Лекция 3

Теорема 1. *1) Подгруппа циклической группы циклическая;*

2) Все подгруппы $\mathbb{Z}$ имеют вид $\langle k\rangle = k\mathbb{Z} \cong \mathbb{Z}$;

3) Все подгруппы $\mathbb{Z}_n$ имеют вид $\langle d\rangle = d\mathbb{Z}_n \cong \mathbb{Z}_{\frac{n}{d}}$ для некоторого d – делителя n;

4) Пусть $m \in \mathbb{Z}_n$. Тогда $\langle m\rangle = \langle НОД(m,n)\rangle$.

Доказательство. 1) Следует из пунктов 2) и 3).

2) Пусть H – подгруппа в $\mathbb{Z}$. Если $H = \{0\}$, то $H = \langle 0\rangle$, что укладывается в утверждение задачи. Пусть $H \neq \{0\}$. Если $h \in H$ – отрицательное число, то положительное число $-h$ также лежит в H. Значит, в H есть натуральные числа. Выберем k – минимальное натуральное число из H. Пусть $h \in H$. Тогда $h = kq + r$, где $0 \le r < k$. При этом $kq \in H$, $h \in H$, следовательно, $r \in H$. Если $r \neq 0$, получаем противоречие с выбором k. Значит, $r = 0$ и h делится на k. Отсюда $H = \langle k\rangle$.

3) Пусть H – подгруппа в $\mathbb{Z}_n$. Если $H = \{0\}$, то $H = \langle n\rangle$, что укладывается в утверждение задачи. Пусть $H \neq \{0\}$. Рассмотрим минимальное натуральное число d такое, что его класс лежит в H. Ясно, что $d < n$. Пусть $h \in H$. Тогда $h = dq + r$, где $0 \le r < d$. При этом $dq \in H$, $h \in H$, следовательно, $r \in H$. Если $r \neq 0$, получаем противоречие с выбором d. Значит, $r = 0$ и h делится на d. Отсюда $H = \langle d\rangle$. Докажем, что d – делитель n. Если это не так, то $n = kd + s$, $0 < s < d$. Но тогда в $\mathbb{Z}_n$ выполнено $s = kd \in H$, противоречие с выбором d. Итак, d – делитель n. Осталось сказать, что порядок d в группе $\mathbb{Z}_n$ равен $\frac{n}{d}$. Значит, $H = \langle d\rangle \cong \mathbb{Z}_{\frac{n}{d}}$.

4) $\langle m\rangle$ – циклическая группа. По лемме **??**, $\operatorname{ord}(m) = \frac{n}{\text{НОД}(m,n)}$. Значит $|\langle m\rangle| = \frac{n}{\text{НОД}(m,n)}$. Следовательно, по пункту 3), $\langle m\rangle = \langle \text{НОД}(m,n)\rangle$. □

Определение 1. Пусть H – подгруппа группы G. Рассмотрим элемент $g \in G$. *Левым смежным классом элемента g по подгруппе H* называется множество

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

Правым смежным классом элемента g по подгруппе H называется множество

$$Hg = \{hg \mid h \in H\}.$$

Лемма 1. *1) $g \in fH$ тогда и только тогда, когда $f^{-1}g \in H$,*

1') $g \in Hf$ тогда и только тогда, когда $gf^{-1} \in H$,

2) Левые (правые) смежные классы – это классы эквивалентности. (Более точно, отношение $g \sim f$, если $g \in fH$ является отношением эквивалентности.)

3) Следующие мощности одинаковы $|gH| = |Hg| = |H|$.

Доказательство. 1) $g \in fH \Longleftrightarrow g = fh \Longleftrightarrow f^{-1}g = h$.

1') $g \in Hf \Longleftrightarrow g = hf \Longleftrightarrow gf^{-1} = h$.

2) Докажем только для левых смежных классов. Для правых аналогично.

Рефлексивность: $g \in gH$ так как $e \in H$,

Симметричность:

$$g \in fH \Longleftrightarrow f^{-1}g \in H \Longleftrightarrow (f^{-1}g)^{-1} = g^{-1}f \in H \Longleftrightarrow f \in gH.$$

Транзитивность:

$$g \in fH, f \in sH \Longrightarrow f^{-1}g \in H, s^{-1}f \in H \Longrightarrow s^{-1}ff^{-1}g = s^{-1}g \in H.$$

3) Следует из того, что $gh_1 = gh_2$ тогда и только тогда, когда $h_1 = h_2$. □

Замечание 1. Из пункта 2 следует, что левые (правые) смежные классы либо не пересекаются, либо совпадают.

