases} x = x_1 + x_2, \text{ где } x_1 \in \mathbb{Z}, \ |x_2| \leqslant \frac{1}{2} \\ y = y_1 + y_2, \text{ где } y_1 \in \mathbb{Z}, \ |y_2| \leqslant \frac{1}{2} \end{cases}$

$\frac{z_1}{z_2} = (x_1 + iy_1) + (x_2 + iy_2)$

Положим $q = x_1 + iy_1 \Rightarrow \frac{z_1}{z_2} - q = x_2 + iy_2 \Rightarrow$

$\Rightarrow \left|\frac{z_1}{z_2} - q\right|^2 = |x_2 + iy_2|^2 = x_2^2 + y_2^2 = |x_2|^2 + |y_2|^2 \leqslant \frac{1}{4} + \frac{1}{4} \leqslant \frac{1}{2}$

Пример: Разделим $z_1 = 1 - 3i \in \mathbb{Z}[\,i\,]$ на $z_2 = 3 - 2i$ с остатком.

$\frac{z_1}{z_2} = \frac{1 - 3i}{3 - 2i} = \frac{(1 - 3i)(3 + 2i)}{13} = \frac{9}{13} - i\frac{7}{13} =$

$= \left(1 - \frac{4}{13}\right) + i\left(-1 + \frac{6}{13}\right) = (1 - i) + \left(-\frac{4}{13} + i\frac{6}{13}\right)$

$\begin{cases} q = 1 - i \\ r = z_1 - qz_2 = 1 - 3i - (1 - i)(3 - 2i) = 1 - 3i - (1 - 5i) = 2i \end{cases}$

$z_2 = qz_1 + r$

$1 - 3i = (1 - i)(3 - 2i) + 2i$

3 Наибольший общий делитель

Вспомним

Опр. Пусть A - ЦК. Наибольшим общим делителем $a, b \in A$ НОД $\{a, b\} = (a, b)$ называется общий делитель a и b, который делится на любой их общий делитель.

Пример.

В ЦК 2 элемента могут не иметь наибольшего общего делителя.

Рассмотрим M - множество многочленов над $\mathbb{R}$, в которых отсутствуют члены первой степени

$M = \{a_0 + a_2x^2 + ... + a_nx^n : a_i \in \mathbb{R} \;\; i = 0, 2, 3...\} \subset \mathbb{R}[x]$.

Легко доказать, что M - ЦК.

$x^5, x^6 \in M$. Найдём НОД $\{x^5, x^6\}$ в M.

Общие делители x^5, x^6 в $\mathbb{R}[x] : 1, x, x^2, x^3, z^4, x^5, x^6 \in \mathbb{R}[x]$.

Общие делители x^5, x^6 в $M : 1, x^2, x^3$.

(поскольку $x \not\in M, \;\; x^5$ не делится на $x^4, \;\; x^6$ не делится на x^5).

Ни один из общих делителей x^5, x^6 в M не делится в M на все их общие делители $\Rightarrow \;\nexists$ НОД $\{x^5, x^6\}$ в M.

Нам известна

Теорема 1.

Если A - ЕК, то $\forall\, a, b \in A \;\; \exists\, (a, b)$ и $(a, b) = au + bv$, где $u, v \in A$.

В ЕК можно найти (a, b) с помощью алгоритма Евклида.

Пример. Найдём $(z_1, z_2) = (1 - 3i, 3 - 2i)$ в $\mathbb{Z}[\,i\,]$.

$\dfrac{z_1}{z_2} = q_1z_2 + r_1, \;\; q_1 = 1 - i, \;\; r_1 = 2i$ (см. пример, разобранный выше)

$\dfrac{z_2}{r_1} = \dfrac{3 - 2i}{2i} = -1 - \dfrac{3}{2}i = (-1 - i) - \dfrac{1}{2}i, \;\; q_2 = -1 - i,$

$r_2 = z_2 - q_2r_1 = 3 - 2i - (-1 - i)2i = 3 - 2i + 2i - 2 = 1$

$\dfrac{r_1}{r_2} = \dfrac{2i}{1} = 2i \in \mathbb{Z}[\,i\,], \;\; q_3 = 2i, \;\; r_3 = 0 \Rightarrow$

$\Rightarrow (1 - 3i, 3 - 2i) = 1$, т.е. $1 - 3i, \;\; 3 - 2i$ - взаимно простые целые гауссовы числа.

Заметим, что частное и остаток задаются в $\mathbb{Z}[\,i\,]$ неоднозначно. Например, разделить z_2 на r_1 с остатком можно так:

$$\frac{z_1}{r_1} = -1 - \frac{3}{2}i = -1 + \left(-2 + \frac{1}{2}\right)i = -1 - 2i + \frac{1}{2}i, \quad q_2' = -1 - 2i$$

$$r_2' = z_2 - q_2' r_1 = 3 - 2i - (-1 - 2i)2i = 3 - 2i - (-2i + 4) = -1$$

$$\frac{r_1}{r_2'} = \frac{2i}{-1} = -2i \in \mathbb{Z}[\,i\,], \;\; q_3' = -2i, \;\; r_3' = 0 \Rightarrow (1 - 3i, 3 - 2i) = -1 \sim 1$$

(НОД определён однозначно с точностью до ассоциированности, т.е. умножения на обратимый элемент)

4 Идеалы кольца

Опр. Подмножество $I \subset A$ кольца A, являющееся подгруппой аддитивной группы кольца $(A, +)$, называется левым идеалом кольца A, если $\forall x \in I \quad \forall a \in A \quad ax \in I$, т.е. $AI \subset I$,
правым идеалом кольца A, если
$\forall x \in I \quad \forall a \in A \quad xa \in I$, т.е. $IA \subset I$,
двусторонним идеалом кольца A, если $\begin{cases} AI \subset I \\ IA \subset I \end{cases}$

Для двусторонних идеалов используется обозначение $I \lhd A$

В случае коммутативного кольца A употребляется просто термин "идеал", т.к. в силу коммутативности понятия левого, правого и двустороннего идеала совпадают.

В любом кольце A есть два несобственных двусторонних идеала : $I_1 = \{\overline{0}\} \lhd A$ и $I_2 = A \lhd A$. Другие двусторонние идеалы называют собственными.

Примеры:

1) $M^j = \{A \in \mathfrak{g}l(n, \mathbb{R}) : A^i = 0 \text{ при } i \neq j, \; i = \overline{1, n}\}$ - множество матриц, в которых все столбцы, кроме A^j, нулевые.
M^j - левый идеал в $\mathfrak{g}l(n, \mathbb{R})$.

2) $M_i = \{A \in \mathfrak{g}l(n,\mathbb{R}) : A_j = 0 \text{ при } i \neq j,\ j = \overline{1,n}\}$ - множество матриц, в которых все строки, кроме A_i, нулевые.
M_i - правый идеал в $\mathfrak{g}l(n,\mathbb{R})$.

3) В $\mathfrak{g}l(n,\mathbb{R})$ нет собственных двусторонних идеалов.
Пусть $I \lhd \mathfrak{g}l(n,\mathbb{R}),\ \ I \neq \{\overline{0}\} \Rightarrow\ \exists\, A \in I : A \neq \overline{0}$.
Пусть $a_{ij} \neq 0 \Rightarrow E_{ki}AE_{jk} = (a_{ij}E_{kk}) \in I\ \ \forall\, k = \overline{1,n} \Rightarrow$
$\Rightarrow \sum\limits_{k=1}^{n}(a_{ij}E_{kk}) = (a_{ij}E) \in I \Rightarrow (a_{ij}^{-1}E)(a_{ij}E) \in I \Rightarrow E \in I \Rightarrow$
$\Rightarrow \forall\, B \in \mathfrak{g}l(n,\mathbb{R})\ BE = B \in I \Rightarrow I = \mathfrak{g}l(n,\mathbb{R})$.

Утв. 1. Если A - КАК1, $x_1, x_2, ..., x_m \in A$,
$(x_1, x_2, ..., x_m) = \{a_1x_1 + a_2x_2 + ... + a_mx_m : a_i \in A,\ i = \overline{1,m}\}$,
то $(x_1, x_2, ..., x_m) \lhd A$.

Док-во:
Очевидно, $(x_1, x_2, ..., x_m) < (A, +)$ - аддитивная подгруппа A
и $\forall\, a \in A\ \ a(\sum\limits_{i=1}^{m} a_ix_i) = \sum\limits_{i=1}^{m} aa_ix_i \in (x_1, x_2, ..., x_m)$.

Утв. 2. Если A - КАК1, $x_1, x_2, ..., x_m \in A$,
то $(x_1, x_2, ..., x_m) \lhd A$ - наименьший по включению идеал A, содержащий $x_1, x_2, ..., x_m$.

Док-во:
Пусть $I \lhd A : x_1, x_2, ..., x_m \in I \Rightarrow$
$\Rightarrow \sum\limits_{i=1}^{m} a_ix_i \in I\ \ \forall\, a_i \in A\ \ i = \overline{1,m} \Rightarrow (x_1, x_2, ..., x_m) \subset I$.

Опр. Пусть $A -$ КАК1, $x_1, x_2, ..., x_m \in A$.
Идеал $(x_1, x_2, ..., x_m) \lhd A$ называется идеалом в A, порождённым элементами $x_1, x_2, ..., x_m$.
Идеал $(x) = xA \lhd A$, порождённый одним элементом $x \in A$, называется главным идеалом.

Примеры:
1) В $\mathbb{Z}$ любая аддитивная подгруппа является циклической, имеет вид

$< m >= m\mathbb{Z}$ и является главным идеалом (m), порожденным элементом m.

2) В $\mathbb{Z}_n$ любая аддитивная подгруппа является циклической, имеет вид $< \overline{m} >= \overline{m}\mathbb{Z}_n$ и является главным идеалом (m), порожденным элементом $\overline{m}$, т.к $\overline{m}\overline{k} = \underbrace{\overline{m} + \overline{m} + ... + \overline{m}}_{k \text{ раз}} \in < \overline{m} >$

Утв. 3.

Если A - кольцо с 1, $I \lhd A$ и $\exists\, a \in I : a \in A^*(a \in I \cap A^*) \Rightarrow I = A$.

Док-во:

Пусть $a \in I \cap A^* \Rightarrow aa^{-1} = 1 \in I \Rightarrow \forall\, b \in A \;\; b1 = b \in I \Rightarrow A = I$.

Теорема 2.

$A -$ КАК1, содержащее более одного элемента, является полем.

$$\Updownarrow$$

A не имеет собственных идеалов.

Док-во:

$\Downarrow$Пусть A - поле, $I \lhd A : I \neq \{\overline{0}\} \Rightarrow$

$\Rightarrow \exists\, a \in I : a \neq \overline{0} \Rightarrow a \in A^* \Rightarrow I = A$.

$\Uparrow$Пусть A не имеет собственных идеалов $\Rightarrow$

$\Rightarrow \forall\, a \in A \diagdown \{\overline{0}\} \Rightarrow (a) \lhd A$ - несобственный идеал,

но $(a) \neq \{\overline{0}\} \Rightarrow (a) = A \Rightarrow$

$\Rightarrow 1 \in (a) \Rightarrow \exists\, b \in A : 1 = ab \Rightarrow b = a^{-1} \in A \Rightarrow A$ - поле.

Лекция №8

1 Максимальный идеал кольца

Опр. Собственный идеал I кольца $A \quad I \lhd A$ называется максимальным идеалом, если он не содержится ни в каком другом собственном идеале кольца A, т.е.

$$\begin{cases} I,\ I' \lhd A \\ I \subset I' \end{cases} \Rightarrow \left[\begin{array}{l} I' = I \\ I' = A \end{array} \right.$$

Утв. 1. Пусть A – KAK 1.

Если любой идеал A является главным, то в A не существует бесконечной цепочки строго возврастающих идеалов:

$I_1 \subset I_2 \subset ... \subset I_k \subset ...$, где $I_k \lhd A,\ I_k \neq I_{k+1}, \quad \forall k \in \mathbb{N}$

Док-во:

Пусть $I_1 \subset I_2 \subset ... \subset I_k \subset ...-$ такая цепочка, $I_k \neq I_{k+1}$

Рассмотрим $I = \bigcup\limits_{j=1}^{\infty} I_j$ и заметим, что

1) $\overline{0} \in I_1 \subset I \Rightarrow \overline{0} \in I$,

2) $a, b \in I \Rightarrow \exists j \in \mathbb{N} : a, b \in I_j \Rightarrow a + b \in I_j \subset I \Rightarrow a + b \in I$,

3) $a \in I \Rightarrow \exists j \in \mathbb{N} : a \in I_j \Rightarrow (-a) \in I_j \subset I \Rightarrow (-a) \in I$,

4) $a \in I,\ b \in A \Rightarrow \exists j \in \mathbb{N} : a \in I_j \Rightarrow ab \in I_j \subset I \Rightarrow ab \in I$.

$1), 2), 3), 4) \Rightarrow I \lhd A$.

Поскольку $A -$ КГИ, $\exists a \in A : I = (a) \Rightarrow \exists k \in \mathbb{N} : a \in I_k \Rightarrow$

$\Rightarrow (a) \subset I_k \subset I = (a) \Rightarrow I_k = (a) \Rightarrow (a) = I_k \subset I_{k+1} \subset I = (a) \Rightarrow$

$\Rightarrow I_{k+1} = (a) \Rightarrow I_k = I_{k+1}$ ⚔

Следствие. Пусть A – KAK 1. Если любой идеал A является главным, то любой собственный идеал содержится в некотором максимальном идеале.

Пример.

Все собственные идеалы $\mathbb{Z}_{20}$: $(2),\ (4)\ , (5),\ (10)$,

причем $(4) \subset (2), (10) \subset (2), (10) \subset (5)$.

Идеалы (2) и (5) являются максимальными.

2 Кольцо главных идеалов

Опр. Кольцо A называется кольцом главных идеалов (КГИ), если
1) A - ЦК,
2) любой идеал в A является главным.

Примеры:
1) $\mathbb{Z}$ - КГИ.
2) Если n не является простым числом, то $\mathbb{Z}_n$ не является КГИ, т.к. хотя любой идеал в этом кольце является главным, $\mathbb{Z}_n$ содержит делители нуля.
(В случае простого n $\mathbb{Z}_n$ является полем)
3) $\mathbb{Z}[x]$ не является КГИ, т.к. хотя $\mathbb{Z}[x]$ - ЦК, но не все идеалы $\mathbb{Z}[x]$ главные.

Докажем, что идеал $(2, x)$ не является главным от противного.
Пусть $(2, x) = (p(x)),\ \ p(x) \in \mathbb{Z}[x] \Rightarrow$

$$\Rightarrow \begin{cases} 2 = p(x)q_1(x) \Rightarrow deg\, p(x) = 0,\ deg\, q_1(x) = 0 \\ \qquad\qquad\qquad\quad \Downarrow \\ x = p(x)q_2(x) \Rightarrow deg\, q_2(x) = 1 \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} p(x) = c \neq 0 \\ q_2(x) = ax + b,\ \ a \neq 0 \end{cases} \Rightarrow x = c(ax + b)\ (*)$$

Положим в $(*)$ $x = 0 \Rightarrow 0 = cb \Rightarrow b = 0 \Rightarrow x = cax \Rightarrow 1 = ca \Rightarrow$
$\Rightarrow 1 \in (c) = (p(x)) = (2, x) \Rightarrow$
$\Rightarrow \exists\ g_1(x),\ g_2(x) \in \mathbb{Z}[x] : 1 = 2g_1(0) + xg_2(x)\ \ (**)$
Положим в $(**)$ $x = 0 \Rightarrow 1 = 2g_1(0) \Rightarrow 2 \in \mathbb{Z}^*$ ⚔

Теорема 1. Евклидово кольцо является кольцом главных идеалов.
A - ЕК $\Rightarrow$ A - КГИ

Док-во:
1) A - ЕК $\Rightarrow$ A - ЦК
2) Докажем, что $\forall I \lhd A$ является главным.
Если $I = \{\overline{0}\}$, то $I = (\overline{0})$ является главным.
Если $I \neq \{\overline{0}\}$, рассмотрим $b \in I \setminus \{\overline{0}\} : N(b) \leqslant N(c) \quad \forall c \in I \setminus \{\overline{0}\}$.

$\forall a \in I \quad \exists q, r \in A : a = qb + r$, где $\left[\begin{array}{l} r = \overline{0} \\ N(r) < N(b) \end{array} \right.$,
но $r = a - qb \in I \Rightarrow N(r) < N(b)$ невозможно $\Rightarrow r = \overline{0} \Rightarrow a = qb \Rightarrow$
$\Rightarrow I = (b) -$ главный идеал.

Пример.
1) $\mathbb{Z} -$ ЕК $\Rightarrow \mathbb{Z} -$ КГИ
2) $K -$ поле $\Rightarrow K[x] -$ ЕК $\Rightarrow K[x] -$ КГИ
3) $\mathbb{Z}[i] -$ ЕК $\Rightarrow \mathbb{Z}[i] -$ КГИ

3 Делимость в ЦК в терминах главных идеалов

Утв. 2. Если $A -$ ЦК, $a, b \in A$, то $b|a \Leftrightarrow (a) \subset (b)$

Док-во:
$\Rightarrow$ $b|a \Rightarrow \exists c \in (A) : a = bc \Rightarrow a \in (b) \Rightarrow (a) \subset (b)$
$\Leftarrow$ $(a) \subset (b) \Rightarrow a \in (b) \Rightarrow \exists \in A : a = bc$

Утв. 3. Если $A -$ ЦК, $a, b \in A$, то $a \sim b \Leftrightarrow (a) = (b)$

Док-во:
$$a \sim b \Leftrightarrow \exists q \in A^* : a = qb \Leftrightarrow \left\{ \begin{array}{l} a|b \\ b|a \end{array} \right. \Leftrightarrow (a) = (b)$$

4 Простые элементы в КГИ

Утв. 4. Если $A -$ КГИ, $a \in A$, то $a -$ простой элемент А $\Leftrightarrow$
$\Leftrightarrow (a) -$ максимальный идеал A

Док-во:
$\Rightarrow$ Пусть $a -$ простой элемент, но (a) не является максимальным идеалом,
т.е. $\exists (b) \lhd A : \left\{ \begin{array}{l} (b) \neq A \\ (b) \neq (a) \end{array} \right.$, $(a) \subset (b) \Rightarrow$
$\Rightarrow \exists\, c \in A : a = bc$, причём $\left\{ \begin{array}{l} b \not\in A^* \text{ (иначе } (b) = A) \\ c \not\in A^* \text{ (иначе } (b) = (a)) \end{array} \right. \Rightarrow$
$\Rightarrow a$ не является простым $\lightning$

$\Leftarrow$ Пусть (a) - максимальный идеал, но a не является простым,
т.е. $\exists\, b, c \in A : a = bc,\ b, c \not\in A^* \Rightarrow$
$\Rightarrow (a) \subset (b)$, причём $\begin{cases} (b) \neq A = (1), \text{ т.к. } b \nsim 1 \\ (b) \neq (a), \text{ т.к. } b \nsim a \end{cases} \Rightarrow$
$\Rightarrow (a)$ не является максимальным идеалом $\lightning$

5 Наибольший общий делитель в КГИ

В КГИ верна Теорема 2, аналогичная Теореме 1 лекции 7.

Теорема 2.
Если A - КГИ, то $\forall\, a, b \in A\ \ \exists$ НОД$\{a, b\} = (a, b)$
и $(a, b) = au + bv$, где $u, v \in A$.

Док-во:
Рассмотрим идеал $(a, b) = \{ax + by : x, y \in A\}$,
он является главным $\Rightarrow \exists\, d \in A : (a, b) = (d) \Rightarrow$
$\Rightarrow d \in (a, b) \Rightarrow \exists u, v \in A : d = au + bv\ \ (*)$.
$d =$НОД$\{a, b\}$, т.к. $\begin{array}{l} (a) \subset (a, b) = (d) \Rightarrow d \,|\, a, \\ (b) \subset (a, b) = (d) \Rightarrow d \,|\, b, \end{array}$
и если d' - общий делитель a и b, то из $(*) \Rightarrow d' \,|\, d$.

Note. В КГИ одно и то же обозначение (a, b) для идеала, порождённого элементами a и b, и для НОД$\{a, b\}$, который порождает тот же самый идеал, является обоснованным.

6 Факториальность кольца главных идеалов

Теорема 2. КГИ является факториальным кольцом,
т.е. если A - КГИ, то $\forall\, a \in A \setminus (A^* \cup \{\overline{0}\})$ можно разложить на простые множители $a = p_1 p_2 ... p_n$, где p_i - простой элемент A, $\ i = \overline{1, n}$,
причём это разложение единственно с точностью до ассоциированности.

