Краткая теория к экзамену по высшей алгебре 19-20 июня 2015

Чудинов Никита (группа 14-4)

1 Лекция 1

Определение 1.1. *Множество с бинарной операцией* — это множество M с заданным отображением

$$M \times M \to M, \quad (a, b) \mapsto a \circ b.$$

Определение 1.2. Множество с бинарной операцией $(M, \circ)$ называется *полугруппой*, если данная бинарная операция ассоциативна, то есть

$$a \circ (b \circ c) = (a \circ b) \circ c, \forall a, b, c \in M.$$

Определение 1.3. Полугруппа $(S, \circ)$ называется *моноидом*, если в ней есть *нейтральный элемент* $e \in S$, такой, что

$$\forall a \in S: \quad e \circ a = a \circ e = a.$$

Определение 1.4. Моноид называется *группой*, если для каждого элемента $a \in S$ найдётся *обратный элемент* a^{-1}, такой, что

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

Определение 1.5. Группа G называется *коммутативной* или *абелевой*, если групповая операция коммутативна, то есть

$$a \circ b = b \circ a, \forall a, b \in G.$$

Определение 1.6. *Порядок* группы G — это количество элементов в G. Группа называется конечной, если её порядок конечен, и бесконечной иначе. Обозначается $|G|$.

Определение 1.7. Подмножество H группы G называется *подгруппой*, если

$$|H| > 0, \quad a \circ b^{-1} \in H, \forall a, b \in H.$$

Предложение 1.1. *Всякая подгруппа в $(\mathbb{Z}, +)$ имеет вид $k\mathbb{Z}$ для некоторого $k \in \mathbb{N}$*

Определение 1.8. Пусть G — группа и $g \in G$. *Циклической подгруппой*, порождённой элементом g называется подмножество

$$\{g^n \mid n \in \mathbb{Z}\} \in G.$$

Элемент g называется *порождающим* или *образующим* для этой группы $\langle g \rangle$.

Определение 1.9. Пусть G — группа и $g \in G$. *Порядком* элемента g называется такое наименьшее натуральное число m, что $g^m = e$. Если такого натурального числа не существует, то говорят, что порядок g равен бесконечности. Обозначение: $\mathrm{ord}(g)$.

Предложение 1.2. *Пусть G — группа и $g \in G$. Тогда* $\mathrm{ord}(g) = |\langle g \rangle|$.

Определение 1.10. Группа G называется *циклической*, если

$$\exists\, g \in G, \quad G = \langle g \rangle.$$

Определение 1.11. Пусть G — группа, $H \subseteq G$ — подгруппа и $g \in G$. *Левым смежным классом* элемента g группы G по подгруппе H называется подмножество

$$gH = \{gh \mid h \in H\}.$$

Определение 1.12. Пусть G — группа, $H \subseteq G$ — подгруппа. *Индексом* подгруппы H в группе G называется число левых смежных классов G по H. Обозначается $[G : H]$.

Теорема (Лагранж). *Пусть G — конечная группа и $H \subseteq G$ — подгруппа. Тогда*

$$|G| = |H| \cdot [G : H].$$

2 Лекция 2

Определение 2.1. Подгруппа H группы G называется *нормальной*, если

$$gH = Hg, \forall g \in G.$$

Предложение 2.1. *Для подгруппы $H \subseteq G$ следующие условия эквивалентны:*

1. *H нормальна;*
2. *$gHg^{-1} \subseteq H, \forall g \in G$;*
3. *$gHg^{-1} = H, \forall g \in G$;*

Определение 2.2. Множество G/H с указанной операцией называется *факторгруппой* группы G по нормальной подгруппе H.

Определение 2.3. Пусть G и F — группы. Отображение $\varphi : G \to F$ называется *гомоморфизмом*, если

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

Определение 2.4. Гомоморфизм групп $\varphi : G \to F$ называется *изоморфизмом*, если отображение φ биективно.

Определение 2.5. Группы G и F называют *изоморфными*, если между ними есть изоморфизм. Обозначение: $G \cong F$.