Определение 2. Индекс подгруппы H группы G – это мощность множества левых смежных классов. Обозначается индекс $[G : H]$

Задача 1. Докажите, что $gH \leftrightarrow Hg^{-1}$ – биекция между левыми и правыми смежными классами, и следовательно мощность правых смежных классов также равна индексу подгруппы. (То, что количество левых и правых смежных классов одинаково для конечной группы будет следовать из теоремы Лагранжа, но это верно и для бесконечных групп.)

Теорема 2. *(Лагранж) Пусть G – конечная группа и H – подгруппа G. Тогда*

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

Доказательство. Поскольку каждый элемент группы G лежит в некотором левом смежном классе и левые смежные классы либо совпадают, либо не пересекаются, вся группа G разбивается на непересекающиеся левые смежные классы. Так как мощность каждого смежного класса равна $|H|$, мощность всей группы равна $|H|$ умножить на количество смежных классов. $\square$

Следствие 1. *(Следствия из теоремы Лагранжа)*
1) Порядок конечной группы делится на порядок ее подгруппы.
2) Порядок конечной группы делится на порядок ее элемента.
3) Для любого элемента g конечной группы G выполнено $g^{|G|} = e$.
4) Группа простого порядка циклическая.
5) (Малая теорема Ферма) Пусть p – простое число и a – число, не делящееся на p. Тогда a^{p-1} имеет остаток 1 при делении на p.

Доказательство. 1) Очевидно следует из теоремы Лагранжа.
2) Пусть g – элемент конечной группы G. Рассмотрим циклическую подгруппу $H = \langle g \rangle$. Поскольку $\mathrm{ord}(g) = |H|$, порядок G делится на $\mathrm{ord}(g)$.
3) Пусть $|G| = \mathrm{ord}(g) \cdot k$. Тогда $g^{|G|} = (g^{\mathrm{ord}(g)})^k = e^k = e$.
4) Пусть $|G| = p$ – простое число. Рассмотрим $g \neq e \in G$. Поскольку порядок g делит p и не равен 1, получаем $\mathrm{ord}(g) = p$. А значит, $G = \langle g \rangle$.
5) Применим пункт 3 к группе $\mathbb{Z}_p^{\times} = (\mathbb{Z}_p \setminus \{0\}, \cdot)$ и ее элементу a. Получаем

$$a^{|\mathbb{Z}_p^{\times}|} = a^{p-1} = 1 (\mathrm{mod}\ p).$$

$\square$

Определение 3. Подгруппа H группы G называется нормальной, если для любого $g \in G$ выполнено $gH = Hg$. То, что H – нормальная подгруппа G обозначается так: $G \triangleright H$.

Обозначим через gHg^{-1} множество $\{ghg^{-1} \mid h \in H\}$.

Лемма 2. *Следующие условия равносильны:*
1) $G \triangleright H$,
2) для каждого $g \in G$ выполнено $gHg^{-1} = H$,
3) для каждого $g \in G$ выполнено $gHg^{-1} \subseteq H$,

Доказательство. $1 \Longrightarrow 2$ В множестве $gH = Hg$ каждый элемент имеет вид $gh_1 = h_2 g$. При этом и h_1 и h_2 пробегают всю группу H. Домножим каждый элемент справа на g^{-1}, получим $gh_1g^{-1} = h_2$. То есть $gHg^{-1} = H$.

$2 \Longrightarrow 3$ Очевидно.

$3 \Longrightarrow 1$. Для каждых $g \in G$ и $h \in H$ выполнено $ghg^{-1} = \tilde{h} \in H$. Тогда $gh = ghg^{-1}g = \tilde{h}g$. Отсюда $gH \subseteq Hg$. Аналогично $hg = gg^{-1}hg = g\widehat{h}$ для $\widehat{h} = g^{-1}hg \in H$. Значит, $gH \supseteq Hg$. В итоге $gH = Hg$. $\square$

Пример 1. *Любая подгруппа в абелевой группе нормальна, так как* $ghg^{-1} = h$.