Док-во:
1) $\exists$ разложения $\forall a \in A \setminus (A^* \cup \{\overline{0}\})$ на простые множители докажем от

противного.

Пусть $\exists\, a_0 \in A^{\diagdown}(A^* \cup \{\overline{0}\}) : a_0$ нельзя разложить на простые множители. Назовём такие элементы плохими.

$a_0 -$ плохой элемент $\Rightarrow$ он не простой $\Rightarrow a_0 = a_1 b_1, \quad a_1, b_1 \notin A^*$

Если $a_1, b_1 -$ хорошие элементы $\Rightarrow a_0 -$ хороший. $\Rightarrow$

$\Rightarrow$ Хотя бы один из $a_1, b_1 -$ плохой. Пусть $a_1 -$ плохой.

$(a_0) \subset (a_1) -$ цепочка строго возрастающих идеалов.

$a_1 = a_2 b_2, \;\; a_2, b_2 \notin A^*$. Если $a_2, b_2 -$ хорошие, то $a_1 -$ хороший. $\Rightarrow$

$\Rightarrow$ Хотя бы один из $a_2, b_2 -$ плохой. Пусть $a_2 -$ плохой.

$(a_0) \subset (a_1) \subset (a_2) -$ цепочка строго возрастающих идеалов.

Продолжая аналогичные рассуждения, получим

$(a_0) \subset (a_1) \subset ... \subset (a_k) \subset ... -$

бесконечную цепочку строго возрастающих идеалов в КГИ. $\Rightarrow$

2) доказательство единственности разложения на простые множители в КГИ идентично доказательству единственности разложения на простые множители в ЕК (см. 2-ую Лекцию 3-его семестра)

Примеры.

1) $\mathbb{Z} -$ факториальное кольцо.

2) $K -$ поле $\Rightarrow K[x] -$ факториальное кольцо

(Напомним, что простые элементы кольца многочленов называются неприводимыми многочленами)

3) $\mathbb{Z}[i] -$ факториальное кольцо.

Разберём пример разложения на простые множители в $\mathbb{Z}[\,i\,]$

$(\mathbb{Z}[\,i\,])^* = \{1, -1, i, -i\}, \;\; z \in (\mathbb{Z}[\,i\,])^* \Leftrightarrow N(z) = 1$

Рассмотрим $2 \in \mathbb{Z}[\,i\,]$.

$2 = (1+i)(1-i), \;\; 1+i \notin (\mathbb{Z}[\,i\,])^*, \;\; 1-i \notin (\mathbb{Z}[\,i\,])^* \Rightarrow$

$\Rightarrow$ 2 не является простым элементом $\mathbb{Z}[\,i\,]$.

Докажем, что $1+i$ является простым элементом в $\mathbb{Z}[\,i\,]$.

Пусть $1+i = z_1 z_2 \Rightarrow N(1+i) = N(z_1)N(z_2) \Rightarrow$

$$\Rightarrow 2 = N(z_1)N(z_2) \Rightarrow \left[\begin{array}{l} \left\{ \begin{array}{l} N(z_1) = 1 \\ N(z_2) = 2 \end{array} \right. \Leftrightarrow z_1 \in (\mathbb{Z}[\,i\,])^* \\ \left\{ \begin{array}{l} N(z_1) = 2 \\ N(z_2) = 1 \end{array} \right. \Leftrightarrow z_2 \in (\mathbb{Z}[\,i\,])^* \end{array} \right.$$

Аналогично доказывается, что $1-i$ является простым элементом в $\mathbb{Z}[\,i\,]$. Следовательно, $2 = (1+i)(1-i)$ является разложением $2 \in \mathbb{Z}[\,i\,]$ на простые множители.

$2 = (-1-i)(-1+i)$ - такое же с точностью до ассоциированности разложение.

4) $\mathbb{Z}[\sqrt{-3}] = \{a + i\sqrt{3}b : a, b \in \mathbb{Z}\}$ не является факториальным кольцом.

Покажем, что в этом кольце разложение на простые множители неоднозначно.

$z = a + i\sqrt{3}b \Rightarrow |z|^2 = a^2 + 3b^2 \in \mathbb{Z}_+$

$$z = a + i\sqrt{3}b \in (\mathbb{Z}[\sqrt{-3}])^* \Leftrightarrow zz^{-1} = 1 \Leftrightarrow \left\{ \begin{array}{l} |z|^2|z^{-1}|^2 = 1 \\ |z| \in \mathbb{Z}_+ \end{array} \right. \Leftrightarrow$$

$$\Leftrightarrow |z|^2 = 1 \Leftrightarrow a^2 + 3b^2 = 1 \Leftrightarrow \left\{ \begin{array}{l} a = \pm 1 \\ b = 0 \end{array} \right. \Leftrightarrow z = \pm 1,$$

т.е. $(\mathbb{Z}[\sqrt{-3}])^* = \{\pm 1\}$

Рассмотрим $4 \in \mathbb{Z}[\sqrt{-3}]$

4 не является простым элементом $\mathbb{Z}[\sqrt{-3}]$, поскольку

$4 = 2 \cdot 2$ $(*)$ и $4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ $(**)$.

$(*)$ - разложение $4 \in \mathbb{Z}[\sqrt{-3}]$ на простые множители.

2 - простой элемент, т.к. если $2 = z_1 z_2 \Rightarrow |2|^2 = |z_1|^2 = |z_1|^2|z_2|^2 \Leftrightarrow$

$$\Leftrightarrow 4 = |z_1|^2|z_2|^2 \Leftrightarrow \left[\begin{array}{l} \left\{ \begin{array}{l} |z_1|^2 = 2 \Leftrightarrow a_1^2 + 3b_1^2 = 2 \text{ невозможно} \\ |z_2|^2 = 2 \Leftrightarrow a_2^2 + 3b_2^2 = 2 \text{ невозможно} \end{array} \right. \\ \left\{ \begin{array}{l} |z_1|^2 = 1 \\ |z_2|^2 = 4 \end{array} \right. \\ \left\{ \begin{array}{l} |z_1|^2 = 4 \\ |z_2|^2 = 1 \end{array} \right. \end{array} \right. \Rightarrow$$

$$\Rightarrow \left[\begin{array}{l} z_1 \in (\mathbb{Z}[\sqrt{-3}])^* \\ z_2 \in (\mathbb{Z}[\sqrt{-3}])^* \end{array} \right. .$$

$(**)$ – также разложение $4 \in \mathbb{Z}[\sqrt{-3}]$ на простые множители
$1 + i\sqrt{3}$ – простой элемент, т.к. если $1 + i\sqrt{3} = z_1 z_2 \Rightarrow$

$$\Rightarrow |1 + i\sqrt{3}|^2 = |z_1|^2 |z_2|^2 \Leftrightarrow 4 = |z_1|^2 |z_2|^2 \Rightarrow \left[\begin{array}{l} z_1 \in (\mathbb{Z}[\sqrt{-3}])^* \\ z_2 \in (\mathbb{Z}[\sqrt{-3}])^* \end{array} \right. ,$$

как мы видели выше.
Аналогично доказывается, что $1 - i\sqrt{3}$ – простой элемент.
$\begin{cases} 1 + i\sqrt{3} \nsim 2 \\ 1 - i\sqrt{3} \nsim 2 \end{cases}$ в кольце $\mathbb{Z}[\sqrt{-3}] \Rightarrow$
$\Rightarrow (*)$ и $(**)$ – два различных разложения $4 \in \mathbb{Z}[\sqrt{-3}]$ на простые множители. $\Rightarrow \mathbb{Z}[\sqrt{-3}]$ не является факториальным кольцом $\Rightarrow$
$\Rightarrow \mathbb{Z}[\sqrt{-3}]$ не является КГИ $\Rightarrow$
$\Rightarrow \mathbb{Z}[\sqrt{-3}]$ не является ЕК.

Лекция №9

1 Факторкольцо

Если A – кольцо, $I < A$ – его аддитивная подгруппа $\Rightarrow$
$\Rightarrow (I,+)$ – нормальная подгруппа $(A,+)$.

$a_1 \equiv a_2 (mod\ I) \Leftrightarrow a_2 - a_1 \in I$

Определено сложение смежных классов:

$(a+I)+(b+I) = (a+b)+I \Rightarrow ({}^{A}/_{I}\ ,+)$ – факторгруппа

${}^{A}/_{I}$ превратится в кольцо, если ввести операцию умножения смежных классов : $(a+I)(b+I) = ab+I$.

Это можно сделать корректно $\Leftrightarrow$ умножение в A согласовано с отношением эквивалентности по $mod\ I$,

т.е. $\begin{cases} a_1 \equiv a_2 (mod\ I) \\ b_1 \equiv b_2 (mod\ I) \end{cases} \Rightarrow a_1 b_1 = a_2 b_2 (mod\ I)$

Утв. 1. Умножение в кольце A согласовано с отношением эквивалентности по $mod\ I \Leftrightarrow I \lhd A$ – двусторонний идеал A.

Док-во:

$\Rightarrow$ Пусть умножение согласовано с отношением эквивалентности по $mod\ I$.

$x \in I \Leftrightarrow x \equiv \overline{0} (mod\ I) \Rightarrow \forall a \in A \ \ ax = a0 (mod\ I)$, т.к. $a \equiv a (mod\ I) \Rightarrow$
$\Rightarrow \forall a \in A \ \ ax \equiv 0 (mod\ I) \Leftrightarrow \forall a \in A \ \ ax \in I \Rightarrow I$ – левый идеал A

Аналогично, I – правый идеал A.

Следовательно, $I \lhd A$.

$\Leftarrow$ Пусть $I \lhd A$

Если $\begin{cases} a_1 \equiv a_2 (mod\ I) \\ b_1 \equiv b_2 (mod\ I) \end{cases}$, т.е. $\begin{cases} a_2 = a_1 + x, \text{ где } x \in I \\ b_2 = b_1 + y, \text{ где } y \in I \end{cases}$, то

$a_2 b_2 = (a_1 + x)(b_1 + y) = a_1 b_1 + x b_1 + a_1 y + xy \Rightarrow$
$\Rightarrow a_2 b_2 - a_1 b_1 = x b_1 + a_1 y + xy \in I \ \ \forall x, y \in I, \ \ \forall a, b \in A$, т.к. $I \lhd A \Rightarrow$
$\Rightarrow a_1 b_1 \equiv a_2 b_2 (mod\ I)$.

Утв. 2. Пусть A – кольцо, $I \lhd A$ – его двусторонний идеал, на A/I определены операции сложения и умножения

$$(*)\begin{cases}(a+I)+(b+I)=(a+b)+I \in A/I \\ (a+I)(b+I)=ab+I \in A/I\end{cases} \qquad \forall (a+I),(b+I) \in A/I,$$

тогда A/I с этими операциями является кольцом.

Док-во:

$(A/I,+)$ - группа по сложению.

Проверим дистрибутивность в A/I.

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

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

При перестановке сомножителей дистрибутивность проверяется аналогично.

Опр. Если A - кольцо, $I \lhd A$ - его двусторонний идеал, то кольцо A/I с операциями, определяемыми $(*)$, называется факторкольцом кольца A по идеалу I.

Пример.

$\forall (m) = m\mathbb{Z} \lhd \mathbb{Z} \quad \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/(m) = \mathbb{Z}_m$ - кольцо вычетов по модулю m.

Note. Пусть A - кольцо, $I \lhd A$. Тогда

A - ассоциативное кольцо $\Rightarrow A/I$ - ассоциативное кольцо,

A - коммутативное кольцо $\Rightarrow A/I$ - коммутативное кольцо,

A - кольцо с единицей $1 \Rightarrow A/I$ - кольцо с единицей $(1+I)$.

2 Критерии того, что факторкольцо является полем

Лемма 1.

Пусть A - кольцо, $I \lhd A$, $I \subset I' \lhd A$, тогда $I'/I \lhd A/I$.

Док-во:

$I \lhd A,\ I \subset I' \lhd A \Rightarrow I \lhd I',\ I'/I \subset A/I$

$a+I \in I'/I \Leftrightarrow\ a \in I'$

1) $0 + I \in {}^{I'}/_{I}$,
2) $(a + I),\ (b + I) \in {}^{I'}/_{I} \Rightarrow\ a, b \in I'\ \Rightarrow\ a + b \in I' \Rightarrow$
$\Rightarrow (a + I) + (b + I) = (a + b) + I \in {}^{I'}/_{I}$,
3) $a + I \in {}^{I'}/_{I} \Rightarrow\ a \in I'\ \Rightarrow\ (-a) \in I'\ \Rightarrow\ -(a + I) = (-a) + I \in {}^{I'}/_{I}$,
4) $b + I \in {}^{A}/_{I},\ a + I \in {}^{I'}/_{I} \Rightarrow\ b \in A,\ a \in I'\ \Rightarrow\ ba \in I' \Rightarrow$
$\Rightarrow (b + I)(a + I) = ba + I \in {}^{I'}/_{I}$,
аналогично, $(a + I)(b + I) \in {}^{I'}/_{I}$.
1), 2), 3), 4) $\Rightarrow {}^{I'}/_{I} \lhd {}^{A}/_{I}$.

Пример.
$(20) \subset (10) \subset \mathbb{Z},\ {}^{\mathbb{Z}}/_{(20)} = \mathbb{Z}_{20},\ {}^{(10)}/_{(20)} = (\overline{10}) \lhd \mathbb{Z}_{20}$.

Лемма 2. Пусть A – кольцо, $I_1, I_2 \lhd A$, тогда
$I_1 + I_2 = \{a_1 + a_2 : a_1 \in I_1,\ a_2 \in I_2\} \lhd A$
Док-во:
1) $\overline{0} = \overline{0} + \overline{0} \in I_1 + I_2$
2) $a_1 + a_2,\ b_1 + b_2 \in I_1 + I_2,\ \ a_1, b_1 \in I_1,\ \ a_2, b_2 \in I_2 \Rightarrow$
$\Rightarrow (a_1 + a_2) + (b_1 + b_2) = (a_1 + b_1) + (a_2 + b_2) \in I_1 + I_2$
3) $a_1 + a_2 \in I_1 + I_2,\ a_1 \in I_1,\ a_2 \in I_2 \Rightarrow -(a_1 + a_2) = (-a_1) + (-a_2) \in I_1 + I_2$
4) $b \in A,\ a_1 + a_2 \in I_1 + I_2,\ a_1 \in I_1,\ a_2 \in I_2 \Rightarrow b(a_1 + a_2) = ba_1 + ba_2 \in I_1 + I_2$,
аналогично, $(a_1 + a_2)b \in I_1 + I_2$
$1), 2), 3), 4) \Rightarrow I_1 + I_2 \lhd A$

Теорема 1. Если $A\ - KAK1,\ I \lhd A$ – собственный идеал, то ${}^{A}/_{I}$ - поле $\Leftrightarrow I$ – максимальный идеал A.
Док-во:
$\Leftarrow$ Пусть ${}^{A}/_{I}$ - поле и $I \subset I' \lhd A :\ I' \neq A \Rightarrow\ {}^{I'}/_{I} \lhd {}^{A}/_{I} : {}^{I'}/_{I} \neq {}^{A}/_{I}$
В поле ${}^{A}/_{I}$ нет собственных идеалов $\Rightarrow {}^{I'}/_{I} = \{\overline{0} + I\} \Leftrightarrow I' = I \Rightarrow$
$\Rightarrow I$ – максимальный идеал A.
$\Rightarrow$ Пусть I – максимальный идеал A, тогда
1) $A\ - KAK1 \Rightarrow {}^{A}/_{I}$ – КАК1
2) I – собственный идеал $\Rightarrow I \neq A \Rightarrow |{}^{A}/_{I}| > 1$

3) $a+I \in {}^{A}/_{I}{}^{\diagdown} \{\overline{0}+I\} \Leftrightarrow a \not\in I \Rightarrow I \subset (a)+I \lhd A$, при этом $I \neq a+I$,
$I -$ максимальный идеал $A \Rightarrow (a)+I = A \Rightarrow 1 \in (a)+I \Rightarrow$
$\Rightarrow 1 = ab+x$, где $b \in A,\ x \in I \Rightarrow 1 \equiv ab(mod\ I) \Rightarrow$
$\Rightarrow ab+I = 1+I$, т.е. $(a+I)(b+I) = 1+I$, т.е. $(b+I) = (a+I)^{-1} \in {}^{A}/_{I}$
$1), 2), 3) \Rightarrow {}^{A}/_{I}$ - поле.

Теорема 2. Если $A -$ КГИ, $a \in A \diagdown (A^* \cup \{\overline{0}\})$, то
${}^{A}/_{(a)}$ - поле $\Leftrightarrow a$ - простой элемент A.

Док-во:
$a \in A^{\diagdown}(A^* \cup \{\overline{0}\}) \Rightarrow (a) -$ собственный идеал A.
${}^{A}/_{(a)}$ - поле $\Leftrightarrow (a)$ - максимальный идеал.
В КГИ (a) - максимальный идеал $\Leftrightarrow a$ - простой элемент A.

Следствие. Если K - поле, $p(x) \in K[x] : deg\, p(x) > 0$, то
${}^{K[x]}/_{(p(x))}$ - поле $\Leftrightarrow$ $p(x)$ - неприводимый многочлен.

3 Нильпотентный радикал кольца

Опр. Пусть A - кольцо, $a \in A$ называется нильпотентным элементом A (нильпотентом), если $\exists\, n \in \mathbb{N} : a^n = \overline{0}$. $\overline{0} \in A$ называется тривиальным нильпотентом.

Опр. Нильпотентным радикалом (нильрадикалом) кольца A называется множество всех его нильпотентов.
$Rad\, A = \{a \in A : \exists\, n_a \in \mathbb{N} : a^{n_a} = \overline{0}\}$.

Утв. 3.
Пусть A - КАК1, тогда $Rad\, A \lhd A$.

Док-во:
1) $\overline{0} \in Rad\, A$.
2) $\begin{cases} a_1 \in Rad\, A, \text{ т.е. } \exists\, n \in \mathbb{N} : a_1^n = \overline{0} \\ a_2 \in Rad\, A, \text{ т.е. } \exists\, m \in \mathbb{N} : a_2^m = \overline{0} \end{cases} \Rightarrow$

$\Rightarrow (a_1+a_2)^{n+m} = \sum\limits_{k=0}^{n+m} C_{n+m}^k a_1^k a_2^{n+m-k} = \overline{0}$, т.к.
при $k = 0, 1, ..., n \;\; a_1^k a_2^{n+m-k} = \overline{0}$, поскольку $a_2^m = \overline{0}$,
при $k = n+1, n+2, ..., n+m \;\; a_1^k a_2^{n+m-k} = \overline{0}$, поскольку $a_1^n = \overline{0} \Rightarrow$
$\Rightarrow a_1 + a_2 \in Rad\, A$.
3) $a \in Rad\, A$, т.е. $\exists\, n \in \mathbb{N} : a^n = \overline{0} \Rightarrow$
$\Rightarrow (-a)^n = (-1)^n a^n = \overline{0} \Rightarrow (-a) \in Rad\, A$.
4) $b \in A, \;\; a \in Rad\, A$, т.е. $\exists\, n \in \mathbb{N} : a^n = \overline{0} \Rightarrow$
$\Rightarrow (ba)^n = b^n a^n = \overline{0} \Rightarrow ba \in A$.
1), 2), 3), 4) $\Rightarrow Rad\, A \lhd A$.

Утв. 4. Пусть A - КАК1, тогда ${}^{A}/_{Rad\, A}$ - кольцо, в котором нет нетривиальных нильпотентов.

Док-во:
Пусть $a + Rad\, A \in {}^{A}/_{Rad\, A}$ и $\exists\, n \in \mathbb{N} : (a + Rad\, A)^n = a^n + Rad\, A =$
$= \overline{0} + Rad\, A \Leftrightarrow a^n \in Rad\, A$, т.е. $\exists\, m \in \mathbb{N} : (a^n)^m = \overline{0} \Leftrightarrow a^{mn} = \overline{0} \Rightarrow$
$\Rightarrow a \in Rad\, A \Rightarrow a + Rad\, A = Rad\, A = \overline{0} + Rad\, A$ - тривиальный нильпотент в ${}^{A}/_{Rad\, A}$.

Утв. 5. Пусть $A -$ КГИ, $b \in A \setminus (A^* \cup \{\overline{0}\})$,
$b = p_1^{k_1} p_2^{k_2} ... p_s^{k_s}$ – разложение b на простые множители,
$p_i \neq p_j$ при $i \neq j, \quad i, j = \overline{1, s}$, тогда $Rad({}^{A}/_{(b)}) = {}^{(p_1 p_2 ... p_s)}/_{(b)}$.