Теорема. *Всякая бесконечная циклическая группа G изоморфна группе $(\mathbb{Z}, +)$.*

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

Определение 2.6. С каждым гомоморфизмом групп $\varphi : G \to F$ связаны его *ядро*

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = e_F\}$$

и *образ*

$$\mathrm{im}(\varphi) = \{a \in F \mid \exists g \in G : \varphi(g) = a\}.$$

Предложение 2.2. *Пусть $\varphi : G \to F$ — гомоморфизм групп. Тогда подгруппа $\ker(\varphi)$ нормальна в G.*

Теорема (о гомоморфизме)**.** *Пусть $\varphi : G \to F$ — гомоморфизм групп. Тогда группа $\mathrm{im}(\varphi)$ изоморфна факторгруппе $G/\ker(\varphi)$.*

Определение 2.7. *Центр* группы G — это подмножество

$$Z(G) = \{a \in G \mid ab = ba, \forall b \in G\}.$$

Предложение 2.3. *Центр $Z(G)$ является нормальной подгруппой группы G.*

Определение 2.8. *Прямым произведением* групп $G_1, \dots, G_m$ называется множество

$$G_1 \times \dots \times G_m = \{(g_1, \dots, g_m) \mid g_1 \in G_1, \dots, g_m \in G_m\}.$$

Теорема (о факторизации и сомножителях)**.** *Пусть $H_1, \dots, H_m$ — нормальные подгруппы в группах $G_1, \dots, G_m$ соответственно. Тогда $H_1 \times \cdot \times H_m$ — нормальная подгруппа в $G_1 \times \dots \times G_m$ и имеет место изоморфизм групп*

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

Теорема. *Пусть $n = ml$ — разложение натурального числа n на два взаимно простых множителя. Тогда имеет место изоморфизм групп*

$$\mathbb{Z}_n \cong \mathbb{Z}_m \times \mathbb{Z}_l.$$

3 Лекция 3

Определение 3.1. Абелева группа A называется *конечно порождённой*, если найдутся такие элементы $a_1, \dots, a_n \in A$, что всякий элемент $a \in A$ представим в виде $a = s_1a_1 + \dots + s_na_n$ для некоторых целых чисел $s_1, \dots, s_n$. При этом элементы $a_1, \dots, a_n$ называются *порождающими* или *образующими* группы A.

Определение 3.2. Конечно порождённая абелева группа A называется *свободной*, если в ней существует *базис*, то есть такой набор элементов $a_1, \dots, a_n$, что каждый элемент $a \in A$ единственным образом представим в виде $a = s_1a_1 + \dots + s_na_n$, где $s_1, \dots, s_n \in \mathbb{Z}$. При этом число n называется рангом свободной абелевой группы A и обозначается $\mathrm{rk}A$.

Предложение 3.1. *Любые два базиса свободной группы содержат одинаковое число элементов.*

Предложение 3.2. *Всякая свободная абелева группа ранга n изоморфна группе $\mathbb{Z}^n$.*

Теорема. *Всякая подгруппа N свободной абелевой группы L ранга n является свободной абелевой группой ранга $\leqslant n$.*

Теорема (о согласованных базисах)**.** *Для всякой подгруппы N свободной абелевой группы L ранга n найдётся такой базис $e_1, \dots, e_n$ группы L и такие натуральные числа $u_1, \dots, u_m, m \leqslant n$, что $u_1e_1, \dots, u_me_m$ — базис группы N и $u_i|u_{i+1}$ при $i = 1, \dots, m-1$.*

Предложение 3.3. *Пусть $e'_1, \dots, e'_n$ — некоторый набор элементов из $\mathbb{Z}^n$. Выразив эти элементы через стандартный базис $e_1, \dots, e_n$, мы можем записать*

$$(e'_1, \dots, e'_n) = (e_1, \dots, e_n)C,$$

где C — целочисленная квадратная матрица порядка n.

Элементы $e'_1, \dots, e'_n$ составляют базис группы $\mathbb{Z}^n$ тогда и только тогда, когда $\det C = \pm 1$.

Определение 3.3. *Целочисленными элементарными преобразованиями строк* матрицы называются преобразования следующих трёх типов:

1. Прибавление к одной строке другой, умноженной на целое число;
2. Перестановка двух строк;
3. Умножение одной строки на -1.

Аналогично определяются *целочисленные элементарные преобразования столбцов* матрицы.

