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

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

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

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

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

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

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

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

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

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

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

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

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

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

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*

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