Док-во:
$a + (b) \in Rad({}^{A}/_{(b)}) \Leftrightarrow \exists\, n \in \mathbb{N} : (a+(b))^n = a^n + (b) = 0 + (b)$, т.е. $a^n \in (b)$
1) Если $a + (b) \in Rad({}^{A}/_{(b)}) \Rightarrow a^n \in (b) \subset (p_1 p_2 ... p_s) \Rightarrow a \in (p_1 p_2 ... p_s) \Rightarrow$
$\Rightarrow a + (b) \in {}^{(p_1 p_2 ... p_s)}/_{(b)}$, т.е. $Rad({}^{A}/_{(b)}) \subset {}^{(p_1 p_2 ... p_s)}/_{(b)}$.
2) Если $a + (b) \in {}^{(p_1 p_2 ... p_s)}/_{(b)} \Rightarrow a \in (p_1 p_2 ... p_s) \Rightarrow$
$\Rightarrow \exists\, m = max\{k_1, k_2, ..., k_s\} : a^m \in (p_1^m p_2^m ... p_s^m) \subset (p_1^{k_1} p_2^{k_2} ... p_s^{k_s}) = (b) \Rightarrow$
$\Rightarrow a + (b) \in Rad\, ({}^{A}/_{(b)})$, т.е. ${}^{(p_1 p_2 ... p_s)}/_{(b)} \subset Rad({}^{A}/_{(b)})$.
1),2) $\Rightarrow Rad({}^{A}/_{(b)}) = {}^{(p_1 p_2 ... p_s)}/_{(b)}$.

Пример. Найдём $Rad\, \mathbb{Z}_{20}$. $\quad \mathbb{Z}_{20} = {}^{\mathbb{Z}}/_{(20)}, \;\; 20 = 2^2 \cdot 5$.
$Rad\, \mathbb{Z}_{20} = Rad({}^{\mathbb{Z}}/_{(20)}) = {}^{(2 \cdot 5)}/_{(20)} = {}^{(10)}/_{(20)} = (\overline{10})$.

Лекция №10

1 Гомоморфизм колец

Опр. Отображение колец $f : A \longmapsto B$ называется гомоморфизмом колец, если $\begin{cases} f(a_1 + a_2) = f(a_1) + f(a_2) \\ f(a_1 a_2) = f(a_1) f(a_2) \end{cases} \quad \forall a_1,\ a_2 \in A$

Пример. Пусть $A, B\ - KAK1,\ A \subset B,\ A[x] -$ кольцо многочленов над A,

Рассмотрим $f : A[x] \longmapsto B -$ отображение подстановки:

$b \in B,\ f(p(x)) = p(b) \in B\ \ \forall p(x) \in A[x]$.

$f -$ гомоморфизм, т.к.

$\begin{cases} f(p_1(x) + p_2(x)) = p_1(c) + p_2(c) = f(p_1(x)) + f(p_2(x)) \\ f(p_1(x) p_2(x)) = p_1(c) p_2(c) = f(p_1(x)) f(p_2(x)) \end{cases}$

Note. Гомоморфизм колец $f : A \longmapsto B$ является гомоморфизмом их аддитивных групп $f : (A, +) \longmapsto (B, +)$.

Опр. Образом гомоморфизма колец $f : A \longmapsto B$ называется

$Im\ f = \{b \in B : \exists\ a \in A : f(a) = b\}$

Утв. 1. Пусть $f : A \longmapsto B$ - гомоморфизм колец, тогда $Im\ f -$ подкольцо B.

Док-во:

1) $Im\ f < (B, +) -$ подгруппа аддитивной группы.

2) Пусть $\begin{cases} b_1 \in Im\ f, \text{ т.е } \exists\ a_1 \in A : b_1 = f(a_1) \\ b_2 \in Im\ f, \text{ т.е } \exists\ a_2 \in A : b_2 = f(a_2) \end{cases} \Rightarrow b_1 b_2 = f(a_1) f(a_2) =$

$= f(a_1 a_2) \Rightarrow b_1 b_2 \in Im\ f$

$1), 2) \Rightarrow Im\ f -$ подкольцо B.

Note.

Если $A -$ коммутативное кольцо $\Rightarrow Im\ f -$ коммутативное кольцо.

Если $A -$ ассоциативное кольцо $\Rightarrow Im\ f -$ ассоциативное кольцо.

Опр. Ядром гомоморфизма колец $f : A \longmapsto B$ называется
$Ker\ f = \{a \in A : f(a) = \overline{0} \in B\}$

Утв. 2. Пусть $f : A \longmapsto B$ – гомоморфизм колец, тогда $Ker\ f \lhd A$ – двусторонний идеал A.

Док-во:
1) $Ker\ f < (A, +)$
2) Пусть $c \in A$, $a \in Ker\, f$, т.е. $f(a) = 0 \Rightarrow \begin{cases} f(ca) = f(c)f(a) = f(c)\overline{0} = \overline{0} \\ f(ac) = f(a)f(c) = \overline{0}f(c) = \overline{0} \end{cases} \Rightarrow$
$\begin{cases} ca \in Ker\, f \\ ac \in Ker\, f \end{cases}$
1), 2) $\Rightarrow Ker\, f \lhd A$ - двусторонний идеал A.

Опр. Сюръективный гомоморфизм колец $f : A \to B$ называется эпиморфизмом.
Гомоморфизм $f : A \to B$ является эпиморфизмом $\Leftrightarrow Im\, f = B$.

Опр. Инъективный гомоморфизм $f : A \to B$ называется мономорфизмом.
Гомоморфизм $f : A \to B$ является мономорфизмом $\Leftrightarrow Ker\, f = \{\overline{0}\}$.

Note. Если $f : A \to B$ гомоморфизм колец, A - кольцо с 1_A, то $f(1_A)$ может не быть единицей в кольце B.

Например, $f : \mathbb{Z}_{20} \to \mathbb{Z}_{20} : f(\overline{z}) = \overline{5}\overline{z}\ \ \forall\, \overline{z} \in \mathbb{Z}_{20},\ f(\overline{1}) = \overline{5}$.
$f(\overline{z}_1 + \overline{z}_2) = \overline{5}(\overline{z}_1 + \overline{z}_2) = \overline{5}\overline{z}_1 + \overline{5}\overline{z}_2 = f(\overline{z}_1) + f(\overline{z}_2)$,
$f(\overline{z}_1 \cdot \overline{z}_2) = \overline{5}\overline{z}_1\overline{z}_2 = \overline{25}\overline{z}_1\overline{z}_2 = \overline{5}\overline{z}_1 \cdot \overline{5}\overline{z}_2 = f(\overline{z}_1)f(\overline{z}_2)$

Утв. 3. Если $f : A \to B$ - эпиморфизм колец, A - кольцо с единицей 1_A, то и B - кольцо с единицей $1_B = f(1_A)$.

Док-во:
f - эпиморфизм $\Rightarrow \forall\, b \in B\ \ \exists a \in A : f(a) = b \Rightarrow$
$\Rightarrow \begin{cases} b = f(a) = f(a \cdot 1_A) = f(a)f(1_A) = bf(1_A) \\ b = f(a) = f(1_A \cdot a) = f(1_A)f(a) = f(1_A)b \end{cases} \Rightarrow f(1_A) = 1_B$

Утв. 4. Если $f : A \to B$ гомоморфизм колец и A является полем, то либо f - мономорфизм, т.е. $Ker\, f = \{\overline{0}\}$,
либо f - тривиальный гомоморфизм, т.е. $Ker\, f = A$.

Док-во:
Пусть f не является мономорфизмом, т.е. $Ker\, f \neq \{\overline{0}\}$.
Пусть $a \in Ker\, f$ и $a \neq \overline{0} \Rightarrow \exists\, a^{-1} \in A \Rightarrow$
$\Rightarrow f(1) = f(aa^{-1}) = f(a)f(a^{-1}) = \overline{0}f(a^{-1}) = \overline{0} \Rightarrow$
$\Rightarrow 1 \in Ker\, f \Rightarrow Ker\, f = A$,
т.е. f - тривиальный гомоморфизм.

2 Изоморфизм колец

Опр. Отображение колец $f : A \to B$ называется изоморфизмом, если $\begin{cases} 1)\ f \text{ - гомоморфизм,} \\ 2)\ f \text{ - биекция.} \end{cases}$

Следовательно, f - изоморфизм $\Leftrightarrow \begin{cases} f \text{ - гомоморфизм,} \\ Im\, f = B, \\ Ker\, f = \{\overline{0}\}. \end{cases}$

Опр. Кольца A и B называются изоморфными ($A \simeq B$), если существует изоморфизм $f : A \longmapsto B$. Поля A и B называются изоморфными, если они изоморфны как кольца.

Утв. 5. Если $f : A \longmapsto B -$ изоморфизм колец, то
$\exists\, f^{-1} : B \longmapsto A -$ тоже изоморфизм колец.

Док-во:
1) $f -$ биекция $\Rightarrow \exists\, f^{-1}$,
2) $f^{-1} : (B, +) \longmapsto (A, +) -$ изоморфизм аддитивных групп,
3) $f^{-1}(b_1b_2) = f^{-1}((f \circ f^{-1})(b_1)(f \circ f^{-1})(b_2)) = f^{-1}(f(f^{-1}(b_1))f(f^{-1}(b_2))) =$
$= f^{-1}(f(f^{-1}(b_1)f^{-1}(b_2))) = (f^{-1} \circ f)(f^{-1}(b_1)f^{-1}(b_2)) = f^{-1}(b_1)f^{-1}(b_2)$.
$1), 2), 3) \Rightarrow \exists f^{-1} : B \longmapsto A -$ изоморфизм.

Note.
Изоморфизм колец $A \simeq B$ является отношением эквивалентности.

Утв. 6. Пусть A и B изоморфные кольца ($A \simeq B$) и одно из колец является полем, тогда и второе кольцо является полем.

Док-во:
Пусть $f : A \longmapsto B$ изоморфизм, $A -$ поле, тогда
1) $Im\ f = B\ -\ KAK1$,
2) $|A| > 1 \Rightarrow |B| > 1$,
3) $\forall b \in B \setminus \{\overline{0}_B\}\ \ \exists\ a \in A \setminus \{\overline{0}_A\} : f(a) = b \Rightarrow 1_B = f(1_A) = f(aa^{-1}) =$
$= f(a)f(a^{-1}) = bf(a^{-1}) \Rightarrow \exists b^{-1} = f(a^{-1}) \in B$
$1), 2), 3) \Rightarrow B -$ поле
Если $B -$ поле, то рассмотрим изоморфизм $f^{-1} : B \longmapsto A$ и аналогично получим, что A также является полем.

3 Теорема о гомоморфизме колец

Теорема 1. Пусть $f : A \to B$ - гомоморфизм колец,
тогда $A/_{Ker\ f} \simeq Im\ f$.

Док-во:
Построим отображение $F : A/_{Ker\ f} \to Im\ f : F(a + Ker\ f) = f(a)$.
В теореме о гомоморфизме групп в прошлом семестре было доказано, что 1) F определено корректно,
2) F - изоморфизм аддитивных групп $\big(A/_{Ker\ f}, +\big) \simeq \big(Im\ f, +\big)$.
Остаётся проверить, что F сохраняет операцию умножения
3) $F\big((a_1 + Ker\ f)(a_2 + Ker\ f)\big) = F(a_1a_2 + Ker\ f) = f(a_1a_2) = f(a_1)f(a_2) =$
$= F(a_1 + Ker\ f)F(a_2 + Ker\ f)$.
$1), 2), 3) \Rightarrow F$ - изоморфизм колец.

Примеры:
(1) Пусть K - поле, $f : K[x] \to K$ - гомоморфизм подстановки :
$\forall\, p(x) \in K[x]\quad f\big(p(x)\big) = p(c) \in K$, где $c \in K$, тогда
1) f - гомоморфизм колец;

2) $Im\, f = K$, т.к. очевидно, что $Im\, f \subset K$, и
$\forall\, r \in K \;\; \exists\, p(x) = r \in K[x] \Rightarrow f(p(x)) = f(r) = r \Rightarrow r \in Im\, f \Rightarrow$
$\Rightarrow K \subset Im\, f$;
3) $Ker\, f = \{p(x) : p(c) = 0\} = \{p(x) : p(x) = (x-c)q(x),\; q(x) \in K[x]\} =$
$= (x-c)K[x] = (x-c) \lhd K[x]$.
Из 1),2),3) по теореме о гомоморфизме колец следует, что
$K[x]/_{(x-c)} \simeq K \;\; \forall\, c \in K$.
В частности, $\mathbb{R}[x]/_{(x-c)} \simeq \mathbb{R} \;\; \forall\, c \in \mathbb{R}$.

(2) Пусть $f : \mathbb{R}[x] \longmapsto \mathbb{C}$ гомоморфизм подстановки:
$\forall p(x) \in \mathbb{R}[x] \;\; f(p(x)) = p(i) \in \mathbb{C}$, тогда
1) $f -$ гомоморфизм колец;
2) $Im\; f = \mathbb{C}$, т.к.очевидно, что $Im\; f \subset \mathbb{C}$, и
$\forall z = a + ib \in \mathbb{C} \;\; \exists\, p(x) = a + bx \in \mathbb{R}[x] : f(p(x)) = a + ib = z \Rightarrow$
$\Rightarrow z \in Im\; f \Rightarrow \mathbb{C} \subset Im\; f$;
3) $Ker\; f = \{p(x) : p(i) = 0\} = \{p(x) : p(i) = 0,\; p(-i) = 0\} =$
$= \{p(x) : p(x) = (x-i)(x+i)q(x),\; q(x) \in \mathbb{R}[x]\} =$
$= \{p(x) : p(x) = (x^2+1)q(x),\; q(x) \in \mathbb{R}[x]\} = (x^2+1)\mathbb{R}[x] = (x^2+1) \lhd \mathbb{R}[x]$
Из $1), 2), 3)$ по теореме о гомоморфизме колец следует, что
$\mathbb{R}[x]/_{(x^2+1)} \simeq \mathbb{C}$

4 Прямые суммы колец

Опр. Внешней прямой суммой колец $A_1,\; A_2, ...,\; A_m$ называется множество $A_1 \oplus A_2 \oplus ... \oplus A_m = \{(a_1, a_2, ..., a_m) : a_i \in A_i, \quad i = \overline{1, m}\}$ с операциями сложения и умножения, определёнными поэлементно.

Утв. 7 Если $A_1,\; A_2, ...,\; A_m -$ кольца, то $A_1 \oplus A_2 \oplus ... \oplus A_m -$ кольцо.
Док-во: проверьте это самостоятельно.

Опр. Кольцо A называется внутренней прямой суммой собственных подколец $A_1,\; A_2, ...,\; A_m \subset A,\;\; A_i \neq \{0\},\;\; A_i \neq A,\;\; i = \overline{1, m}$ и обозначает-

ся $A = A_1 \oplus A_2 \oplus ... \oplus A_m$, если

$\begin{cases} 1)\ (A,+) = (A_1 \oplus A_2 \oplus ... \oplus A_m, +), \text{ т.е. аддитивная группа кольца } A \\ \text{является внутренней прямой суммой своих собственных подгрупп} \\ \text{(см. Лекцию 12 прошлого семестра);} \\ 2)\ a_i a_j = \overline{0} \text{ при } i \neq j,\ a_i \in A_i,\ a_j \in A_j,\ \ i,j = \overline{1,m} \end{cases}$

Note. Если $a, b \in A = A_1 \oplus A_2 \oplus ... \oplus A_m$, где A_i – подкольцо A, $i = \overline{1,m}$, то из $\begin{cases} 1) \\ 2) \end{cases} \Rightarrow ab = (a_1 + a_2 + ... + a_m)(b_1 + b_2 + ... + b_m) =$
$= a_1 b_1 + a_2 b_2 + ... + a_m b_m$

Понятия внутренней и внешней прямой суммы колец связаны между собой так же, как соотвествующие понятия для групп.

Утв. 8. Пусть A - кольцо, $A_1, A_2, ..., A_m$ - его собственные подкольца, тогда $A = A_1 \oplus A_2 \oplus ... \oplus A_m$

$\Updownarrow$

$\begin{cases} 1')\ \forall\, a \in A \text{ единственным образом представляется в виде} \\ \quad a = a_1 + a_2 + ... + a_m, \text{ где } a_i \in A_i,\ i = \overline{1,m}; \\ 2')\ A_i \lhd A \text{ - двусторонний идеал } A,\ \ i = \overline{1,m}. \end{cases}$

Док-во:

Заметим, что $1) \Leftrightarrow 1')$, т.к. $(A,+)$ - абелева группа.

Покажем, что $\begin{cases} 1) \\ 2) \end{cases} \Rightarrow 2')$.

$\forall\, b \in A\ \ b = b_1 + b_2 + ... + b_m,\ \ b_j \in A_j,\ \ j = \overline{1,m}$

$\forall\, a \in A_i\ \ \forall\, b \in A \begin{cases} ba_i = (\sum\limits_{j=1}^{m} b_j)a_i = b_i a_i \in A_i \Rightarrow ba_i \in A_i, \\ \text{аналогично, } a_i b \in A_i \end{cases} \Rightarrow$

$\Rightarrow A_i \lhd A,\ \ i = \overline{1,m}.$

Покажем, что $\begin{cases} 1') \\ 2') \end{cases} \Rightarrow 2)$.

Пусть $a_i \in A_i,\ a_j \in A_j,\ i \neq j,\ i,j = \overline{1,m}$,

тогда $a_i a_j \in A_i \cap A_j$, т.к. $A_i, A_j \lhd A$.

Если $a_i a_j \neq \overline{0}$, то этот элемент двумя способами представляется в виде суммы элементов подколец $A_1, ..., A_m$:

$a_i a_j = \overline{0} + ... + \overline{0} + a_i a_j + \overline{0} + ... + \overline{0}$, где $a_i a_j \in A_i$,

$a_i a_j = \overline{0} + ... + \overline{0} + a_i a_j + \overline{0} + ... + \overline{0}$, где $a_i a_j \in A_j$. $\Rightarrow$
$\Rightarrow a_i a_j = \overline{0}$ при $i \neq j$, $i, j = \overline{1, m}$.

Утв. 9. Пусть A - кольцо, A_1, A_2 - его собственные подкольца,

тогда $A = A_1 \oplus A_2 \Leftrightarrow \begin{cases} 1'') & A = A_1 + A_2 \\ 2'') & A_1 \cap A_2 = \{\overline{0}\} \\ 3'') & A_1, A_2 \lhd A. \end{cases}$

Док-во:

Т.к. A_1, A_2 - собственные подгруппы аддитивной группы A, $\begin{cases} 1'') \\ 2'') \end{cases} \Leftrightarrow 1')$.

Условия $3'')$ и $2')$ совпадают.

5 Идемпотенты. Критерий разложимости кольца в прямую сумму собственных подколец.

Опр.

Пусть A - кольцо, $a \in A$ называется идемпотентом, если $a^2 = a$.

Note.

В любом кольце с 1 существуют тривиальные идемпотенты $\overline{0}$ и 1.

Утв. 10. Если e - нетривиальный идемпотент кольца с 1,

то e - делитель нуля.

Док-во:

$$\begin{cases} e^2 = e \\ e \neq \overline{0} \\ e \neq 1 \end{cases} \Rightarrow \begin{cases} e(e-1) = \overline{0} \\ e \neq \overline{0} \\ e - 1 \neq \overline{0} \end{cases}$$

Утв. 11. Если e_1 - нетривиальный идемпотент кольца A с 1, то $e_2 = 1 - e_1$ - также нетривиальный идемпотент A и $e_1 e_2 = \overline{0}$.

Док-во:

$e_2^2 = (1 - e_1)^2 = 1 - 2e_1 + e_1^2 = 1 - 2e_1 + e_1 = 1 - e_1 = e_2$,
$e_1 e_2 = e_1(1 - e_1) = e_1 - e_1^2 = \overline{0}$.

Теорема 2. Критерий разложимости КАК1 в прямую сумму собственных подколец.

Пусть A - КАК1, A_1, A_2 - собственные подкольца A, тогда

$A = A_1 \oplus A_2 \Leftrightarrow \exists$ нетривиальный идемпотент $e \in A$.

Док-во:

$\Rightarrow$ Пусть $A = A_1 \oplus A_2 \Rightarrow A_1, A_2$ - собственные идеалы A.

$\exists\, e_1 \in A_1,\ e_2 \in A_2 : 1 = e_1 + e_2\ (*),\ \ e_1 e_2 = \overline{0}$.

Умножим $(*)$ на $e_1 \Rightarrow e_1 = e_1^2 + e_1 e_2 = e_1^2 \Rightarrow$

$\Rightarrow e_1 = e_1^2$, при этом:

$e_1 \neq \overline{0}$, т.к. иначе $e_2 = 1 \Rightarrow A_2 = A \Rightarrow A_2$ - несобственный идеал $\lightning$,

$e_1 \neq 1$, т.к. иначе $A_1 = A \Rightarrow A_1$ - несобственный идеал $\lightning$,

т.е. $e = e_1$ - нетривиальный идемпотент в A.

