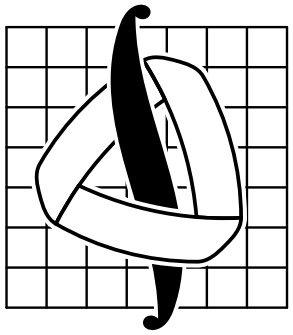
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА
Механико-математический факультет



Конспект лекций по алгебре

Лектор — Иван Владимирович Аржанцев

3 семестр, II поток

Москва, 2013 г.

Оглавление

Предисловие

Лекции, кроме последней, читал Иван Владимирович Аржанцев, профессор кафедры высшей алгебры. На последней лекции его заменял Дмитрий Андреевич Тимашёв, доцент кафедры высшей алгебры. В связи с этим в конспектах последних двух лекций могут содержаться незначительные намеренные (с целью сохранения целостности материала) отклонения от настоящего порядка изложения.

Конспект подготовил Ираклий Глунчадзе, студент группы 207. Для вёрстки использовалась издательская система LaTeX 2ε с подключённым, помимо прочих, пакетом XY-pic.

Эта версия была скомпилирована 16 декабря 2013 г. Последняя версия всегда доступна по адресу vk.cc/1V5GwX. *Планируется также добавить к ней в качестве приложения решения некоторых задач из лекций, разобранные И. В. Аржанцевым и студентами группы 207 на семинарских занятиях. Кроме того, существует вариант конспекта, покрывающий только тему «Теория групп», но разделённый на билеты коллоквиума по ней:* vk.cc/1V5KCd.

Будьте осторожны! Это не курс лекций, а только их конспект, не претендующий на истину в последней инстанции. От любой ответственности за успешность подготовки к контрольным мероприятиям по этому документу, а также за попытки использовать его на таких мероприятиях в качестве «шпаргалки» наборщик отказывается.

Для любых пожеланий и замечаний используйте электронную почту chingizkahn@yandex.ru *или страницу ВКонтакте* vk.com/iglunchadze.

Спасибо Владимиру Беляеву, Дмитрию Быстрову, Александру Запрягаеву, Арсению Каданеру, Михаилу Кузину, Татьяне Овчинниковой, Ольге Парамоновой, Павлу Степчкову, Анатолию Ширыкалову и всем, кого я мог не вспомнить, за содействие в поиске ошибок и опечаток.

Посвящается Келли.

Начало лекции № 1 от 2 сентября 2013 г.

I. Теория групп

§ 1. Основные определения

Определение. *Группой* называется множество G с бинарной операцией $G \times G \to G$ (стандартное обозначение: $(a, b) \mapsto ab$), удовлетворяющей следующим требованиям:

1. ассоциативность: $(ab)\,c = a\,(bc) \quad \forall\, a, b, c \in G$;
2. наличие нейтрального элемента: $\exists\, e \in G : ea = ae = a \quad \forall\, a \in G$;
3. наличие обратного элемента: $\forall\, a \in G \;\; \exists\, a^{-1} \in G : aa^{-1} = a^{-1}a = e$.

Если бинарная операция обладает из перечисленного только ассоциативностью, то G называется *полугруппой*. Полугруппа с нейтральным элементом называется *моноидом*.

Определение. Группа называется *коммутативной*, или *абелевой*, если $ab = ba \;\; \forall\, a, b \in G$.

Для коммутативных групп используются аддитивные обозначения: вместо G пишут A, вместо ab пишут $a+b$, вместо e пишут 0, вместо a^{-1} — $-a$.

Определение. *Подгруппой* группы G называется такое её подмножество $H \subseteq G$, что $e \in H$ и если $a, b \in H$, то $ab^{-1} \in H$.

Определение. *Гомоморфизмом* групп G_1 и G_2 называется отображение $\varphi : G_1 \to G_2$, такое что $\forall\, a, b \in \in G_1 \;\; \varphi\,(ab) = \varphi\,(a)\,\varphi\,(b)$.

Замечание.

1. $\varphi\,(e_1 e_1) = \varphi\,(e_1)\,\varphi\,(e_1) = \varphi\,(e_1) = e_2$;
2. $e_2 = \varphi\,(e_1) = \varphi\left(aa^{-1}\right) = \varphi\,(a)\,\varphi\left(a^{-1}\right) \Rightarrow \varphi\left(a^{-1}\right) = \varphi\,(a)^{-1}$.

Определение. *Изоморфизмом* групп называется их биективный гомоморфизм. Если между G_1 и G_2 существует изоморфизм, то говорят, что они *изоморфны*, что обозначается так: $G_1 \cong G_2$.