Предложение 3.4. *Всякую прямоугольную матрицу $C = (c_{ij}$ размера $n \times m$ назовём диагональной и обозначим $diag(u_1, \dots, u_p)$, если $c_{ij} = 0$ при $i \neq j$ и $c_{ii} = u_i$ при $i = 1, \dots, p$, где $p = min(n, m)$.*

4 Лекция 4

Определение 4.1. Конечная абелева группа называется *примарной*, если её порядок равен p^k для некоторого простого числа p.

Теорема. *Всякая конечно порождённая абелева группа A разлагается в прямую сумму примарных и бесконечных циклических подгрупп, то есть*

$$A \cong \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z},$$

где $p_1, \dots, p_s$ — простые числа (необязательно попарно различные), а $k_1, \dots, k_s \in \mathbb{N}$. Кроме того, число бесконечных циклических слагаемых, а также число и порядки примарных циклических слагаемых определено однозначно.

Предложение 4.1. *Всякая конечная абелева группа разлагается в прямую сумму примарных циклических подгрупп, причем число и порядки примарных циклических слагаемых определено однозначно.*

Определение 4.2. *Экспонентой* конечной абелевой группы A называется число $\exp A$, равное наименьшему общему кратному порядков элементов из A.

Предложение 4.2. *Конечная абелева группа A является циклической тогда и только тогда, когда $\exp A = |A|$.*

5 Лекция 5

Определение 5.1. *Действием* группы G на множестве X называется отображение $G \times X \to X, (g, x) \mapsto gx$, удовлетворяющее следующим условиям:

1. $ex = x, \forall x \in X$ (e — нейтральный элемент группы G);
2. $g(hx) = (gh)x, \forall g, h \in G, x \in X$.

Определение 5.2. *Орбитой* точки $x \in X$ называется подмножество

$$Gx = \{x' \in X \mid x' = gx \text{ для некоторого } g \in G\} = \{gx \mid g \in G\}$$

Определение 5.3. *Стабилизатором (стационарной подгруппой)* точки $x \in X$ называется подгруппа $\mathrm{St}(x) = \{g \in G \mid gx = x\}$.

Определение 5.4. Действие G на X называется *транзитивным*, если для любых $x, x' \in X$ найдётся такой элемент $g \in G$, что $x' = gx$. Иными словами, все точки множества X образуют одну орбиту.

Определение 5.5. Действие G на X называется *свободным*, если для любой точки $x \in X$ условие $gx = x$ влечёт $g = e$. Иными словами, $\mathrm{St}(x) = \{e\}$ для всех $x \in X$.

Определение 5.6. Действие G на X называется *эффективным*, если условие $gx = x$ для всех $x \in X$ влечёт $g = e$. Иными словами, $\bigcup\limits_{x \in X} \mathrm{St}(x) = \{e\}$.

Определение 5.7. *Ядром неэффективности* действия группы G на множестве X называется подгруппа $K = \{g \in G \mid gx = x, \forall x \in X\}$.

Определение 5.8. Два действия группы G на множествах X и Y называются изоморфными, если существует такая биекция $\varphi : X \to Y$, что

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

Предложение 5.1. *Всякое свободное транзитивное действие группы G на множестве X изоморфно действию группы G на себе левыми сдвигами.*

Предложение 5.2. *Действия группы G на себе правыми и левыми сдвигами изоморфны.*

Теорема (Кэли)**.** *Всякая конечная группа G порядка n изоморфна подгруппе симметрической группы S_n.*

6 Лекция 6

Определение 6.1. *Кольцом* называется множество R с двумя бинарными операциями «+» (сложение) и «×» (умножение), обладающими следующими свойствами:

1. $(R, +)$ является абелевой группой (называемой *аддитивной группой* кольца R);
2. выполнены левая и правая дистрибутивности, то есть
$$a(b + c) = ab + ac, \quad (b + c)a = ba + ca, \forall a, b, c \in R;$$
3. $a(bc) = (ab)c, \forall a, b, c \in R$ (ассоциативность умножения);
4. $\exists 1 \in R$ (называемый единицей), что
$$a1 = 1a = a, \forall a \in R.$$

Определение 6.2. Кольцо R называется *коммутативным*, если $ab = ba, \forall a, b \in R$.