Пример 2. $\mathrm{SL}_n(\mathbb{C})$ *– нормальная подгруппа в* $\mathrm{GL}_n(\mathbb{C})$. *Действительно, пусть* $A \in \mathrm{GL}_n(\mathbb{C})$, $B \in \mathrm{SL}_n(\mathbb{C})$. *Тогда* $\det(ABA^{-1}) = \det A \det B (\det A)^{-1} = 1$. *То есть* $ABA^{-1} \in \mathrm{SL}_n(\mathbb{C})$.

Пример 3. *Подгруппа* $\langle (1,2) \rangle = \{\mathrm{id}, (1,2)\} \subseteq S_3$ *не является нормальной. В самом деле,*

$$(1,2,3)(1,2)(1,2,3)^{-1} = (1,2,3)(1,2)(1,3,2) = (2,3) \notin \langle (1,2) \rangle.$$

Определение 4. Пусть H – нормальная подгруппа в группе G. Факторгруппа G/H – это множество (левых, они же правые) смежных классов по подгруппе H с операцией

$$(g_1H) \cdot (g_2H) = (g_1g_2)H.$$

Определение умножения в факторгруппе требует проверки корректности, то есть проверки того, что результат умножения не зависит от выбора представителей в смежных классах. Потенциальная проблема содержится в том, что $g_1H = g_1'H$, $g_2H = g_2'H$, но при этом смежный класс g_1g_2H может не совпадать с $g_1'g_2'H$. Тогда умножение называется некорректным.

Предложение 1. *Пусть* G *– группа,* H *– подгруппа. Тогда умножение на множестве левых смежных классов корректно тогда и только тогда, когда* H *нормальна.*

Доказательство. Пусть H нормальна и $g_1H = g_1'H$, $g_2H = g_2'H$. Получаем, что $g_1'^{-1}g_1 \in H$ и $g_2'^{-1}g_2 \in H$. Обозначим $g_1'^{-1}g_1$ через h. Имеем

$$(g_1'g_2')^{-1}(g_1g_2) = g_2'^{-1}g_1'^{-1}g_1g_2 = g_2'^{-1}hg_2 \in H$$

Это означает, что g_1g_2H совпадает с $g_1'g_2'H$. Значит, умножение корректно.

Пусть теперь H не нормальна. Тогда найдутся $g \in G$ и $h \in H$ такие, что $ghg^{-1} \notin H$. Тогда $gH = (gh)H$. Рассмотрим следующие смежные классы: $gH = (gh)H$ и $g^{-1}H$. Имеем $gH \cdot g^{-1}H = H$, но $(gh)H \cdot g^{-1}H = (ghg^{-1})H \neq H$. Значит, умножение не корректно. $\square$

Легко видеть, что G/H действительно группа. Ассоциативность произведения следует из ассоциативности произведения в G, единичный элемент – это $eH = H$, обратный к gH элемент – это $g^{-1}H$. Из теоремы Лагранжа следует, что если G – конечная группа, то $|G/H| = \frac{|G|}{|H|}$.

Пример 4. *Найдем, чему изоморфна факторгруппа* $\mathbb{Z}/n\mathbb{Z}$. *Подгруппа* $n\mathbb{Z}$ *нормальна, так как группа* $\mathbb{Z}$ *абелева. Смежные классы имеют вид* $k+n\mathbb{Z}$. *При этом* $k+n\mathbb{Z} = l+\mathbb{Z}$ *тогда и только тогда, когда* k *и* l *имеют одинаковые остатки при делении на* n. *Сопоставим смежному классу* $k + n\mathbb{Z}$ *остаток при делении* k *на* n. *Докажем, что это сопоставление – это изоморфизм* ψ *между* $\mathbb{Z}/n\mathbb{Z}$ *и* $\mathbb{Z}_n$. *Действительно, сложению* *смежных классов соответствует сложение остатков. Кроме того* ψ *сюръективно, так как любой остаток – это остаток некоторого числа* k*, а значит, он равен* $\psi(k + n\mathbb{Z})$*. Проверим инъективность* ψ*. Пусть* $\psi(k + n\mathbb{Z}) = \psi(l + n\mathbb{Z})$*. Значит,* k *и* l *сравнимы помодулю* n*. Следовательно,* $k + n\mathbb{Z} = l + n\mathbb{Z}$*.*