$\Leftarrow$ Пусть $e \in A -$ нетривиальный идемпотент. $\Rightarrow (1-e) -$ нетривиальный идемпотент. Обозначим $e_1 = e,\ e_2 = 1 - e \Rightarrow e_1 e_2 = \overline{0}$

Рассмотрим $A_1 = (e_1) \lhd A,\ A_2 = (e_2) \lhd A$.

$A_1,\ A_2 -$ собственные идеалы A, поскольку $A_i \neq \{0\}$ и $A_i \neq A,\ \ i = 1, 2$,

т.к. иначе $1 = e_i x \Rightarrow e_i \in A^*,\ i = 1, 2$, но $e_i -$ делитель нуля $\lightning$

$1'')\ A = A_1 + A_2$, т.к. $\forall a \in A\ \ a = a1 = a(e_1 + e_2) = ae_1 + ae_2$,

$ae_1 \in A_1,\ ae_2 \in A_2$,

$2'')\ A_1 \cap A_2 = \{\overline{0}\}$, т.к. если $a \in A_1 \cap A_2$, то $a = e_1 x = e_2 y$,

где $x, y \in A \Rightarrow a = e_1^2 x = e_1 e_2 y = \overline{0}$

$3'')\ A_1,\ A_2 \lhd A$

$1''),\ 2''),\ 3'') \Rightarrow A = A_1 \oplus A_2 -$ прямая сумма собственных подколец

Note. Пусть A - КАК1, $A = A_1 \oplus A_2,\ \ A_1 = (e_1),\ \ A_2 = (e_2)$, где e_1, e_2 - нетривиальные идемпотенты в A, тогда

$a = a_1 + a_2 = ae_1 + ae_2 = ae_1^2 + ae_2^2 = (ae_1)e_1 + (ae_2)e_2 = a_1 e_1 + a_2 e_2$.

Пример.

Рассмотрим $\mathbb{Z}_n,\ n = mk,\ (m, k) = 1$.

$\exists\, x, y \in \mathbb{Z} : mx + ky = 1\ \ (*)$,

если (x_0, y_0) - частное решение $(*)$, то $[mx_0]_n + [ky_0]_n = [1]_n\ \ (**)$ в $\mathbb{Z}_n$.

Тогда $e_1 = [mx_0]_n$ - нетривиальный идемпотент в $\mathbb{Z}_n$,
т.к. умножив $(**)$ на $[mx_0]_n$, получаем $[mx_0]_n^2 + [ky_0]_n[mx_0]_n = [mx_0]_n \Rightarrow$
$\Rightarrow [mx_0]_n^2 = [mx_0]_n$, т.е. $e_1^2 = e_1$,
$e_2 = [ky_0]_n$ - второй нетривиальный идемпотент в $\mathbb{Z}_n$.
Рассмотрим идеалы $(e_1) = ([mx_0]_n) \lhd \mathbb{Z}_n$, $(e_2) = ([ky_0]_n) \lhd \mathbb{Z}_n$.
$\mathbb{Z}_n = (e_1) \oplus (e_2) = ([mx_0]_n) \oplus ([ky_0]_n)$ - внутренняя прямая сумма.
$(e_1) = ([mx_0]_n) \simeq \mathbb{Z}_k$, $(e_2) = ([ky_0]_n) \simeq \mathbb{Z}_m$
$\mathbb{Z}_n \simeq \mathbb{Z}_k \oplus \mathbb{Z}_m$ - внешняя прямая сумма.
Если $f : \mathbb{Z}_n \to \mathbb{Z}_k \oplus \mathbb{Z}_m$ - изоморфизм,
то $\forall [z]_n \in \mathbb{Z}_n \;\; f([z]_n) = ([z]_k, [z]_m)$,
$\forall ([r_1]_k, [r_2]_m) \in \mathbb{Z}_k \oplus \mathbb{Z}_m \;\; f^{-1}([r_1]_k, [r_2]_m) = [r_1 mx_0 + r_2 ky_0]_n$.

Лекция №11

1 Китайская теорема об остатках(КТО)

Теорема 1. КТО в классической формулировке.

Для любого набора остатков $r_1,\ r_2, ...,\ r_n$ от деления на попарно взаимно простые числа $m_1,\ m_2, ...,\ m_n \in \mathbb{N}$ можно найти целое число, которое даёт остаток r_i при делении на m_i для каждого i от 1 до n, причём два таких числа отличаются друг от друга на целое кратное числа $m_1 m_2 ...\ m_n$.

Мы докажем Теорему 2 для КГИ. Теорема 1 будет её частным случаем.

Лемма 1. Пусть $A -$ КГИ, $a_1,\ a_2 \in A : (a_1, a_2) = 1$,
тогда $(a_1) \cap (a_2) = (a_1 a_2)$.

Док-во:
1) Пусть $c \in (a_1) \cap (a_2) \Rightarrow c = a_1 u = a_2 v, \quad u, v \in A$
$(a_1, a_2) = 1 \Rightarrow \exists\ x, y \in A :\ a_1 x + a_2 y = 1 \Rightarrow$
$\Rightarrow c a_1 x + c a_2 y = c \Rightarrow$
$\Rightarrow a_2 v a_1 x + a_1 u a_2 y = c \Rightarrow$
$\Rightarrow a_1 a_2 (vx + uy) = c \Rightarrow$
$\Rightarrow c \in (a_1 a_2) \Rightarrow (a_1) \cap (a_2) \subset (a_1 a_2)$
2) Очевидно, $(a_1 a_2) \subset (a_1) \cap (a_2)$
$1), 2) \Rightarrow (a_1) \cap (a_2) = (a_1 a_2)$

Лемма 2. Пусть $A -$ КГИ, $a,\ a_1,\ a_2, ...,\ a_m \in A : (a, a_i) = 1$,
$i = \overline{1, m}$, тогда $(a,\ a_1 a_2 ... a_m) = 1$

Док-во:
$(a, a_i) = 1 \Rightarrow \exists\ x_i,\ y_i \in A :\ a x_i + a_i y_i = 1,\ \ i = \overline{1, m} \Rightarrow$
$\Rightarrow \prod\limits_{i=1}^{m} (a x_i + a_i y_i) = 1 \ \ (*)$

Перемножив выражения в левой части $(*)$, получим сумму элементов кольца A, один из которых равен $a_1 a_2 ... a_m y_1 y_2 ... y_m$, а все остальные содержат множитель a. $\Rightarrow$

$\Rightarrow \prod_{i=1}^{m}(ax_i + a_i y_i) = aX + a_1 a_2 ... a_m Y = 1$, где $X,\ Y \in A \Rightarrow$
$\Rightarrow (a,\ a_1 a_2 ... a_m) = 1$

Теорема 2. КТО для КГИ.
Пусть A – КГИ, $a_1,\ a_2, ...,\ a_n \in A : (a_i, a_j) = 1$ при $i \neq j, \quad i, j = \overline{1, n}$,
тогда ${}^{A}/_{(a_1 a_2 ... a_n)} \simeq {}^{A}/_{(a_1)} \oplus {}^{A}/_{(a_2)} \oplus . . . \oplus {}^{A}/_{(a_n)}$

Док-во:
Докажем теорему индукцией по n.
1) $n = 2,\ \ a_1,\ a_2 \in A : (a_1, a_2) = 1 \Rightarrow {}^{A}/_{(a_1 a_2)} = {}^{A}/_{(a_1)} \oplus {}^{A}/_{(a_2)}$

Рассмотрим $\varphi : A \longmapsto {}^{A}/_{(a_1)} \oplus {}^{A}/_{(a_2)}$:
$\forall u \in A\ \ \varphi(u) = (u + (a_1),\ u + (a_2))$.

а) Покажем, что φ является гомоморфизмом колец.
$\varphi(u + v) = (u + v + (a_1),\ u + v + (a_2)) =$
$= (u + (a_1),\ u + (a_2)) + (v + (a_1),\ v + (a_2)) = \varphi(u) + \varphi(v)$
$\varphi(uv) = (uv + (a_1),\ uv + (a_2)) =$
$= (u + (a_1),\ u + (a_2))(v + (a_1),\ v + (a_2)) = \varphi(u)\varphi(v)$

б) $Im\ \varphi = {}^{A}/_{(a_1)} \oplus {}^{A}/_{(a_2)}$

Очевидно, что $Im\ \varphi \subset {}^{A}/_{(a_1)} \oplus {}^{A}/_{(a_2)}$.

Покажем, что ${}^{A}/_{(a_1)} \oplus {}^{A}/_{(a_2)} \subset Im\ \varphi$.
$(a_1, a_2) = 1 \Rightarrow \exists\, x, y \in\ A : a_1 x + a_2 y = 1 \Rightarrow \begin{cases} \varphi(a_2 y) = (1 + (a_1),\ 0 + (a_2)) \\ \varphi(a_1 x) = (0 + (a_1),\ 1 + (a_2)) \end{cases}$

$\forall (r + (a_1),\ s + (a_2)) \in {}^{A}/_{(a_1)} \oplus {}^{A}/_{(a_2)} \quad \exists\, u = ra_2 y + sa_1 x \in A :$

$\varphi(u) = \varphi(ra_2 y + sa_1 x) = \varphi(r)\varphi(a_2 y) + \varphi(s)\varphi(a_1 x) =$
$= (r+(a_1),\ r+(a_2))(1+(a_1),\ 0+(a_2))+(s+(a_1),\ s+(a_2))(0+(a_1),\ 1+(a_2)) =$
$= (r + (a_1),\ 0 + (a_2)) + (0 + (a_1),\ s + (a_2)) = (r + (a_1),\ s + (a_2)) \Rightarrow$
$\Rightarrow (r + (a_1),\ s + (a_2)) \in Im\ \varphi \Rightarrow {}^{A}/_{(a_1)} \oplus {}^{A}/_{(a_2)} \subset Im\ \varphi$

в) $Ker\ \varphi = (a_1 a_2)$

$Ker\ \varphi = \{u \in A : \varphi(u) = (0 + (a_1),\ 0 + (a_2))\} =$

$= \{u \in A : u \in (a_1),\ u \in (a_2)\} = (a_1) \cap (a_2) = (a_1 a_2)$

Из а),б),в) по теореме о гомоморфизме колец $\Rightarrow$

$\Rightarrow {}^{A}/_{(a_1 a_2)} \simeq {}^{A}/_{(a_1)} \oplus {}^{A}/_{(a_2)}$.

2) Пусть утверждение теоремы верно для $(n-1)$,

докажем, что оно верно для n.

$(a_n, a_i) = 1,\ \ i = \overline{1, n-1} \Rightarrow (a_n, a_1 a_2 ... a_{n-1}) = 1 \Rightarrow$

из 1) $\Rightarrow {}^{A}/_{(a_1 a_2 ... a_{n-1} a_n)} \simeq {}^{A}/_{(a_1 a_2 ... a_{n-1})} \oplus {}^{A}/_{(a_n)}$.

По предположению индукции

${}^{A}/_{(a_1 a_2 ... a_{n-1})} \simeq {}^{A}/_{(a_1)} \oplus {}^{A}/_{(a_2)} \oplus ... \oplus {}^{A}/_{(a_{n-1})} \Rightarrow$

$\Rightarrow {}^{A}/_{(a_1 a_2 ... a_{n-1} a_n)} \simeq {}^{A}/_{(a_1)} \oplus {}^{A}/_{(a_2)} \oplus ... \oplus {}^{A}/_{(a_{n-1})} \oplus {}^{A}/_{(a_n)}$

Примеры:

(1) K - поле $\Rightarrow\ K[x]$ - КГИ

$c_i \in K,\ c_i \neq c_j$ при $i \neq j,\ i, j = \overline{1, n} \Rightarrow$

$\Rightarrow ((x - c_i), (x - c_j)) = 1$ при $i \neq j,\ i, j, = \overline{1, n}$

${}^{K[x]}/_{((x-c_1)(x-c_2)...(x-c_n))} \simeq$

$\simeq {}^{K[x]}/_{(x-c_1)} \oplus {}^{K[x]}/_{(x-c_2)} \oplus ... \oplus {}^{K[x]}/_{(x-c_n)}$,

${}^{K[x]}/_{(x-c_i)} \simeq\ K \Rightarrow$

$\Rightarrow {}^{K[x]}/_{((x-c_1)(x-c_2)...(x-c_n))} \simeq\ K \oplus K \oplus ... \oplus K$

(2) ${}^{R[x]}/_{(x^4-1)} = {}^{R[x]}/_{((x-1)(x+1)(x^2+1))} \simeq$

$\simeq R[x]/_{(x-1)} \oplus R[x]/_{(x+1)} \oplus R[x]/_{(x^2+1)} \simeq \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{C}$

Note. Теорема 1 является частным случаем Теоремы 2 при $A = \mathbb{Z},\ a_i = m_i,\ i = \overline{1,n}$.

2 Решение системы сравнений

Пусть $m_1, m_2, ..., m_n \in \mathbb{N} : (m_i, m_j) = 1$ при $i \neq j,\ \ i, j = \overline{1,n}$

Найдём $z \in \mathbb{Z}$:

$$\begin{cases} z \equiv r_1 (mod\, m_1) \\ z \equiv r_2 (mod\, m_2) \\ ..... \\ z \equiv r_n (mod\, m_n) \end{cases} \Rightarrow z \equiv r_i (mod\, m_i),\ \ i = \overline{1,n} \ \Leftrightarrow\ [z]_{m_i} = [r_i]_{m_i},\ i = \overline{1,n}$$

$(m_i, m_j) = 1$ при $i \neq j,\ \ i, j = \overline{1,n} \Rightarrow (m_i, \prod\limits_{\substack{j=1 \\ j \neq i}}^{n} m_j) = 1$ (по лемме 2) $\Rightarrow$

$\Rightarrow \exists\, x_i, y_i \in \mathbb{Z} : m_i x_i + (\prod\limits_{\substack{j=1 \\ j \neq i}}^{n} m_j) y_i = 1.$

Обозначим $(\prod\limits_{\substack{j=1 \\ j \neq i}}^{n} m_j) y_i = l_i.$

$$\begin{cases} \Big[(\prod\limits_{\substack{j=1 \\ j \neq i}}^{n} m_j) y_i\Big]_{m_i} = [l_i]_{m_i} = [1]_{m_i} \\ \Big[(\prod\limits_{\substack{j=1 \\ j \neq i}}^{n} m_j) y_i\Big]_{m_j} = [l_i]_{m_j} = [\overline{0}]_{m_j} \text{ при } j \neq i,\ \ j = \overline{1,n} \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} [\ r_i l_i\ ]_{m_i} = [r_i]_{m_i} [l_i]_{m_i} = [r_i]_{m_i} \\ [\ r_i l_i\ ]_{m_j} = [r_i]_{m_j} [l_i]_{m_j} = [\overline{0}]_{m_j} \text{ при } j \neq i,\ \ j = \overline{1,n} \end{cases} \Rightarrow$$

$\Rightarrow [r_1 l_1 + r_2 l_2 + ... + r_n l_n]_{m_i} = [r_i]_{m_i},\ \ i = \overline{1,n} \Rightarrow$

$\Rightarrow z = r_1 l_1 + r_2 l_2 + ... + r_n l_n + k(m_1 m_2 ... m_n)$, где $k \in \mathbb{Z}$.

Пример. Найти наименьшее положительное $z \in \mathbb{Z}$:

$$(*) \begin{cases} z \equiv 2 (mod\, 57) \\ z \equiv 7 (mod\, 91) \\ z \equiv 43 (mod\, 179) \end{cases}$$

$m_1 = 57,\ m_2 = 91,\ m_3 = 179$

$r_1 = 2,\ r_2 = 7,\ r_3 = 43$

$(m_1, m_2m_3) = 1 \Rightarrow \exists\, x_1, y_1 \in \mathbb{Z} : m_1x_1 + m_2m_3y_1 = 1$, т.е.

$51x_1 + 91 \cdot 179y_1 = 1.$

Решаем это диофантово уравнение, чтобы найти $l_1 = m_1m_2y_1$

$$A = \begin{pmatrix} 57 & 91\cdot 179 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \overset{-179A^1+A^2}{\longrightarrow} \begin{pmatrix} 57 & 34\cdot 179 \\ 1 & -179 \\ 0 & 1 \end{pmatrix} \overset{-3\cdot 34A^1+A^2}{\longrightarrow} \begin{pmatrix} 57 & 34\cdot 8 \\ . & . \\ 0 & 1 \end{pmatrix} \longrightarrow$$

Поскольку нас интересует только y_1, мы можем не следить за второй строчкой матрицы.

$$\longrightarrow \begin{pmatrix} 57 & 272 \\ . & . \\ 0 & 1 \end{pmatrix} \overset{-5A^1+A^2}{\longrightarrow} \begin{pmatrix} 57 & -13 \\ . & . \\ 0 & 1 \end{pmatrix} \overset{4A^2+A^1}{\longrightarrow} \begin{pmatrix} 5 & -13 \\ . & . \\ 4 & 1 \end{pmatrix} \longrightarrow$$

$$\overset{3A^1+A^2}{\longrightarrow} \begin{pmatrix} 5 & 2 \\ . & . \\ 4 & 13 \end{pmatrix} \overset{-2A^2+A^1}{\longrightarrow} \begin{pmatrix} 1 & 2 \\ . & . \\ -22 & 13 \end{pmatrix} \Rightarrow y_1 = -22 \Rightarrow$$

$\Rightarrow l_1 = m_2m_3y_1 = (91 \cdot 179)(-22)$

Аналогично находятся $l_2 = m_1m_3y_2 = (57 \cdot 179)(-33)$,

$l_3 = m_1m_2y_3 = (57 \cdot 91)(-45) \Rightarrow$

$\Rightarrow z = r_1l_1 + r_2l_2 + r_3l_3 + km_1m_2m_3 =$

$= 2(91 \cdot 179)(-22) + 7(57 \cdot 179)(-33) + 43(57 \cdot 91)(-45) + k \cdot 57 \cdot 91 \cdot 179 =$

$= -(716\,716 + 2\,356\,893 + 10\,036\,845) + k\,928\,473 =$

$= -13\,110\,454 + k\,928\,473$ - общее решение $(*)$

$z > 0 \Leftrightarrow k > \dfrac{13\,110\,454}{928\,473} \approx 14,1$

Наименьшее положительное z получается при $k = 15$.

$z = -13\,110\,454 + 15 \cdot 928\,473 = 816\,641.$

3 Характеристика поля

Опр. Характеристикой *char K* поля K называется наименьшее натуральное число $n \in \mathbb{N} : \underbrace{1 + 1 + ... + 1}_{n} = \overline{0}$.

Если такого числа $n \in \mathbb{N}$ не существует, то $char\, K = 0$.
Т.о., $char\, K = ord_+ 1$, если $ord_+ 1 < \infty$
и $char\, K = 0$, если $ord_+ 1 = \infty$.

Примеры:
(1) $\mathbb{F}_p = \mathbb{Z}_p$, p - простое число $\Rightarrow char\, \mathbb{F}_p = p$.
(2) $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $char\, \mathbb{Q} = char\, \mathbb{R} = char\, \mathbb{C} = 0$.
(3) $\mathbb{F}_p(x) = Quot\, \mathbb{F}_p[x]$ - поле рациональных функций над $\mathbb{F}_p$ - бесконечное поле ненулевой характеристики, $char\, \mathbb{F}_p(x) = p$.

Утв. 1. Пусть K - поле, $char\, K \neq 0$, тогда
$\forall\, a \in K \setminus \{\overline{0}\}$ $ord_+ a = char\, K$.

Док-во:
$$\begin{cases} a \neq \overline{0} \\ \underbrace{a + a + ... + a}_{m} = \overline{0} \end{cases} \Leftrightarrow \begin{cases} a \neq \overline{0} \\ a(\underbrace{1 + 1 + ... + 1}_{m}) = \overline{0} \end{cases} \Leftrightarrow \underbrace{1 + 1 + ... + 1}_{m} = \overline{0} \Rightarrow$$
$\Rightarrow ord_+ a = ord_+ 1 = char\, K$.

Утв. 2. Пусть K - поле, $char\, K = n \neq 0$, тогда n - простое число.

Док-во:
Пусть $char\, K = n = ml$, где $n, m, l \in \mathbb{N}$, $m, l < n$.

$$\underbrace{1 + 1 + ... + 1}_{n=ml} = (\underbrace{1 + 1 + ... + 1}_{m})(\underbrace{1 + 1 + ... + 1}_{l}) = \overline{0} \Rightarrow \left[\begin{array}{l} \underbrace{1 + 1 + ... + 1}_{m} = \overline{0} \\ \underbrace{1 + 1 + ... + 1}_{l} = \overline{0} \end{array} \right. \Rightarrow$$

$$\Rightarrow \left[\begin{array}{l} ord_+ 1 \leqslant m < n = char\, K \ \text{Ж} \\ ord_+ 1 \leqslant l < n = char\, K \ \text{Ж} \end{array} \right. \Rightarrow n \text{ - простое число.}$$

Лекция №12

1 Простое подполе

Опр. Подполе F поля K называется его простым подполем, если F не содержит никакого другого подполя K, т.е. является его наименьшим по включению подполем.