Определение 6.3. Элемент $a \in R$ называется *обратимым*, если $\exists b \in R, ab = ba = 1$.

Определение 6.4. Элемент $a \in R$ называется *левым* (соответственно *правым*) *делителем нуля*, если $a \neq 0$ и $\exists b \in R, b \neq 0, ab = 0$ (соответственно, $ba = 0$).

Определение 6.5. Элемент $a \in R$ называется *нильпотентом*, если $a \neq 0$, и $\exists m \in \mathbb{N}$, что $a^m = 0$.

Определение 6.6. Элемент $a \in R$ называется *идемпотентом*, если $a^2 = a$.

Определение 6.7. *Полем* называется коммутативное кольцо ассоциативное кольцо K с единицей, в котором всякий ненулевой элемент обратим.

Предложение 6.1. *Кольцо вычетов $\mathbb{Z}_n$ является полем тогда и только тогда, когда n — простое число.*

Определение 6.8. *Алгеброй* над полем K (или, кратко, K*-алгеброй*) называется множество A с операциями сложения, умножения и умножения на элементы поля K, обладающими следующими свойствами:

1. относительно сложения и умножения на элементы из K множество A есть векторное пространство;

2. относительно сложения и умножения A есть кольцо;

3. $(\lambda a)b = a(\lambda b) = \lambda(ab), \forall \lambda \in K; a, b \in A$.

Размерностью алгебры A называется её размерность как векторного пространства над K. Обозначение: $\dim_K A$.

Определение 6.9. *Подкольцом* кольца R называется всякое подмножество $R' \subset R$, замкнутое относительно операций сложения и умножения (то есть $a + b \in R', ab \in R', \forall a, b \in R'$) и являющееся кольцом относительно этих операций. *Подполем* называется всякое подкольцо, являющееся полем.

Определение 6.10. *Подалгеброй* алгебры A (над полем K) называется всякое подмножество $A' \subset A$, замкнутое относительно всех трёх имеющихся в A операций (сложения, умножения и умножения на элементы из K) и являющееся алгеброй (над K) относительно этих операций.

Определение 6.11. *Изоморфизмом* колец, алгебр называется всякий гомоморфизм, являющийся биекцией.

Определение 6.12. Подмножество I кольца R называется *(двусторонним) идеалом*, если оно является подгруппой по сложению и $ra \in I, ar \in I, \forall a \in I, r \in R$.

Определение 6.13. Идеал I называется *главным*, если существует такой элемент $a \in R, I = (a)$. В таком случае говорят, что I порождён элементом a.

Определение 6.14. Кольцо R/I называется *факторкольцом* кольца R по идеалу I.

Теорема (о гомоморфизме для колец)**.** *Пусть $\varphi : R \to R'$ — гомоморфизм колец. Тогда имеет место изоморфизм*

$$R/\ker\varphi \cong \mathrm{im}\varphi$$

Определение 6.15. Кольцо R называется *простым*, если в нём нет собственных (двусторонних) идеалов.

Определение 6.16. *Центром* алгебры A над полем K называется её подмножество

$$Z(A) = \{a \in A \mid ab = ba, \forall b \in A\}.$$

Теорема. *Пусть K — поле, n — натуральное число и $A = \mathrm{Mat}(n \times n, K)$ — алгебра квадратных матриц порядка n над полем K.*

1. *$Z(A) = \{\lambda E \mid \lambda \in K\}$, где E — единичная матрица (в частности, $Z(A)$ — одномерное подпространство в A);*

2. *алгебра A проста (как кольцо).*

7 Лекция 7

Определение 7.1. Элемент $b \in R$ *делит* элемент $a \in R$, (пишут $b|a$), если существует элемент $c \in R, a = bc$.

Определение 7.2. Два элемента $a, b \in R$ называют *ассоциированными*, если $a = bc$ для некоторого обратимого элемента $c \in R$.

Определение 7.3. Кольцо R без делителей нуля, не являющееся полем, называют *евклидовым*, если существует функция

$$N : R\backslash\{0\} \to \mathbb{Z}_{\geqslant 0},$$

называемая *нормой*, удовлетворяющая следующим условиям:

1. $N(ab) \geqslant N(A), \forall a, b \in R\backslash\{0\}$;

2. $\forall a, b \in R, b \neq 0, \exists q, r \in R : a = qb + r$, и либо $r = 0$, либо $N(r) < N(b)$.