Утв. 1. Если $L -$ подполе поля K, то $\overline{0}, 1$ поля K принадлежат L.

Док-во:

$\overline{0} \in K \Rightarrow \overline{0} \in L$, поскольку $(L, +) -$ подгруппа $(K, +)$.

Докажем, что единица e поля L совпадает с $1 \in K$.

$e^2 = e \Rightarrow e(e-1) = \overline{0} \Rightarrow$ поскольку в поле нет делителей нуля

$$\left[\begin{array}{l} e = \overline{0} \\ e = 1 \end{array}\right. \overset{\text{☹}}{\Rightarrow} e = 1 \Rightarrow 1 \in L$$

Утв. 2. Простое подполе в любом поле единственно.

Док-во:

Пусть $F_1, F_2 -$ два простых подполя поля K.

Рассмотрим $F_1 \cap F_2$.

$\overline{0}, 1 \in F_1 \cap F_2$, легко видеть $F_1 \cap F_2$ является подполем поля K.

$$\left\{\begin{array}{l} F_1 \cap F_2 \in F_i \;\; i = \overline{1,2} \\ F_i - \text{простое подполе} \end{array}\right. \Rightarrow F_i = F_1 \cap F_2 \Rightarrow F_1 = F_2$$

Теорема 1. Пусть $K -$ поле, $F -$ его простое подполе, тогда

1) $char\ K = p \neq 0 \Leftrightarrow F \simeq \mathbb{F}_p$,

2) $char\ K = 0 \Leftrightarrow F \simeq \mathbb{Q}$.

Док-во: Рассмотрим отображение $\psi : \mathbb{Z} \longmapsto F$, $\forall n \in \mathbb{N}$

$\psi(n) = \underbrace{1 + 1 + ... + 1}_{n} \in F$

$\psi(0) = \overline{0} \in F$

$\psi(-n) = \underbrace{(-1) + (-1) + ... + (-1)}_{n} \in F.$

Докажем, что $\psi -$ гомоморфизм колец

а) $m, n \in \mathbb{N}, m \geqslant n$

$\psi(m+n) = \underbrace{1+1+...+1}_{m+n} = \underbrace{1+1+...+1}_{m} + \underbrace{1+1+...+1}_{n} = \psi(m) + \psi(n);$

$\psi(m+(-n)) = \psi(m-n)) = \underbrace{1+1+...+1}_{m-n} =$

$= \underbrace{1+1+...+1}_{m} + \underbrace{(-1)+(-1)+...+(-1)}_{n} = \psi(m) + \psi(-n);$

$\psi((-m)+n) = \psi(-(m-n)) = \underbrace{(-1)+(-1)+...+(-1)}_{m-n} =$

$= \underbrace{(-1)+(-1)+...+(-1)}_{m} + \underbrace{1+1+...+1}_{n} = \psi(-m) + \psi(n);$

$\psi((-m)+(-n)) = \psi(-(m+n)) = \underbrace{(-1)+(-1)+...+(-1)}_{m+n} =$

$= \underbrace{(-1)+(-1)+...+(-1)}_{m} + \underbrace{(-1)+(-1)+...+(-1)}_{n} = \psi(-m) + \psi(-n);$

$l \in \mathbb{Z} \quad \psi(l+0) = \psi(l) = \psi(l) + \overline{0} = \psi(l) + \psi(0)$

б) $m, n \in \mathbb{N}$

$\psi(mn) = \underbrace{1+1+...+1}_{mn} = \underbrace{(1+1+...+1)}_{m}\underbrace{(1+1+...+1)}_{n} = \psi(m)\psi(n);$

$\psi((-m)n) = \psi(-mn) = \underbrace{(-1)+(-1)+...+(-1)}_{mn} =$

$= \underbrace{((-1)+(-1)+...+(-1))}_{m}\underbrace{(1+1+...+1)}_{n} = \psi(-m)\psi(n);$

$\psi((-m)(-n)) = \psi(mn) = \underbrace{1+1+...+1}_{mn} =$

$= \underbrace{((-1)+(-1)+...+(-1))}_{m}\underbrace{((-1)+(-1)+...+(-1))}_{n} = \psi(-m)\psi(-n);$

$l \in \mathbb{Z} \quad \psi(l \cdot 0) = \psi(0) = \overline{0} = \psi(l)\psi(0)$

1) $\Leftrightarrow$

Если $char\ K = p \neq 0$, то $Ker\ \psi = \{kp : k \in \mathbb{Z}\} = (p) \lhd \mathbb{Z}$.

По теореме о гомоморфизме $Im\ \psi \simeq {}^{\mathbb{Z}}\!/_{(p)} = \mathbb{Z}_p = \mathbb{F}_p \Rightarrow$

$\Rightarrow Im\ \psi -$ поле, $Im\ \psi \subset F \Rightarrow F = Im\ \psi$, т.к. $F -$ простое подполе $\Rightarrow$

$\Rightarrow F \simeq \mathbb{F}_p$

2) $\Leftrightarrow$

Если $char\ K = 0$, то $Ker\ \psi = \{\overline{0}\}$.

По теореме о гомоморфизме $Im\ \psi \simeq \mathbb{Z} \Rightarrow$

$\Rightarrow Im\ \psi -$ кольцо, $Im\ \psi \subset F$

Рассмотрим $\mathbb{Q} = Quot\ \mathbb{Z}$ и распространим ψ на $\mathbb{Q}$, построив $\Psi : \mathbb{Q} \longmapsto F$.

Определим $\Psi(\frac{m}{n}) \ \ \forall \frac{m}{n} \in \mathbb{Q}$:

$\Psi(\frac{m}{n}) = \dfrac{\psi(m)}{\psi(n)}, \ \ m \in \mathbb{Z}, \in \mathbb{Z}^{\diagdown}\{0\}.$

$\Psi(\frac{m}{1}) = \dfrac{\psi(m)}{\psi(1)} = \psi(m)$, т.е. ${\Psi}\big|_{\mathbb{Z}} = \psi$.

Проверим, что Ψ определено корректно.

$\dfrac{m}{n} = \dfrac{m_1}{n_1} \Leftrightarrow mn_1 = nm_1 \Rightarrow \psi(mn_1) = \psi(nm_1) \Leftrightarrow \psi(m)\psi(n_1) = \psi(n)\psi(m_1)\ (*)$

Умножим $(*)$ на $(\psi(n))^{-1}(\psi(n_1))^{-1} \Rightarrow \dfrac{\psi(m)}{\psi(n)} = \dfrac{\psi(m_1)}{\psi(n_1)} \Rightarrow \Psi(\frac{m}{n}) = \Psi(\frac{m_1}{n_1})$

Проверим, что Ψ - гомоморфизм:

а) $\Psi(\frac{m}{n} + \frac{s}{t}) = \Psi(\frac{mt+sn}{nt}) = \dfrac{\psi(mt+sn)}{\psi(nt)} = \dfrac{\psi(m)\psi(t)+\psi(s)\psi(n)}{\psi(n)\psi(t)} =$

$\dfrac{\psi(m)}{\psi(n)} + \dfrac{\psi(s)}{\psi(t)} = \Psi(\frac{m}{n}) + \Psi(\frac{s}{t})$

б) $\Psi(\frac{m}{n} \cdot \frac{s}{t}) = \Psi(\frac{ms}{nt}) = \dfrac{\psi(ms)}{\psi(nt)} = \dfrac{\psi(m)\psi(s)}{\psi(n)\psi(t)} = \dfrac{\psi(m)}{\psi(n)} \cdot \dfrac{\psi(s)}{\psi(t)} = \Psi(\frac{m}{n}) \cdot \Psi(\frac{s}{t})$

$Ker\,\Psi = \{\overline{0}\}$, т.к. Ψ - нетривиальный гомоморфизм поля $\mathbb{Q}$ в F.

По теореме о гомоморфизме $Im\,\Psi \simeq \mathbb{Q} \Rightarrow$

$\Rightarrow Im\,\Psi$ - поле, $Im\,\Psi \subset F \Rightarrow F = Im\,\Psi$, т.к. F - простое подполе $\Rightarrow$

$\Rightarrow F \simeq \mathbb{Q}$.

Мы доказали $\begin{cases} 1) \circledcirc \\ 2) \circledcirc \end{cases}$, т.е. $\begin{cases} \text{если } char\, K = p \neq 0 \Rightarrow F \simeq \mathbb{F}_p, \\ \text{если } char\, K = 0 \Rightarrow F \simeq \mathbb{Q}, \end{cases}$

а поскольку условия $char\, K = p \neq 0$ и $char\, K = 0$
являются взаимоисключающими, отсюда следует
1) $char\, K = p \neq 0 \Leftrightarrow F \simeq \mathbb{F}_p$,
2) $char\, K = 0 \Leftrightarrow F \simeq \mathbb{Q}$.

Note. Из доказательства теоремы ясно, что простое подполе F поля K изоморфно $Im\,\psi$ или $Im\,\Psi$, т.е. в любом случае ненулевыми элементами F являются кратные 1, кратные (-1) и их отношения.

Следствие. Если F - простое подполе поля K,
$\varphi : K \to K$ автоморфизм, то $\varphi\big|_F = id$.
(Любой автоморфизм поля оставляет на месте все элементы его простого подполя.)

Док-во:

$$\varphi \text{ - автоморфизм} \Rightarrow \begin{cases} \varphi(\overline{0}) = \overline{0} \\ \varphi(1) = 1 \\ \varphi(\underbrace{1+1+...+1}_{m}) = \underbrace{1+1+...+1}_{m} \\ \varphi(-1) = -1 \\ \varphi(-a) = -\varphi(a) \\ \varphi(b^{-1}) = (\varphi(b))^{-1} \end{cases} \Rightarrow$$

$\Rightarrow \forall\, a \in F \Rightarrow \varphi(a) = a$

2 Расширение поля. Степень расширения.

Опр. Если поле K является подполем поля L, то поле L называется расширением поля K.
Поле L можно рассматривать как линейное пространство над полем K.
(Элементы L - «векторы», а элементы K - «числа».)

Определены линейные операции в L над K :
$\forall\, x, y \in L \Rightarrow x + y \in L$,
$\forall\, x \in L,\ \forall\, \alpha \in K \Rightarrow \alpha x \in L$,
выполняются аксиомы линейного пространства:
1) $x + y = y + x \ \ \forall\, x, y \in L$,
2) $(x + y) + x = x + (y + z) \ \ \forall\, x, y, z \in L$,
3) $\exists\, \overline{0} \in L : \overline{0} + x = x + \overline{0} = x \ \ \forall\, x \in L$,
4) $\forall\, x \in L \ \ \exists (-x) \in L : x + (-x) = (-x) + x = \overline{0}$,
5) $1x = x \ \ \forall\, x \in L,\ 1 \in K$,
6) $(\alpha\beta)x = \alpha(\beta x) \ \ \forall\, x \in L, \ \ \forall\, \alpha, \beta \in K$,
7) $\alpha(x + y) = \alpha x + \alpha y \ \ \forall\, x, y \in L,\ \forall\, \alpha \in K$,
8) $(\alpha + \beta)x = \alpha x + \beta x \ \ \forall\, x \in L,\ \forall\, \alpha, \beta \in K$.

Обозначим $dim_K L$ размерности линейного пространства L над K.

Опр. Если $dim_K L < \infty$, то поле L называется конечным расширением поля K, а $dim_K L$ называется степенью расширения L над K.

Примеры:
(1) $\mathbb{R} \subset \mathbb{C}$, $\mathbb{C}$ - конечное раширение $\mathbb{R}$ степени 2,
т.к. $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$, $< 1, i >$ - базис $\mathbb{C}$ над $\mathbb{R}$ $\Rightarrow dim_{\mathbb{R}}\mathbb{C} = 2$.
(2) $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{R}$ не является конечным расширением $\mathbb{Q}$, т.к. если бы $dim_{\mathbb{Q}}\mathbb{R} = n < \infty$, то существовало бы биективное соответствие между $\mathbb{R}$ и $\mathbb{Q}^n$, следовательно, $\mathbb{R}$ было бы счётным множеством. $\lightning$.

Утв. 3. Если K - конечное поле ($|K| < \infty$), а L - его конечное расширение степени n ($dim_K L = n < \infty$), то L - конечное поле
и $|L| = |K|^n$.

Док-во:
$dim_K L = n \Rightarrow \exists\ < e_1, e_2, ..., e_n >$ - базис L над $K \Rightarrow$
$\Rightarrow \forall\, x \in L \ \ \exists\, \alpha_1, \alpha_2, ..., \alpha_n \in K : x = \alpha_1 e_1 + \alpha_2 e_2 + ... + \alpha_n e_n$,
α_i может принимать любое из $|K|$ значений, $i = \overline{1, n} \Rightarrow |L| = |K|^n$.

Следствие. Если L - конечное поле, F - его простое подполе, то $|L| = p^n$, где $p = char\, L$ - простое число, $n = dim_F L \in \mathbb{N}$.

Док-во:

$|L| < \infty \Rightarrow ord_+ 1 < \infty \Rightarrow char\, L \neq 0 \Rightarrow char\, L = p$ - простое число $\Rightarrow$
$\Rightarrow$ простое подполе поля L $F \simeq \mathbb{F}_p \Rightarrow |F| = |\mathbb{F}_p| = p$,
$F \subset L,\ |L| < \infty \Rightarrow dim_F L = n < \infty,\ n \in N \Rightarrow |L| = |F|^n = p^n$.

Теорема 2. Если L - конечное расширение поля K, а M - конечное расширение поля L, то M - конечное расширени поля K
и $dim_K M = dim_K L\, dim_L M$.

$$\begin{cases} K, L, M \text{ - поля}, \\ K \subset L \subset M, \\ dim_K L < \infty, \\ dim_L M < \infty \end{cases} \Rightarrow \quad dim_K M = dim_K L \cdot dim_L M.$$

Док-во:

$$\text{Пусть } \begin{cases} dim_K L = l \Rightarrow \exists < f_1, f_2, ..., f_l > \text{ - базис } L \text{ над } K \\ dim_L M = m \Rightarrow \exists < g_1, g_2, ..., g_m > \text{ - базис } M \text{ над } L \end{cases} \Rightarrow$$

$\Rightarrow < f_1 g_1, f_1 g_2, ..., f_l g_m >$ - базис M над K.

0) $f_1 g_1, f_1 g_2, ..., f_l g_m \in M$

1) Пусть $\sum\limits_{\substack{i=\overline{1,l} \\ j=\overline{1,m}}} x_{ij} f_i g_j = \overline{0} \Leftrightarrow \sum\limits_{j=1}^{m} \big(\sum\limits_{i=1}^{l} x_{ij} f_i \big) g_j = \overline{0}$

$g_1, g_2, ..., g_m$ - линейно независимая система $\Rightarrow \sum\limits_{i=1}^{l} x_{ij} f_i = \overline{0}\ \ \forall\, j = \overline{1, m}$;
$f_1, f_2, ..., f_l$ - линейно независимая система $\Rightarrow$
$\Rightarrow x_{ij} = \overline{0}\ \ \forall\, i = \overline{1, l}\,,\ \ \forall\, j = \overline{1, m} \Rightarrow f_1 g_1, f_2 g_2, ..., f_l g_m$ - линейно независимая система.

2) $\forall\, a \in M\ \exists\, y_1, ..., y_m \in L : a = \sum\limits_{j=1}^{m} y_j g_j$, т.к. $< g_1, g_2, ..., g_m >$ - базис M над L,

$\forall\, y_j \in L,\ j = \overline{1, m}\ \ \exists\, x_{1j}, x_{2j}, ..., x_{lj} \in K : y_j = \sum\limits_{i=1}^{l} x_{ij} f_i$,
т.к. $< f_1, f_2, ..., f_m >$ - базис L над $K \Rightarrow$

$\Rightarrow a = \sum\limits_{j=1}^{m} \big(\sum\limits_{i=1}^{l} x_{ij} f_i \big) g_j = \sum\limits_{\substack{i=\overline{1,l} \\ j=\overline{1,m}}} x_{ij} f_i g_j \Rightarrow$

0),1),2) $\Rightarrow$ $< f_1 g_1, f_1 g_2, ..., f_l g_m >$ - базис M над $K \Rightarrow$

$\Rightarrow dim_K M = l \cdot m = dim_K L \cdot dim_L M.$

Утв. 4. Если M – конечное расширение своего простого подполя F, K – подполе $M \Rightarrow K$ – конечное расширение F и $dim_F K | dim_F M$.

Док-во:

$F \cap K$ – подполе $F \Rightarrow F = F \cap K \Rightarrow F \subset K \subset M \Rightarrow$

$\Rightarrow K$ – линейное подпространство пространства M над $F \Rightarrow$

$\Rightarrow dim_F K \leqslant dim_F M = n < \infty$

$dim_F M = n < \infty \Rightarrow \exists$ $< e_1, ..., e_n >$ – базис M над $F \Rightarrow$

$M = L_F[e_1, e_2, ..., e_n] = L_K[e_1, e_2, ..., e_n]$

$dim_F M = rk_F\{e_1, e_2, ..., e_n\},$

$dim_K M = rk_K\{e_1, e_2, ..., e_n\} \Rightarrow dim_K M \leqslant dim_F M = n < \infty \Rightarrow$

$\Rightarrow$ по теореме 2 $dim_F M = dim_F K \cdot dim_K M$

Следствие. Если M – поле, F – его простое подполе, $dim_F M$ – простое число, то F – единственное собственное подполе поля M.

Док-во:

Пусть K – подполе $M \Rightarrow F \subset K \subset M$ и $dim_F M = dim_F K \cdot dim_K M$

Поскольку $dim_F M$ – простое число, то $\left[\begin{array}{l} dim_F K = dim_F M \Rightarrow K = M \\ dim_F K = 1 \Rightarrow K = F \end{array} \right.$

Лекция №13

1 Алгебраические элементы расширения поля

Опр. Пусть K, L – поля, $K \subset L$. Элемент $u \in L$ называется алгебраическим над K, если u является корнем некоторого нетривиального многочлена над K, т.е. существует $f(x) \in K[x] \setminus \{\overline{0}\} : f(u) = \overline{0}$.
Если такого многочлена не существует, то элемент $u \in L$ называется транцендентным над K.

Note. $\forall a \in K \subset L$ является алгебраическим элементом над K, т.к. a является корнем многочлена $x - a \in K[x] \setminus \{\overline{0}\}$.

Примеры:
(1) $\mathbb{Q} \subset \mathbb{R}$, $\sqrt{2} \in \mathbb{R}$ является алгебраическим элементом над $\mathbb{Q}$, т.к. $\sqrt{2}$ – корень $x^2 - 2 \in \mathbb{Q}[x] \setminus \{\overline{0}\}$
(2) $\mathbb{R} \subset \mathbb{C}$, $i \in \mathbb{C}$ является алгебраическим элементом над $\mathbb{R}$, т.к. i – корень $x^2 + 1 \in \mathbb{R}[x] \setminus \{\overline{0}\}$

Опр. Пусть K, L – поля, $K \subset L$. Поле L называется алгебраическим расширением поля K, если любой элемент поля L является алгебраическим над K.

2 Простое алгебраическое расширение поля.

Опр. Пусть K, L – поля, $K \subset L$. Поле L называется простым алгебраическим расширением поля K, если
$L = K[u] = \{p(u) : p(x) \in K[x],\ u \in L : \exists f(x) \in K[x] \setminus \{\overline{0}\} : f(u) = \overline{0}\}$,
алгебраический элемент $u \in L$ называется примитивным элементом этого расширения.

Теорема 1. Пусть K – поле, $f(x) \in K[x]$ – неприводимый многочлен, $deg\ f(x) = n > 1$. Тогда $L = {}^{K[x]}/_{(f(x))}$ – поле, $K \subset L$,

$dim_K L = n$ и L – простое алгебраическое расширение K.

Док-во:

L – поле, поскольку $f(x)$ – неприводимый многочлен.

Обозначим $[p(x)]$ смежный класс $p(x) + (f(x)) \in {}^{K[x]}/_{(f(x))} = L$.

При этом смежный класс $[a]$ многочлена a, $deg\ a \leqslant 0$ можно отождествить с $a \in K$, поскольку если $a, b \in K : a \neq b$, то $[a] \neq [b]$. $\Rightarrow K \subset L$.
Т.к. $\forall p(x) \in K[x]\ \ p(x) = f(x)q(x) + r(x)$,
где $q(x), r(x) \in K[x],\ deg\ r(x) < deg\ f(x) = n \Rightarrow$
$\Rightarrow r(x) = a_0x^{n-1} + a_1x^{n-2} + ... + a_{n-2}x + a_{n-1},\ \ a_i \in K,\ \ i = \overline{0, n-1} \Rightarrow$
$\Rightarrow \forall\ [p(x)] \in L \quad [p(x)] = [a_0x^{n-1} + a_1x^{n-2} + ... + a_{n-2}x + a_{n-1}] =$
$= [a_0][x]^{n-1} + [a_1][x]^{n-2} + ... + [a_{n-2}][x] + [a_{n-1}] =$
$= a_0[x]^{n-1} + a_1[x]^{n-2} + ... + a_{n-2}[x] + a_{n-1},\ \ a_i \in K,\ \ i = \overline{0, n-1}.$

Докажем, что $< [x]^{n-1}, [x]^{n-2}, ..., 1 >$ – базис линейного пространства L над полем K.
0) $[x]^{n-1}, [x]^{n-2}, ..., 1 \in L$

1) Пусть $a_0[x]^{n-1} + a_1[x]^{n-2} + ... + a_{n-2}[x] + a_{n-1}1 = \overline{0} \in L \Leftrightarrow$
$\Leftrightarrow a_0x^{n-1} + a_1x^{n-2} + ... + a_{n-2}x + a_{n-1}1 = f(x)g(x),\ \ g(x) \in K[x]$
Если $g(x) \neq \overline{0}$, то $deg\ f(x)g(x) \geqslant n$,
а $deg(a_0x^{n-1} + a_1x^{n-2} + ... + a_{n-2}x + a_{n-1}1) < n \quad \lightning \Rightarrow g(x) = \overline{0} \Rightarrow$
$\Rightarrow a_0x^{n-1} + a_1x^{n-2} + ... + a_{n-2}x + a_{n-1} = \overline{0} \Rightarrow a_i = \overline{0} \quad i = \overline{0, n-1} \Rightarrow$
$\Rightarrow [x]^{n-1}, [x]^{n-2}, ..., 1$ – линейно независимая система векторов линейного пространства L над K.

2) $\forall\ [p(x)] \in L\ \ p(x) = a_0[x]^{n-1} + a_1[x]^{n-2} + ... + a_{n-2}[x] + a_{n-1}$,
$a_i \in K,\ \ i = \overline{0, n-1} \Rightarrow [x]^{n-1}, [x]^{n-2}, ..., 1$ – полная система в L над K

$0), 1), 2) \Rightarrow < [x]^{n-1}, [x]^{n-2}, ..., 1 >$ – базис линейного пространства L над полем K. $\Rightarrow dim_K L = n = deg\ f(x)$.
Элемент $u = [x] \in L$ является корнем $f(x)$, т.к. $f([x]) = [f(x)] = \overline{0} \in L$,

$L = K[u] = \{a_0u^{n-1} + a_1u^{n-2} + ... + a_{n-2}u + a_{n-1}, a_i \in K, \ \ f(u) = \overline{0}\} \Rightarrow$
$\Rightarrow L -$ простое алгебраическое расширение K,
$u = [x] -$ примитивный элемент этого расширения.
Говорят, что поле $L = {}^{K[x]}/_{(f(x))}$ получено из поля K с помощью присоединения корня неприводимого многочлена $f(x)$.

Примеры:
(1) $\mathbb{Q}[\sqrt{2}] \simeq {}^{\mathbb{Q}[x]}/_{(x^2-2)} -$ простое алгебраическое расширение $\mathbb{Q}$,
$\sqrt{2} -$ примитивный элемент расширения, корень неприводимого над $\mathbb{Q}$ многочлена $x^2 - 2$, $dim_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}] = 2 = deg(x^2 - 2)$.
(2) $\mathbb{C} \simeq {}^{\mathbb{R}[x]}/_{(x^2+1)} = \mathbb{R}[i] -$ простое алгебраическое расширение $\mathbb{R}$,
$i -$ примитивный элемент расширения, корень неприводимого над $\mathbb{R}$ многочлена $x^2 + 1$, $dim_{\mathbb{R}}\mathbb{C} = 2 = deg(x^2 + 1)$.

3 Минимальный многочлен алгебраического элемента расширения поля

Опр.
Пусть K, L - поля, $K \subset L$, $u \in L$ - алгебраический элемент над K.
Минимальным многочленом $u \in L$ называется $m_u(x) \in K[x]\setminus\{\overline{0}\}$:

$$\begin{cases} 1)\ m_u(u) = \overline{0}, \\ 2)\ deg\, m_u(x) = min\big\{deg\, f(x) : f(x) \in K[x]\setminus\{\overline{0}\},\ f(u) = \overline{0}\big\}, \\ 3)\ \text{старший коэффициент } m_u(x) \text{ равен 1.} \end{cases}$$

Note. Очевидно, что для любого алгебраического элемента u существует минимальный многочлен $m_u(x)$, причём из 3) следует, что он определён однозначно.

Утв. 1. Пусть K, L - поля, $K \subset L$, $u \in L$ - алгебраический элемент над $K \Rightarrow I_u = \big\{f(x) \in K[x] : f(u) = \overline{0}\big\} \lhd K$ и $I_u \neq \{\overline{0}\}$.

Док-во:
$I_u \neq \{\overline{0}\}$, т.к. I_u содержит $f(x) \in K[x]\setminus\{\overline{0}\} : f(u) = \overline{0}$.
Рассмотрим $\varphi : K[x] \to L$ - гомоморфизм подстановки,

$\forall\, p(x) \in K[x]\ \ \varphi(p(x)) = p(u) \in L$
Тогда $I_u = Ker\,\varphi \lhd K[x]$.

Утв. 2. Пусть K, L - поля, $K \subset L$, $u \in L$ - алгебраический элемент над $K \Rightarrow I_u = \big(m_u(x)\big)$.

Док-во:
K - поле $\Rightarrow K[x]$ - КГИ; $I_u \lhd K[x]$, $I_u \neq \{\overline{0}\} \Rightarrow$
$\Rightarrow \exists\, h(x) \in K[x]\diagdown\{\overline{0}\} : I_u = (h(x))$, $h(x)$ определён однозначно с точностью до ассоциированности.
1) $h(u) = \overline{0}$
2) $\forall\, f(x) \in I_u\diagdown\{\overline{0}\}\ \ f(x) = h(x)g(x),\ g(x) \neq \overline{0} \Rightarrow deg\, h(x) \leqslant deg\, f(x)$
Пусть старший коэффициент $h(x)$ равен $a_0 \Rightarrow$
$\Rightarrow \dfrac{1}{a_0}h(x) = m_u(x),\ h(x) \sim m_u(x) \Rightarrow I_u = (m_u(x))$.

Утв. 3. Пусть K, L - поля, $K \subset L$, $u \in L$ - алгебраический элемент над $K \Rightarrow m_u(x) \in K[x]$ - неприводимый многочлен.

Док-во:
$m_u(x) \neq \overline{0}$, пусть $m_u(x)$ - приводимый многочлен, тогда
$m_u(x) = h(x)g(x)$, где $h(x), g(x) \in K[x] : \begin{cases} 0 < deg\, h(x) < deg\, m_u(x) \\ 0 < deg\, g(x) < deg\, m_u(x). \end{cases}$
$m_u(u) = h(u)g(u) = \overline{0} \Rightarrow \left[\begin{array}{l} h(u) = \overline{0} \\ g(u) = \overline{0} \end{array}\right.$,
но $deg\, m_u(x) = min\{deg\, f(x) : f(x) \in K[x]\diagdown\{\overline{0}\},\ \ f(u) = \overline{0}\}$ $\Rightarrow\!\!\!\!\!\!\diagup$
$\Rightarrow\ m_u(x)$ - неприводимый многочлен.

Утв. 4. Пусть K, L - поля, $K \subset L$, $u \in L$ - алгебраический элемент над K, $p(x) \in K[x]$ - неприводимый многочлен, $p(u) = \overline{0}$, тогда
$p(x) \sim m_u(x)$, а если старший коэффициент $p(x)$ равен единице,
то $p(x) = m_u(x)$.

Док-во:
$p(u) = \overline{0} \Rightarrow p(x) \in I_u = (m_u(x)) \Rightarrow p(x) = m_u(x)q(x)$, но $p(x)$ неприводимый многочлен $\Rightarrow q(x) \in \big(K[x]\big)^* = K^* \Rightarrow p(x) \sim m_u(x)$.

Примеры:

(1) $m_{\sqrt{2}}(x) = x^2 - 2$, т.к. $x^2 - 2 \in \mathbb{Q}[x]$ - неприводимый аннулирующий многочлен $\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$.

(2) $m_i(x) = x^2 + 1$, т.к. $x^2 + 1 \in \mathbb{R}[x]$ - неприводимый аннулирущий многочлен $i \in \mathbb{C}$, $\mathbb{R} \subset \mathbb{C}$.

Теорема. Пусть K, L - поля, $K \subset L$, тогда $u \in L$ является алгебраическим элементом над $K \Leftrightarrow dim_K K[u] < \infty$.

Док-во:

$\Leftarrow$ Пусть $dim_K K[u] = n < \infty$, тогда система $u^n, u^{n-1}, ..., u, 1$, состоящая из $(n+1)$ элемента, является линейно зависимой $\Rightarrow$

$\Rightarrow \exists\, a_0, a_1, ..., a_n \in K$, не все равные нулю одновременно:

$a_0 u^n + a_1 u^{n-1} + ... + a_{n-1} u + a_n = \overline{0} \Rightarrow$

$\Rightarrow$ u - корень $f(x) = a_0 x^n + a_1 x^{n-1} + ... + a_n \in K[x] \setminus \{\overline{0}\}$, т.е.

u - алгебраический элемент над K.

$\Rightarrow$ Пусть $u \in L$ - алгебраический элемент над $K \Rightarrow$

$\Rightarrow$ $\exists\, m_u(x) \in K[x] \setminus \{\overline{0}\}$, пусть $deg\, m_u(x) = n$, $m_u(x) = x^n + a_1 x^{n-1} + ... + a_n$

$m(u) = \overline{0} \Rightarrow u^n = -a_1 u^{n-1} - a_2 u^{n-2} - ... - a_n 1 \Rightarrow$

$\Rightarrow$ любая степень элемента u линейно выражается через $u^{n-1}, u^{n-2}, ..., u, 1 \Rightarrow$

$\Rightarrow K[u]$ принадлежит линейной оболочке $u^{n-1}, n^{n-2}, ..., u, 1 \Rightarrow$

$\Rightarrow dim_K K[u] \leqslant rk\{u^{n-1}, u^{n-2}, ..., u, 1\} \leqslant n < \infty$.

Следствие. Пусть K, L - поля, $K \subset L$, $dim_K L < \infty$,
тогда L - алгебраическое расширение K.

Док-во:

$\forall\, u \in L$ $K[u]$ - линейное подпространство линейного пространства L над $K \Rightarrow dim_K K[u] \leqslant dim_K L < \infty \Rightarrow u$ является алгебраическим элементом над K.

Утв. 5. Пусть K, L - поля, $K \subset L$, $u \in L$ - алгебраический элемент над $K \Rightarrow K[u] \simeq {}^{K[x]}/_{(m_u(x))}$ - поле и $dim_K K[u] = deg\, m_u(x)$.

Док-во:

Рассмотрим $\varphi : K[x] \to L$ - гомоморфизм подстановки,

$\forall\, p(x) \in K[x]\ \ \varphi(p(x)) = p(u)$.
$Ker\,\varphi = I_u = (m_u(x))$.
$Im\,\varphi = K[u]$.
По теореме о гомоморфизме колец ${}^{K[x]}/_{(m_u(x))} \simeq K[u]$.
$m_u(x) \in K[x]$ - неприводимый многочлен $\Rightarrow K[u]$ - поле.
По теореме 1 $dim_K K[u] = deg\, m_u(x)$.

Лекция №14

1 Эндоморфизм Фробениуса

Теорема 1. Пусть K – поле, $char\ K = p \neq 0$,
$\Phi : K \longmapsto K$, $\forall u \in K\ \ \Phi(u) = u^p \in K$, тогда
Φ является эндоморфизмом поля K.

Док-во:

1) $\Phi(a+b) = (a+b)^p = \sum\limits_{m=0}^{p} C_p^m a^m b^{p-m} = a^p + b^p = \Phi(a) + \Phi(b)$, т.к.

$$\begin{cases} p - \text{простое} \Rightarrow (p,l) = 1,\ l = \overline{1, p-1} \Rightarrow (p, m!) = 1,\ m = \overline{1, p-1} \\ C_p^m = \dfrac{p!}{m!(p-m)!} = \dfrac{p(p-1)...(p-m+1)}{1 \cdot 2...m} \in \mathbb{Z},\ m = \overline{1, p-1} \end{cases} \Rightarrow$$

$$\Rightarrow \frac{(p-1)(p-2)...(p-m+1)}{1 \cdot 2...m} \in \mathbb{Z},\ m = \overline{1, p-1} \Rightarrow C_p^m \vdots\ p,\ m = \overline{1, p-1} \Rightarrow$$

$\Rightarrow C_p^m = \overline{0}$ в K, $m = \overline{1, p-1}$

2) $\Phi(ab) = (ab)^p = a^p\, b^p = \Phi(a)\Phi(b)$

1), 2) $\Rightarrow \Phi$ – гомоморфизм K в себя $\Rightarrow \Phi$ – эндоморфизм K.

Φ называется эндоморфизмом Фробениуса

Следствие 1. Эндоморфизм Фробениуса является мономорфизмом.

Док-во:

K – поле, Φ – нетривиальный гомоморфизм, т.к. $\Phi(1) = 1 \neq \overline{0} \Rightarrow$
$\Rightarrow Ker\ \Phi = \{\overline{0}\} \Rightarrow \Phi$ – мономорфизм.

Следствие 2. Если K – конечное поле, то эндоморфизм Фробениуса является автоморфизмом.

Док-во:

1) $Ker\ \Phi = \{\overline{0}\}$.

2) По теореме о гомоморфизме $Im\ \Phi \simeq {}^{K}/_{Ker\ \Phi} = K \Rightarrow$
$\Rightarrow K \simeq Im\ \Phi \subset K$, но $|K| < \infty \Rightarrow |Im\ \Phi| = |K| \Rightarrow Im\ \Phi = K$.

1), 2) $\Rightarrow \Phi$ – автоморфизм поля K.

Note. Вообще нетривиальный эндоморфизм конечного поля является его автоморфизмом. Доказывается аналогично.

Утв. 1. Пусть K - поле, $char\, K = p \neq 0,\ F$ - простое подполе K, $\Phi : K \to K$ - эндоморфизм Фробениуса, тогда $\Phi|_F = id$.

Док-во:

$F \simeq \mathbb{F}_p \Rightarrow |F^*| = p - 1 \Rightarrow$

$\Rightarrow \forall\, a \in F^*\ \ a^{p-1} = 1$ (малая теорема Ферма) $\Rightarrow \forall\, a \in F\ \ a^p = a$,

т.е. $\forall\, a \in F\ \ \Phi(a) = a$.

Будем далее отождествлять простое подполе $F \simeq \mathbb{F}_p$ с полем $\mathbb{F}_p$.

Утв. 2. Пусть K - поле, $char\, K = p \neq 0$, тогда эндоморфизм Фробениуса поля K - линейный оператор в линейном пространстве K над простым подполем $\mathbb{F}_p$.

Док-во:

0) $\Phi : K \to K$,

1) $\Phi(a + b) = \Phi(a) + \Phi(b)\ \ \forall\, a, b \in K$,

2) $\Phi(\lambda a) = \Phi(\lambda)\Phi(a) = \lambda\Phi(a)\ \ \forall\, a \in K,\ \forall\, \lambda \in \mathbb{F}_p$.

Утв. 3.

Пусть $f(x) \in \mathbb{F}_p[x],\ p$ - простое число, тогда $(f(x))^p = f(x^p)$.

Док-во:

$f(x) \in \mathbb{F}_p[x] \subset \mathbb{F}_p(x) = Quot\, \mathbb{F}_p[x]$.

Рассмотрим $\Phi : \mathbb{F}_p(x) \to \mathbb{F}_p(x)$ - эндоморфизм Фробениуса поля $\mathbb{F}_p(x)$.

Пусть

$f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n = \sum\limits_{m=0}^{n} a_m x^{n-m},\ a_m \in \mathbb{F}_p,\ m = \overline{0, n}.$

$(f(x))^p = \Phi(f(x)) = \sum\limits_{m=0}^{n} \Phi(a_m)\Phi(x^{n-m}) = \sum\limits_{m=0}^{n} a_m(\Phi(x))^{n-m} = f(\Phi(x)) =$

$= f(x^p)$.

Следствие.

Пусть K - поле, $char\, K = p \neq 0,\ f(x) \in \mathbb{F}_p[x],\ u \in K$ - корень $f(x)$,

тогда u^p - тоже корень $f(x)$.

Док-во:

$f(u) = \{\overline{0}\} \Rightarrow f(u^p) = (f(u))^p = (\overline{0})^p = \overline{0}$.

Утв. 4. Пусть K - конечное поле, $char\, K = p,\ dim_{\mathbb{F}_p} K = n$,
$\Phi : K \to K$ автоморфизм Фробениуса,
тогда $\Phi^n = id,\ \Phi^k \neq id\ \forall\, k = \overline{1, n-1}$.

Док-во:

$|K| = p^n \Rightarrow |K^*| = p^n - 1 \Rightarrow \forall\, a \in K^*\ a^{p^n-1} = 1 \Rightarrow$
$\Rightarrow \forall\, a \in K\ \ a^{p^n} = a \Rightarrow \Phi^n(a) = a \quad \forall\, a \in K \Rightarrow \Phi^n = id.$
Пусть $0 < k < n-1,\ \Phi^k = id$, т.е. $\Phi^k(a) = a \quad \forall a \in K$,
т.е. $a^{p^k} = a \quad \forall a \in K \Leftrightarrow \forall a \in K$ является корнем
многочлена $x^{p^k} - x \in \mathbb{F}_p[x]$ степени p^k.
Следовательно, многочлен степени p^k имеет в поле $K \quad p^n$ различных корней $\Rightarrow p^n \leqslant p^k \Rightarrow n \leqslant k \quad \Rightarrow \Phi^k \neq id \quad \forall\, k = \overline{1, n-1}$.

Note. Утв.4 означает, что $ord\ \Phi = n$ в группе автоморфизмов конечного поля $K:\ |K| = p^n$.

Теорема 2. Пусть $f(x) \in \mathbb{F}_p[x]$ − неприводимый многочлен, $deg\ f(x) = n,\quad u$ − корень $f(x)$ в поле K − расширении $\mathbb{F}_p$, тогда $u, u^p, u^{p^2}, ..., u^{p^{k-1}}$ − различные корни $f(x)$ в K.

Док-во:

u - корень $f(x) \Rightarrow u^p$ - корень $f(x) \Rightarrow u^{p^2} = (u^p)^p$ - корень $f(x)$ и т.д. $\Rightarrow$
$\Rightarrow u^{p^k}$ - корень $f(x) \quad \forall\, k = \overline{0, n-1}$
Заметим, что $u^{p^k} \in \mathbb{F}_p[u] = {}^{\mathbb{F}_p[x]}\!/_{(f(x))} \subset K$.
$f(x)$ - неприводимый многочлен $\Rightarrow \mathbb{F}_p[u]$ - конечное поле, $dim_{\mathbb{F}_p}\mathbb{F}_p[u] = n$.
Рассмотрим $\Phi : \mathbb{F}_p[u] \longmapsto \mathbb{F}_p[u]$ - автоморфизм.
Докажем, что $u^{p^m} \neq u^{p^l}$, при $m \neq l,\ \ m, l = \overline{0, k-1}$.
Заметим, что $u^{p^k} = \Phi^k(u),\ \ k = \overline{0, n-1}$.
Пусть $\Phi^m(u) = \Phi^l(u),\ m > l,\ \ m, l = \overline{0, k-1} \Rightarrow \Phi^{m-l}(u) = u$.
Обозначим $k = m - l$, тогда $\Phi^k(u) = u \Rightarrow \Phi^k(g(u)) = g(\Phi^k(u)) =$
$= g(u)\ \ \forall\, g(u) \in \mathbb{F}_p[u] \Rightarrow \Phi^k = id$ на $\mathbb{F}_p[u],\ 0 < k < n\ \Rightarrow$ все корни u^{p^k}

при разных $k = \overline{0, n-1}$ различны между собой.