Определение 7.4. *Наибольшим общим делителем* элементов a и b кольца R называется их общий делитель, который делится на любой другой их общий делитель. Обозначение: (a, b).

Теорема. *Пусть R — евклидово кольцо и a, b — произвольные элементы. Тогда:*

1. *существует наибольший общий делитель (a, b);*
2. *существуют такие элементы $u, v \in R$, что $(a, b) = ua + vb$.*

Определение 7.5. Кольцо R называется *кольцом главных идеалов*, если всякий идеал в R является главным.

Теорема. *Всякое евклидово кольцо является кольцом главных идеалов.*

Определение 7.6. Ненулевой необратимый элемент p кольца R называется *простым*, если он не может быть представлен в виде $p = ab$, где $a, b \in R$ — необратимые элементы.

Определение 7.7. Кольцо R называется *факториальным*, если всякий его ненулевой необратимый элемент «разложим на простые множители», то есть представим в виде произведения (конечного числа) простых элементов, причём это представление единственно с точностью до перестановки множителей и ассоциированности.

Теорема. *Всякое евклидово кольцо является факториальным.*

Определение 7.8. Многочлен $f(x) \in R[x]$ называется *примитивным*, если в R нет необратимого элемента, который делит все коэффициенты многочлена $f(x)$.

Теорема. *Если R — факториальное кольцо с полем отношений K и многочлен $f(x) \in R[x]$ разлагается в произведение двух многочленов в кольце $K[x]$, то он разлагается в произведение двух пропорциональных им многочленов в кольце $R[x]$.*

Предложение 7.1. *Если многчлен $f(x) \in R[x]$ может быть разложен в произведение двух многочленов меньшей степени в кольце $K[x]$, то он может быть разложен и в произведение двух многочленов меньшей степени в кольце $R[x]$.*

Теорема. *Если кольцо R факториально, то кольцо многочленов $R[x]$ тоже факториально.*

Теорема. *Пусть K — произвольное поле. Тогда кольцо многочленов $K[x_1, \ldots, x_n]$ факториально.*

8 Лекция 8

Определение 8.1. Многочлен $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, где K — произвольное поле, называется *симметрическим*, если $f(x_{\tau(1)}, \ldots, x_{\tau(n)}) = f(x_1, \ldots, x_n)$ для всякой перестановки $\tau \in S_n$.

Определение 8.2. *Элементарными симметрическими многочленами* называются такие многочлены:

$$\begin{aligned}
\sigma_1(x_1, \ldots, x_n) &= x_1 + x_2 + \cdots + x_n; \\
\sigma_2(x_1, \ldots, x_n) &= \sum_{1 \leqslant i < j \leqslant n} x_i x_j; \\
\ldots &= \ldots \\
\sigma_k(x_1, \ldots, x_n) &= \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} x_{i_1} x_{i_2} \ldots x_{i_k}; \\
\ldots &= \ldots \\
\sigma_n(x_1, \ldots, x_n) &= x_1 x_2 \ldots x_n;
\end{aligned}$$

Теорема (Основная теорема о симметрических многочленах)**.** *Для всякого симметрического многочлена $f(x_1, \ldots, x_n)$ существует и единственен такой многочлен $F(y_1, \ldots, y_n)$, что*

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

Определение 8.3. *Старшим членом* ненулевого многочлена $f(x_1, \ldots, x_n)$ называется наибольший в лексикографическом порядке встречающийся в нём одночлен. Обозначение: $L(f)$.

Теорема (о старшем члене)**.** *Пусть* $f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ *— произвольные ненулевые многочлены. Тогда* $L(fg) = L(f)L(g)$.

Теорема (Виет)**.** *Пусть* $\alpha_1, \ldots, \alpha_n$ *— корни многочлена* $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. *Тогда*

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

Определение 8.4. *Дискриминантом* многочлена $h(x) = a_n x^n + \cdots + a_1 x + a_0$ с корнями $\alpha_1, \ldots, \alpha_n$ называется выражение

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