Пример:
$f(x) = x^2 + x - 1 \in \mathbb{F}_3[x]$ – неприводимый многочлен, т.к. f(x) не имеет корней в $\mathbb{F}_3$.
$u = [x]$ – корень $f(x)$ в $K = \mathbb{F}_3[u] = {}^{\mathbb{F}_3[x]}/_{(f(x))} \Rightarrow u^3$ – второй корень $f(x)$ в K.
$u^3 = u \cdot u^2 = u(1-u) = u - u^2 = u - (1-u) = 2u - 1 = -u - 1$, т.к. $u^2 + u - 1 = 0$.
$f(x) = (x-u)(x-u^3) = (x-u)(x+u+1)$ – разложение $f(x)$ на линейные множители над K.
Проверка: $f(x) = (x-u)(x+u+1) = x^2 + \cancel{ux} + x - \cancel{ux} - u^2 - u = x^2 + x - 1$.

2 Производная многочлена над произвольным полем

В математическом анализе $\forall\ f(x) \in \mathbb{R}[x]$ определена производная $f'(x) \in \mathbb{R}[x]$. Отображение $D : \mathbb{R}[x] \to \mathbb{R}[x]$, ставящее $\forall\, f(x) \in \mathbb{R}[x]$ в соответствие его производную, обладает свойствами:
1) линейности,
2) $D(fg) = Df \cdot g + f \cdot Dg\ \forall\, f, g \in \mathbb{R}[x]$,
3) $Dx = 1$.

Можно распространить понятие производной на многочлены над любым полем, хотя определение производной из математического анализа не будет иметь смысла в этом случае.

Теорема 3. Пусть K - поле, тогда $\exists!$ отображение $D : K[x] \to K[x]$, обладающее свойствами:
1) линейности, т.е. $\begin{cases} D(f+g) = Df + Dg\ \forall\, f, g \in K[x] \\ D(af) = aDf\ \forall\, f \in K[x],\ \forall\, a \in K \end{cases}$,
2) $D(fg) = Df \cdot g + f \cdot Dg \quad \forall\, f, g \in K[x]$,
3) $Dx = 1$.

Док-во:

(!)Пусть $D : K[x] \to K[x]$, обладающее свойствами 1)-3),
тогда $D(1) = D(1 \cdot 1) = D(1) \cdot 1 + 1D(1) = D(1) + D(1) \Rightarrow D(1) = \overline{0}$.
Докажем по индукции, что $Dx^n = nx^{n-1}$.
При $n = 1 \;\; Dx = 1$ - это свойство 3).
Пусть $Dx^{n-1} = (n-1)x^{n-2}$, тогда $Dx^n = D(x^{n-1}x) =$
$= (Dx^{n-1})x + x^{n-1}Dx = (n-1)x^{n-2}x + x^{n-1} = (n-1)x^{n-1} + x^{n-1} = nx^{n-1} \Rightarrow$
$\Rightarrow D$ однозначно определено на $x^n, \; n = 0, 1, 2, ... \Rightarrow \forall\, f(x) \in K[x]$.

($\exists$) Определим отображение D на $x^n, \; n = 0, 1, 2, ...$:
$D(1) = \overline{0}$,
$D(x^n) = nx^{n-1} \; \forall\, n \in \mathbb{N}$,
распространим его $\forall\, f(x) \in K[x]$ с помощью линейности:
$f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n. \Rightarrow D\, f(x) =$
$= D(a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n) = a_0nx^{n-1} + a_1(n-1)x^{n-1} + ... + a_{n-1}$.
Таким образом, свойства 1) и 3) для отображения D выполнены.

Проверим свойство 2). В силу линейности D достаточно его проверить для $f(x) = x^m, \; g(x) = x^l$.
$D(fg) = D(x^m x^l) = D(x^{m+l}) = (m+l)x^{m+l-1} = mx^{(m-1)+l} + lx^{m+(l-1)} =$
$= mx^{m-1}x^l + x^m lx^{l-1} = D(x^m)x^l + x^m D(x^l) = Df \cdot g + f \cdot Dg$.

Опр.
Производной $f'(x)$ многочлена $f(x) \in K[x]$ назвается $Df(x) \in K[x]$, т.е.
для $f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n \in K[x]$
$f'(x) = a_0nx^{n-1} + a_1(n-1)x^{n-2} + ... + a_{n-1}$.

3 Кратные корни многочленов

Опр. Пусть L, K - поля, $K \subset L$.
$u \in L$ назвается корнем $f(x) \in K[x]$ кратности m, если
$f(x) = (x-u)^m g(x)$, где $g(x) \in K[x] : g(u) \neq \overline{0}$.
Корень кратности $m \geqslant 2$ называется кратным,

а корень кратности $m = 1$ - простым корнем.

Утв. 5. Пусть K, L - поля, $K \subset L$, тогда
$u \in L$ является кратным корнем $f(x) \in K[x] \Leftrightarrow \begin{cases} f(u) = \overline{0} \\ f'(u) = \overline{0} \end{cases}$.

Док-во:
$\Leftarrow$ Пусть u - кратный корень $f(x) \Rightarrow f(x) = (x-u)^2 g(x),\ g(x) \in K[x] \Rightarrow$
$\Rightarrow f'(x) = 2(x-u)g(x) + (x-u)^2 g'(x) \Rightarrow \begin{cases} f(u) = \overline{0} \\ f'(u) = \overline{0} \end{cases}$.
$\Leftarrow$ Пусть $\begin{cases} f(u) = \overline{0} \\ f'(u) = \overline{0} \end{cases}$, но u - простой корень $f(x)$, т.е.
$f(x) = (x-u)g(x),\ g(u) \neq \overline{0} \Rightarrow f'(x) = g(x) + (x-u)g'(x) \Rightarrow$
$\Rightarrow f'(u) = g(u) \neq \overline{0}\ \not\Rightarrow$ u - кратный корень $f(x)$.

Утв. 6. Если K, L - поля, $K \subset L$, $u \in L$, то
u - общий корень $f(x)$, $g(x) \in K[x] \Leftrightarrow u$ - корень $(f(x), g(x)) \in K[x]$.

Док-во:
Пусть $(f(x), g(x)) = d(x)$, тогда $f(x) = d(x)f_1(x),\ g(x) = d(x)g_1(x)$,
$d(x) = f(x)q_1(x) + g(x)q_2(x)$.

$$\Leftarrow \begin{cases} d(x) = f(x)q_1(x) + g(x)q_2(x) \\ f(u) = 0 \\ g(u) = 0 \end{cases} \Rightarrow d(u) = 0,$$

$$\Leftarrow \begin{cases} f(x) = d(x)f_1(x) \\ g(x) = d(x)g_1(x) \\ d(u) = 0 \end{cases} \Rightarrow \begin{cases} f(u) = 0 \\ g(u) = 0 \end{cases}.$$

Следствие. Пусть K, L - поля, $K \subset L$, $u \in L$, тогда u - кратный корень $f(x) \in K[x] \Leftrightarrow u$ - корень $(f(x), f'(x)) \in K[x]$.

Утв. 7. Пусть K - поле, $|K| < \infty$, $char\, K = p$, $f(x) \in K[x]$,
тогда $f'(x) = \overline{0} \Leftrightarrow \exists\, g(x), h(x) \in K[x] : f(x) = g(x^p) = (h(x))^p$.

Док-во:
Пусть $f(x) = a_0 x^n + a_1 x^{n-1} + ... + a_n = \sum\limits_{m=0}^{n} a_m x^{n-m} \Rightarrow$

$\Rightarrow f'(x) = a_0 n x^{n-1} + a_1(n-1)x^{n-2} + ... + a_{n-1} = \sum\limits_{m=0}^{n-1} a_m(n-m)x^{n-m-1}$.
$f'(x) = \overline{0} \Leftrightarrow a_m(n-m) = \overline{0} \ \ \forall\, m = \overline{0, n-1}$
$\Leftarrow$ Если $a_m \neq 0 \Rightarrow n - m = pl \Rightarrow f(x)$ содержит только степени x^p, т.е. $f(x) = g(x^p)$, где $g(x) \in K[x]$.
Рассмотрим эндоморфизм Фробениуса
$\Phi : K(x) \to K(x), \ \ (K(x) = Quot\, K[x])$.
$|K| < \infty \Rightarrow {\Phi|}_K$ - автоморфизм $\Rightarrow \ \exists\, ({\Phi|}_K)^{-1} : K \to K$.

Если $g(x) = b_0 x^s + b_1 x^{s-1} + ... + b_{s-1}x + b_s \in K[x]$, рассмотрим
$h(x) = ({\Phi|}_K)^{-1}(b_0)x^s + ({\Phi|}_K)^{-1}(b_1)x^{s-1} + ... + ({\Phi|}_K)^{-1}(b_s) \in K[x]$.
Тогда $\Phi(h(x)) = (h(x))^p = b_0(x^p)^s + b_1(x^p)^{s-1} + ... + b_s = g(x^p) = f(x)$.
$\Leftarrow$ Очевидно, если $f(x) = (h(x))^p = g(x^p)$, то $f'(x) = \overline{0}$.

Утв. 8. Если K - поле нулевой характеристики или конечное поле, $f(x) \in K[x]$ - неприводимый многочлен, то $f'(x) \neq \overline{0}$.

Док-во:
1) Пусть $K : char\, K = 0$.
$f(x)$ - неприводимый $\Rightarrow deg\ f(x) \geqslant 1 \Rightarrow deg\, f'(x) \geqslant 0 \Rightarrow f'(x) \neq \overline{0}$
2) Пусть $K : |K| < \infty \Rightarrow char\, K = p \neq 0$.
Пусть $f'(x) = \overline{0} \Rightarrow \ \exists\, h(x) \in K[x] : f(x) = (h(x))^p$,
но $f(x)$ - неприводимый $\not\Rightarrow f'(x) \neq \overline{0}$.

Утв. 9. Если K – поле нулевой характеристики или конечное поле, $f(x) \in K[x]$ – неприводимый многочлен, то $f(x)$ не имеет кратных корней ни в каком расширении L поля K.

Док-во:
$$\begin{cases} f(x) - \text{неприводимый} \Rightarrow f'(x) \neq 0 \\ deg\ f'(x) < deg\ f(x) \end{cases} \Rightarrow (f(x), f'(x)) = 1 \Rightarrow$$

$\Rightarrow (f(x), f'(x))$ не имеет корней ни в каком поле $L \supset K \Rightarrow$
$\Rightarrow f(x)$ не имеет кратных корней ни в каком поле $L \supset K$.

Лекция №15

1 Конечные подгруппы мультипликативной группы поля

Лемма 1. Пусть G – группа, $a, b \in G : ab = ba,\ (ord\, a, ord\, b) = 1$, тогда $ord(ab) = ord\, a\ ord\, b$.

Док-во:

Пусть $ord\, a = m,\ ord\, b = k,\ ord(ab) = s$.

$(ab)^{mk} = (a^m)^k (b^k)^m = e \in G \Rightarrow s | mk\ \ (1)$.

$(ab)^s = a^s b^s = e \Rightarrow a^s = b^{-s}$.

$ord\, a^s = \dfrac{m}{(m,s)},\ ord\, b^{-s} = ord\, b^s = \dfrac{k}{(k,s)} \Rightarrow \dfrac{m}{(m,s)} = \dfrac{k}{(k,s)}$. $(*)$

Пусть $d_1 = (m,s) \Rightarrow \begin{cases} m = d_1 \widetilde{m} \\ s = d_1 s_1 \end{cases}$, пусть $d_2 = (k,s) \Rightarrow \begin{cases} k = d_2 \widetilde{k} \\ s = d_2 s_2 \end{cases}$

$(*) \Leftrightarrow \widetilde{m} = \widetilde{k} \Rightarrow \begin{cases} m = d_1 \widetilde{m} \\ k = d_2 \widetilde{k} = d_2 \widetilde{m} \end{cases}$, но $(m,k) = 1 \Rightarrow \begin{cases} \widetilde{m} = 1 \\ \widetilde{k} = 1 \end{cases} \Rightarrow$

$\Rightarrow \begin{cases} m = d_1 \\ k = d_2 \end{cases} \Rightarrow \begin{cases} s = m s_1 \\ s = k s_2 \end{cases} \Rightarrow \begin{cases} m | s \\ k | s \\ (m,k) = 1 \end{cases} \Rightarrow mk | s\ \ (2)$

$(1), (2) \Rightarrow s = mk$, т.е $ord(ab) = ord\, a\ ord\, b$

Теорема 1. Пусть K – поле, $G < K^* : |G| = n < \infty \Rightarrow G$ – циклическая группа. (Любая конечная подгруппа мультипликативной группы поля является циклической).

Док-во:

Пусть $G = \{g_1, g_2, ...g_n\}$

Рассмотрим $m =$НОК$\{ord\, g_1, ord\, g_2, ..., ord\, g_n\}$.

Докажем, что $\exists\, a \in G : ord\, a = m$.

Пусть $m = p_1^{s_1} p_2^{s_2} ... p_k^{s_k}$, p_i – простое число, $p_i \neq p_j$ при $i \neq j,\ \ i, j = \overline{1,k}$.

Из определения $m \Rightarrow \forall i = \overline{1,k}\ \ \exists\, a_i \in G : ord\ a_i = p_i^{s_i} l_i,\ (p_i, l_i) = 1 \Rightarrow$

$\Rightarrow ord\, a_i^{l_i} = p_i^{s_i},\ \ (ord\, a_i^{l_i}, ord\, a_j^{l_j}) = 1$ при $i \neq j,\ \ i, j = 1, k$.

Рассмотрим $a = a_1^{l_1} a_2^{l_2} ... a_k^{l_k}$.
Из леммы $\Rightarrow ord\, a = ord\, a_1^{l_1}\ ord\, a_2^{l_2} ... ord\, a_k^{l_k} = p_1^{s_1} p_2^{s_2} ... p_k^{s_k} = m$.
$ord\, a \leqslant ord\, G \Rightarrow m \leqslant n$ (1)
$m \vdots ord\, g_j,\ j = \overline{1,n} \Rightarrow g^m = 1\ \forall\ g \in G < K^* \Rightarrow$
$\Rightarrow$ многочлен $x^m - 1$ имеет в поле K n корней,
но $deg(x^m - 1) = m \Rightarrow n \leqslant m$ (2)
(1), (2) $\Rightarrow n = m$, т.е. $|G| = ord\, a \Rightarrow G =< a >$.

Следствие. Мультипликативная группа K^* конечного поля K циклическая.

Пример. K - поле, $|K| = p^n \Rightarrow$
$\Rightarrow (K^*, \cdot\,) \simeq \mathbb{Z}_{p^n - 1},\ \ (K, +) \simeq \mathbb{Z}_p \times \mathbb{Z}_p \times ... \times \mathbb{Z}_p$.

2 Поле разложения многочлена

Опр. Пусть K, L - поля, $K \subset L$, $u_1, u_2, ..., u_n \in L$, тогда подполем $K(u_1, u_2, ..., u_n)$, порождённым над K элементами $u_1, u_2, ..., u_n$, называется $K(u_1, u_2, ..., u_n) = Quot\, K[u_1, u_2, ..., u_n]$.

Note. $K(u_1, u_2, ..., u_n)$ - наименьшее по включению подполе L, содержащее элементы $u_1, u_2, ..., u_n$.

Если $u \in L$ - алгебраический над K элемент, то $K(u) = K[u]$.

Утв. 1. Если K - поле, $u_1, u_2, ..., u_n$ - алгебраические над K элементы, $L = K(u_1, u_2, ..., u_n)$, то L - конечное расширение поля K.

Док-во:
Докажем, что $K(u_1, u_2, ..., u_m) = K(u_1, u_2, ..., u_{m-1})(u_m)$.
$K(u_1, u_2, ..., u_{m-1})(u_m)$ - множество рациональных функций
от u_m с рациональными коэффициентами из $K(u_1, u_2, ..., u_{m-1})$.
Приведя эти коэффициенты к общему знаменателю,
увидим, что $K(u_1, u_2, ..., u_{m-1})(u_m) \subset K(u_1, u_2, ..., u_m)$.

$K(u_1, u_2, ..., u_{m-1})(u_m)$ - поле, содержащее $u_1, u_2, ..., u_{m-1}, u_m$,
но $K(u_1, u_2, ..., u_m)$ - наименьшее поле, содержащее эти элементы $\Rightarrow$
$\Rightarrow K(u_1, u_2, ..., u_{m-1})(u_m) = K(u_1, u_2, ..., u_m)$.

Если u_m - алгебраический элемент над K, то u_m - алгебраический элемент над $K(u_1, u_2, ..., u_{m-1}) \Rightarrow$
$\Rightarrow K(u_1, u_2, ..., u_m)$ является конечным расширением $K(u_1, u_2, ..., u_{m-1})$.
В цепочке расширений
$K \subset K(u_1) \subset K(u_1, u_2) \subset ... \subset K(u_1, u_2, ..., u_m) \subset ... \subset K(u_1, u_2, ..., u_n) = L$
каждое расширение является конечным над предыдущим подполем $\Rightarrow$
$\Rightarrow L = K(u_1, u_2, ..., u_n)$ является конечным расширением поля K.

Опр. Расширение L поля K называется полем разложения многочлена $f(x) \in K[x]$, если L - наименьшее по включению поле, над которым $f(x)$ раскладывается на линейные множители.

Note. Поле L разложения многослена $f(x) \in K[x]$ порождается над K его корнями.

Теорема 2. Пусть K - поле, тогда для любого многочлена $f(x) \in K[x]$ существует поле разложения.

Док-во:

Построим поле L - поле разложения $f(x) \in K[x]$.
Разложим $f(x)$ на неприводимые множители.

Если все эти множители первой степени, то $L = K$.

Если среди неприводимых множителей $f(x)$ есть многочлен $f_1(x) : deg\, f_1(x) > 1$, то присоединим к K корень этого многочлена α_1, получим $K_1 = K[\alpha_1] = {}^{K[x]}/_{(f_1(x))}$, $K \subset K_1$.

Разложим $f(x) \in K[x] \subset K_1[x]$ на неприводимые множители над $K_1 = K[\alpha_1]$. Среди них есть линейный множитель $(x - \alpha_1)$.

Если все неприводимые множители теперь имеют степень 1,
то $L = K[\alpha_1]$.

Если среди неприводимых множителей есть $f_2(x) \in K_1[x]$:
$deg\, f_1(x) > 1$, то присоединяя к K_1 его корень α_2, получим

$K_2 = K_1[\alpha_2] = {}^{K_1[x]}/_{(f_2(x))}$, $K_2 = K_1[\alpha_2] = K[\alpha_1, \alpha_2]$ и т.д.
Получим цепочку расширений $K = K_0 \subset K_1 \subset ... \subset K_{m-1} \subset K_m \subset ...$,
где $K_m = K_{m-1}[\alpha_m]$, α_m - корень неприводимого многочлена
$f_m(x) \in K_{m-1}[x] : deg\, f_m(x) > 1$, $f_m(x)$ - делитель $f(x)$.

$\exists\, s \in \mathbb{N},\ s \leqslant deg\, n : L = K[\alpha_1, \alpha_2, ..., \alpha_s]$ - поле разложения $f(x)$.

Следствие 1.
Поле разложения $f(x) \in K[x]$ - конечное расширение поля K.

Следствие 2.
Если K - конечное поле, то поле разложения $f(x) \in K[x]$ - конечное поле.

Note. Если $F, \widetilde{F}$ - поля, $\varphi : F \to \widetilde{F}$ - гомоморфизм,
то φ можно продолжить до гомоморфизма $\varphi : F[x] \to \widetilde{F}[x]$,
определив $\forall\, p(x) = a_0x^m + a_1x^{m-1} + ... + a_m \in F[x]$
$\varphi(p(x)) = \varphi(a_0x^m + a_1x^{m-1} + ... + a_m) = \varphi(a_0)x^m + \varphi(a_1)x^{m-1} + ... + \varphi(a_m) \in \widetilde{F}[x]$.
Очевидно, что $\varphi : F[x] \to \widetilde{F}[x]$ и φ сохраняет операции сложения и умножения многочленов.

Обозначим $\varphi(p(x)) = \widetilde{p}(x)$.

Лемма 2. Пусть $F, \widetilde{F}$ - поля, $\varphi : F \to \widetilde{F}$ - гомоморфизм.
$F[\alpha]$ - расширение поля F, полученное присоединением корня неприводимого многочлена $f(x) \in F[x]$.

Тогда
1) если $\Psi : F[\alpha] \to \widetilde{F}$ - гомоморфизм : ${}^{\Psi}|_F = \varphi$, $\beta = \Psi(\alpha)$, то $\widetilde{f}(\beta) = \overline{0}$;
2) если $\beta \in \widetilde{F}$ - корень $\widetilde{f}(x) \in \widetilde{F}[x]$, то отображение $\Psi : F[\alpha] \to \widetilde{F}$,
определённое по правилу $\Psi(p(\alpha)) = \widetilde{p}(\beta)\ \forall\, p(\alpha) \in F[\alpha]$,
является гомоморфизмом и ${}^{\Psi}|_F = \varphi$.

Док-во:
1) Пусть $\Psi : F[\alpha] \to \widetilde{F}$ - гомоморфизм : ${}^{\Psi}|_F = \varphi$. $\Rightarrow$
$\Rightarrow \Psi(p(\alpha)) = \Psi(a_0\alpha^m + a_1\alpha^{m-1} + ... + a_m) =$
$= \Psi(a_0)(\Psi(\alpha))^m + \Psi(a_1)(\Psi(\alpha))^{m-1} + ... + \Psi(a_m) =$
$= \varphi(a_0)\beta^m + \varphi(a_1)\beta^{m-1} + ... + \varphi(a_m) = \widetilde{p}(\beta)$, где $\beta = \Psi(\alpha)$. $\Rightarrow$

$\Rightarrow$ т.к. $f(\alpha) = \overline{0} \Rightarrow \Psi(f(\alpha)) = \widetilde{f}(\beta) = \overline{0}$.

2) Покажем, что Ψ определено корректно.
Пусть $p_1(\alpha) = p_2(\alpha) \Leftrightarrow p_1(x) = p_2(x) + f(x)g(x)$, где $g(x) \in F[x] \Rightarrow$
$\Rightarrow \widetilde{p_1}(x) = \widetilde{p_2}(x) + \widetilde{f}(x)\widetilde{g}(x)$, где $\widetilde{g}(x) \in \widetilde{F}(x) \Rightarrow \widetilde{p_1}(\beta) = \widetilde{p_2}(\beta) \Leftrightarrow$
$\Leftrightarrow \Psi(p_1(\alpha)) = \Psi(p_2(\alpha))$.

Ясно, что $\Psi : F[\alpha] \to \widetilde{F}$ является гомоморфизмом и $\Psi|_F = \varphi$.

Опр. Пусть L_1, L_2 - расширения поля K, $\varphi : L_1 \to L_2$ гомоморфизм. φ называется гомоморфизмом над K, если $\varphi|_K = id$.

Теорема 3. Пусть K - поле, $f(x) \in K[x]$, тогда поле разложения многочлена $f(x)$ единственно с точностью до изоморфизма над K.

Док-во:
Пусть L - поле разложения $f(x) \in K[x]$, построенное в теореме 2,
а $\widetilde{L}$ - другое поле разложения $f(x)$.
$K = K_0 \subset K_1 \subset ... \subset K_{m-1} \subset K_m \subset ... \subset K_s = L$.
Построим последовательность гомоморфизмов
$\varphi_m : K_m \to \widetilde{L}$, $m = 0, 1, ..., s$ такую, что $\varphi_0 = id$, $\varphi_m|_{K_{m-1}} = \varphi_{m-1}$.
$K_m = K_{m-1}[\alpha_m]$, где α_m - корень неприводимого многочлена
$f_m(x) \in K_{m-1}[x]$, $f(x) \vdots f_m(x)$ над K_{m-1}.

Если гомоморфизм $\varphi_{m-1} : K_{m-1} \to \widetilde{L}$ уже построен и продолжен до гомоморфизма $\varphi_{m-1} : K_{m-1}[x] \to \widetilde{L}[x]$,
$\widetilde{p}(x) = \varphi_{m-1}(p(x))$ $\forall\, p(x) \in K_{m-1}[x]$, то $\widetilde{f}(x) = f(x) \vdots \widetilde{f_m}(x)$ над $\widetilde{L}$.
$f(x)$ раскладывается на линейные множители над $\widetilde{L} \Rightarrow$
$\Rightarrow \exists\, \beta_m \in \widetilde{L} : \widetilde{f_m}(\beta_m) = \overline{0}$.

Положим $\varphi_m(p(\alpha_m)) = \widetilde{p}(\beta_m)$ $\forall\, p(\alpha_m) \in K_{m-1}[\alpha_m]$.
Из леммы 2 $\Rightarrow \varphi_m : K_m \to \widetilde{L}$ - гомоморфизм, $\varphi_m|_{K_{m-1}} = \varphi_{m-1}$, $\varphi_m|_K = \mathrm{id}$.

$L = K_s = K[\alpha_1, \alpha_2, ..., \alpha_s]$.
$\varphi_s : L \longmapsto \widetilde{L}$ гомоморфизм нетривиальный, т.к. $\varphi_s|_K = id \Rightarrow$
$\Rightarrow$ Поскольку $L -$ поле, $\varphi_s -$ мономорфизм. $\Rightarrow$
$\Rightarrow$ По теореме о гомоморфизме $L \simeq Im\,\varphi_s \Rightarrow$
$\Rightarrow Im\,\varphi_s \simeq L$ является подполем поля разложения $\widetilde{L}$, над которым $f(x)$

раскладывается на линейные множители, но $\widetilde{L}$ - наименьшее такое поле $\Rightarrow Im\,\varphi_s = \widetilde{L} \Rightarrow \widetilde{L} \simeq L$.

Примеры:

(1) $f(x) = x^3 - 2 \in \mathbb{F}_7[x]$ − неприводимый многочлен, т.к. $deg\, f(x) = 3$ и $f(x)$ не имеет корней в $\mathbb{F}_7$.
Рассмотрим $\mathbb{F}_7[\alpha] \simeq {}^{\mathbb{F}_7[x]}/_{(x^3-2)}$, $\alpha = [x]$ − корень $f(x) = x^3 - 2 \Rightarrow$
$\Rightarrow \alpha, \alpha^7, \alpha^{49}$ − корни $f(x)$, различные между собой.
$\alpha, \alpha^7, \alpha^{49} \in \mathbb{F}_7[\alpha] \Rightarrow \mathbb{F}_7[\alpha]$ − поле, над которым $f(x)$ раскладывается на линейные множители, и $\mathbb{F}_7[\alpha]$ − минимальное из таких полей, поскольку $\mathbb{F}_7[\alpha]$ − наименьшее поле, содержащее α. $\Rightarrow$
$\Rightarrow \mathbb{F}_7[\alpha] \simeq {}^{\mathbb{F}_7[x]}/_{(x^3-2)}$ − поле разложения $f(x)$.
$dim_{\mathbb{F}_7}\mathbb{F}_7[\alpha] = deg\, f(x) = 3 \Rightarrow$ Поле разложения $f(x) = x^3 - 2$ над $\mathbb{F}_7$ имеет степень расширения 3.
Разложим $f(x)$ на линейные множители над $\mathbb{F}_7[\alpha]$.
$f(x) = (x-\alpha)(x-\alpha^7)(x-\alpha^{49}) = (x-\alpha)(x+3\alpha)(x-2\alpha)$.
$\alpha^3 = 2 \Rightarrow \alpha^6 = -3 \Rightarrow \alpha^7 = -3\alpha,\ \alpha^{49} = (\alpha^6)^8\alpha = (-3)^8\alpha = 2\alpha$.
Сделаем проверку:
$f(x) = (x-\alpha)(x+3\alpha)(x-2\alpha) = (x-\alpha)(x^2+\alpha x+\alpha^2) =$
$= x^3 + \alpha x^2 + \alpha^2 x - \alpha x^2 - \alpha^2 x - \alpha^3 = x^3 - 2$

(2) $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ − неприводимый многочлен, т.к. $deg\, f(x) = 3$ и $f(x)$ не имеет корней в $\mathbb{Q}$.
Рассмотрим $\mathbb{Q}[\alpha] \simeq {}^{\mathbb{Q}[x]}/_{(x^3-2)}$, $\alpha = \sqrt[3]{2}$ − корень $f(x)$, $\alpha^3 = 2$.
$\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{2^2} : a, b, c \in \mathbb{Q}\} \subset \mathbb{R}$.
$f(x) = x^3 - (\sqrt[3]{2})^3 = (x - \sqrt[3]{2})(x^2 + x\sqrt[3]{2} + \sqrt[3]{2^2})$.
Квадратный трехчлён $x^2 + x\sqrt[3]{2} + \sqrt[3]{2^2}$ не имеет действительных корней, поскольку $D = -3\sqrt[3]{2^2} < 0$. $\Rightarrow f(x)$ не раскладывается на линейные множители над $\mathbb{Q}[\alpha] \subset \mathbb{R}$.
Рассмотрим $x^2 + x\sqrt[3]{2} + \sqrt[3]{2^2} = x^2 + \alpha x + \alpha^2$ над $\mathbb{Q}[\alpha]$, этот многочлен имеет степень 2 и не имеет корней в $\mathbb{Q}[\alpha] \Rightarrow$ он неприводим над $\mathbb{Q}[\alpha]$.
Рассмотрим $\mathbb{Q}[\alpha][\beta] \simeq {}^{\mathbb{Q}[\alpha][x]}/_{(x^2+\alpha x+\alpha^2)} = \mathbb{Q}[\alpha, \beta]$,

где $\beta^2 + \alpha\beta + \alpha^2 = 0$,
$\beta = \dfrac{-\alpha + i\alpha\sqrt{3}}{2}$ – корень $x^2 + \alpha x + \alpha^2,\ \beta \in \mathbb{Q}[\alpha, \beta] \subset \mathbb{C}$,
$\overline{\beta} = \dfrac{-\alpha - i\alpha\sqrt{3}}{2}$ – второй корень $x^2 + \alpha x + \alpha^2,\ \overline{\beta} \in \mathbb{Q}[\alpha, \beta] \subset \mathbb{C}$,
$\overline{\beta} = -\alpha - \beta \Rightarrow \mathbb{Q}[\alpha, \beta]$ – поле разложения $f(x)$, т.к. $\mathbb{Q}[\alpha, \beta]$ – наименьшее поле, над которым $f(x)$ раскладывается на линейные множители.
$f(x) = (x - \alpha)(x - \beta)(x - \overline{\beta}) = (x - \alpha)(x - \beta)(x + \alpha + \beta)$ – разложение на линейные множители над $\mathbb{Q}[\alpha, \beta]$.
Сделаем проверку:
$f(x) = (x - \alpha)(x - \beta)(x + \alpha + \beta) = (x - \alpha)(x^2 + \alpha x + \cancel{\beta x} - \cancel{\beta x} - \alpha\beta - \beta^2) =$
$= (x - \alpha)(x^2 + \alpha x + \alpha^2) = x^3 - \alpha^3 = x^3 - 2$.
$\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset \mathbb{Q}[\alpha, \beta]$
$dim_{\mathbb{Q}}\mathbb{Q}[\alpha] = 3$, т.к. $\mathbb{Q}[\alpha] \simeq {\mathbb{Q}[x]}/{(x^3 - 2)}$, $\quad deg(x^3 - 2) = 3$.
$dim_{\mathbb{Q}[\alpha]}\mathbb{Q}[\alpha, \beta] = 2$, т.к. $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\alpha][\beta] \simeq {\mathbb{Q}[\alpha][x]}/{(x^2 + \alpha x + \alpha^2)}$,
$deg(x^2 + \alpha x + \alpha^2) = 2$.
$dim_{\mathbb{Q}}\mathbb{Q}[\alpha, \beta] = dim_{\mathbb{Q}}\mathbb{Q}[\alpha]\ dim_{\mathbb{Q}[\alpha]}\mathbb{Q}[\alpha, \beta] = 3 \cdot 2 = 6$.
Поле разложения многочлена $f(x) = x^3 - 2$ над полем $\mathbb{Q}$ имеет степень расширения 6.

Лекция №16

1 Существование и единственность конечного поля порядка p^n - поля Галуа.

Лемма. Пусть $\varphi : K \longmapsto K$ – нетривиальный эндоморфизм поля K, $L = \{a \in K : \varphi(a) = a\}$ – множество неподвижных точек φ, тогда L – подполе K.

Док-во:

$L \subset K \Rightarrow$ все свойства K, выражаемые тождествами, выполняются в L.

1) $\varphi(\overline{0}) = \overline{0} \Rightarrow \overline{0} \in L$,

2) $a, b \in L$, т.е. $\begin{cases} \varphi(a) = a \\ \varphi(b) = b \end{cases} \Rightarrow \varphi(a+b) = \varphi(a) + \varphi(b) = a + b \Rightarrow a + b \in L$,

3) $a \in L$, т.е. $\varphi(a) = a \Rightarrow \varphi(-a) = -\varphi(a) = -a \Rightarrow (-a) \in L$,

4) $a, b \in L$, т.е. $\begin{cases} \varphi(a) = a \\ \varphi(b) = b \end{cases} \Rightarrow \varphi(ab) = \varphi(a)\,\varphi(b) = ab \Rightarrow ab \in L$,

5) $\varphi(1) = 1$, т.к. φ – нетривиальный эндоморфизм поля $K \Rightarrow 1 \in L$,

6) $\varphi(1) \neq \varphi(\overline{0}) \Rightarrow 0 \neq 1$, т.е. $|L| > 1$,

7) $\forall\, a \in L \setminus \{\overline{0}\}$ $1 = \varphi(1) = \varphi(aa^{-1}) = a\varphi(a^{-1}) \Rightarrow \varphi(a^{-1}) = a^{-1} \Rightarrow$
$\Rightarrow a^{-1} \in L$.

$1) - 7) \Rightarrow L$ – подполе K.

Теорема 1. Для любого простого числа p и любого натурального числа n существует единственное с точностью до изоморфизма поле, состоящее из p^n элементов.

Док-во:

$\textcircled{!}$Пусть K – поле: $|K| = p^n$. Докажем, что такое поле единственно с

точностью до изоморфизма.
K – поле $\Rightarrow |K^*| = p^n - 1 \Rightarrow \forall a \in K^* \ \ a^{p^n-1} = 1 \Rightarrow \forall a \in K \ \ a^{p^n} = a$, т.е.
$\forall\, a \in K$ является корнем многочлена $q(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.
$deg\, q(x) = p^n \Rightarrow q(x)$ имеет не более p^n корней. $\Rightarrow$
$\Rightarrow$ Множество корней $q(x)$ совпадает с полем K. $\Rightarrow$
$\Rightarrow K$ – минимальное поле, над которым $q(x)$ раскладывается на линейные множители, т.е. K – поле разложения многочлена $q(x) \in \mathbb{F}_p[x] \Rightarrow$
$\Rightarrow$ Поле разложения K единственно с точностью до изоморфизма над $\mathbb{F}_p$, но $\mathbb{F}_p$ – простое подполе K, следовательно любой изоморфизм K оставляет на месте все элементы $\mathbb{F}_p$, т.е. является изоморфизмом над $\mathbb{F}_p \Rightarrow$
$\Rightarrow \ K$ единственно с точностью до изоморфизма.
($\exists$) Докажем, существание поля $K : |K| = p^n$.
Рассмотрим многочлен $q(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.
$\exists$ поле разложения этого многослена K (конечное поле).
В K лежат все корни многочлена $q(x)$.
Множество его корней $L = \{a \in K : a^{p^n} - a = 0\} = \{a \in K : \Phi^n(a) = a\}$ есть множество неподвижных точек автоморфизма Φ^n, где Φ - автоморфизм Фробениуса поля K.
Из леммы $\Rightarrow \ L$ - подполе K.
Над $L\ q(x)$ раскладывается на линейные множители $\Rightarrow$
$\Rightarrow K = L \Rightarrow |K|$ равен числу различных корней $q(x)$.
$q'(x) = p^n x^{p^n-1} - 1 = -1 \Rightarrow q'(x)$ не имеет корней ни в каком поле $\Rightarrow$
$\Rightarrow q(x)$ не имеет кратных корней ни в каком поле $\Rightarrow$
$\Rightarrow \ |K| = deg\, q(x) = p^n$.

Опр. Любое конечное поле $K : |K| = p^n$ называется полем Галуа и обозначается $GF(p^n)$ или $\mathbb{F}_{p^n}$.

Следствие. Если $f(x)$, $g(x) \in \mathbb{F}_p[x]$ - неприводимые многочлены : $deg\, f(x) = deg\, g(x)$, то $\mathbb{F}_p[x]/_{(f(x))} \simeq \mathbb{F}_p[x]/_{(g(x))}$.

Док-во:
Пусть $deg\, f(x) = deg\, g(x) = n$.
Тогда $\mathbb{F}_p[x]/_{(f(x))}$ и $\mathbb{F}_p[x]/_{(g(x))}$ - поля, содержащие p^n элементов.

Пример.

$f(x) = x^2 + 1,\ g(x) = x^2 + x - 1 \in \mathbb{F}_3[x]$ - неприводимые многочлены.

$\mathbb{F}_3[\alpha] = \{a + b\alpha : \alpha^2 + 1 = \overline{0},\ a, b \in \mathbb{F}_3\} \simeq {}^{\mathbb{F}_3[x]}/_{(x^2+1)}$

$\mathbb{F}_3[\gamma] = \{a + b\gamma : \gamma^2 + \gamma - 1 = \overline{0},\ a, b \in \mathbb{F}_3\} \simeq {}^{\mathbb{F}_3[x]}/_{(x^2+x-1)}$

$\mathbb{F}_3[\alpha] \simeq \mathbb{F}_3[\gamma]$.

Построим изоморфизм $\varphi : \mathbb{F}_3[\alpha] \to \mathbb{F}_3[\gamma]$ явно.

Для этого найдём корень многочлена $x^2 + 1$ в поле $\mathbb{F}_3[\gamma]$.

$(a + b\gamma)^2 + 1 = \overline{0}$

$a^2 + 2ab\gamma + b^2\gamma^2 + 1 = \overline{0}$

$a^2 + 2ab\gamma + b^2(1 - \gamma) + 1 = \overline{0}$

$a^2 + b^2 + 1 + \gamma(2ab - b^2) = \overline{0}.$

$$\begin{cases} a^2 + b^2 + 1 = \overline{0} \\ b(2a - b) = \overline{0} \end{cases} \quad \begin{cases} \left[\begin{array}{l} b = \overline{0} \quad \varnothing \\ b = -a \end{array}\right. \\ a^2 + b^2 = -1 \end{cases} \quad \begin{cases} b = -a \\ 2a^2 = -1 \end{cases} \quad \begin{cases} b = -a \\ a^2 = 1 \end{cases}$$

$$\left[\begin{array}{l} \begin{cases} a = 1 \\ b = -1 \end{cases} \\ \qquad\qquad \Rightarrow 1 - \gamma,\ -1 + \gamma - \text{ корни} \quad f(x) = x^2 + 1 \ \text{ в } \ \mathbb{F}_3[\gamma]. \\ \begin{cases} a = -1 \\ b = 1 \end{cases} \end{array}\right.$$

Положим $\varphi(1) = 1, \varphi(\alpha) = 1 - \gamma$.

Определим $\varphi : \mathbb{F}_3[\alpha] \longmapsto \mathbb{F}_3[\alpha]$.

$\varphi -$ гомоморфизм $\Rightarrow \varphi(p(\alpha)) = p(\varphi(\alpha)) = p(1 - \alpha) \quad \forall\, p(\alpha) \in \mathbb{F}_3[\alpha]$.

$f(\alpha) = \overline{0},\ \ \varphi(f(\alpha)) = f(\varphi(\alpha)) = \varphi(\alpha^2+1) = (1-\gamma)^2+1 = 1-2\gamma+\gamma^2+1 =$

$= \gamma^2 + \gamma - 1 = \overline{0}.$

φ определено корректно, т.к.

$p_1(\alpha) = p_2(\alpha) \Leftrightarrow p_1(\alpha) = p_2(\alpha) + f(\alpha)q(\alpha) \Rightarrow$

$\Rightarrow \varphi(p_1(\alpha)) = \varphi(p_2(\alpha)) + \varphi(f(\alpha))\varphi(q(\alpha)) \Rightarrow$

$\Rightarrow p_1(\varphi(\alpha)) = p_2(\varphi(\alpha)) + f(\varphi(\alpha))q(\varphi(\alpha)) \Rightarrow p_1(1 - \gamma) = p_2(1 - \gamma).$

φ сохраняет операции сложения и умножения.

2 Существование над полем $\mathbb{F}_p$ неприводимых многочленов любой положительной степени

Теорема 2. Для любого простого p и любого натурального n существует неприводимый многочлен степени n над $\mathbb{F}_p$.

Док-во:

Существует поле $\mathbb{F}_{p^n}$, его мультипликативная группа $\mathbb{F}_{p^n}^*$ - циклическая. Пусть $\mathbb{F}_{p^n}^* = <\alpha> \Rightarrow \mathbb{F}_{p^n} = \mathbb{F}_p[\alpha] \Rightarrow \exists\, m_\alpha(x) \in \mathbb{F}_p[x] : m_\alpha(x)$ - неприводимый многочлен и $deg\, m_\alpha(x) = n$.

Note. Над другими полями могут не существовать неприводимые многочлены любой положительной степени. Например, над $\mathbb{C}$ все неприводимые многочлены имеют степень один, а над $\mathbb{R}$ - один или два.