Так как изоморфизм $\varphi\colon G_1 \to G_2$ биективен, то существует обратное к нему отображение $\varphi^{-1}\colon G_2 \to G_1$. Докажем, что это отображение — гомоморфизм.

Теорема 1. $\varphi^{-1}\,(cd) = \varphi^{-1}\,(c)\,\varphi^{-1}\,(d)$.

□ $\quad \varphi\left(\varphi^{-1}\,(cd)\right) = cd = \varphi\left(\varphi^{-1}\,(c)\right)\varphi\left(\varphi^{-1}\,(d)\right) = \varphi\left(\varphi^{-1}\,(c)\,\varphi^{-1}\,(d)\right)$.

При этом φ — биекция. ■

Определение. *Эндоморфизмом* группы называется её гомоморфизм в себя. *Автоморфизмом* группы называется её изоморфизм в себя.

Определение. Пусть $\varphi\colon G_1 \to G_2$ — гомоморфизм. Тогда его *ядром* называется множество $\operatorname{Ker}\varphi \stackrel{\text{def}}{=} \{a \in G_1 \mid \varphi\,(a) = e_2\}$, а его *образом* называется множество $\operatorname{Im}\varphi \stackrel{\text{def}}{=} \{b \in G_2 \mid \exists\, a \in G_1 \colon \varphi\,(a) = b\}$.

Задача 1. *Доказать, что* $\operatorname{Ker}\varphi \subseteq G_1$ *и* $\operatorname{Im}\varphi \subseteq G_2$ *— подгруппы в своих группах.*

Определение. *Порядок* группы G — это число её элементов $|G|$. Группа называется *конечной*, если $|G| < \infty$, и *бесконечной* в ином случае.

§ 2. Примеры групп

2.1. Числовые

1. Аддитивные:
   - $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ — бесконечные;
   - $(\mathbb{Z}_n, +)$ — конечная.
2. Мультипликативные:
   - $(\mathbb{Z}^{\times}, \times)$ [1] $= \{\pm 1\}$;

[1] Здесь и далее верхним индексом $\times$ обозначаем подмножество, составленное из всех обратимых и только обратимых элементов множества.

- если F — поле, то $(\mathbb{F}^\times, \times) = F \setminus \{0\}$ — группа;
- $(\mathbb{Z}_n^\times, \times) = \left\{\overline{k} \mid (k, n) = 1\right\}$, при этом $|\mathbb{Z}_n^\times| = \varphi(n)$, где φ — функция Эйлера;
- $\left(\mathbb{Z}_p^\times, \times\right) = \left\{\overline{1}, \ldots, \overline{p-1}\right\}$, где p — простое.

2.2. Подстановки

1. $\mathbf{S}_n$ — симметрическая группа, $|\mathbf{S}_n| = n!$.
2. $\mathbf{A}_n$ — знакопеременная группа (чётные подстановки), $|\mathbf{A}_n| = \frac{n!}{2}$.
3. *Группа Клейна* $\mathbf{V}_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ коммутативна.

Задача 2. *Доказать, что:*

1. $\mathbf{S}_n$ *коммутативна* $\Leftrightarrow n \leqslant 2$;
2. $\mathbf{A}_n$ *коммутативна* $\Leftrightarrow n \leqslant 3$.

2.3. Матрицы

Пусть F — поле. Матрицы будем рассматривать над ним. Говоря про группы матриц, операцией подразумевают умножение.

1. $\mathbf{GL}_n(F)$ — *общая линейная группа* (матрицы с ненулевым определителем, то есть обратимые).
2. $\mathbf{SL}_n(F)$ — *специальная линейная группа* (матрицы с определителем, равным единице).
3. $\mathbf{D}_n(F)$ — группа диагональных матриц.
4. $\mathbf{B}_n(F)$ — группа верхнетреугольных матриц.
5. $\mathbf{U}_n(F)$ — группа *унитреугольных матриц* (верхнетреугольных матриц, у которых на главной диагонали стоят единицы).
6. $\mathbf{O}_n(F) = \left\{A \mid AA^T = E\right\} = \{A \mid (Av, Aw) = (v, w) \ \ \forall v, w \in F^n\}$, где $(\cdot, \cdot)$ — невырожденная билинейная симметрическая форма, $(v, w) = x_1y_1 + \ldots + x_ny_n$, — *ортогональная группа* (у всех ортогональных матриц определитель по модулю равен единице).
7. $\mathbf{SO}_n(F)$ — *специальная ортогональная группа* (подгруппа ортогональной группы, составленная из матриц, определитель которых равен единице).
8. $\mathbf{U}_n(\mathbb{C}) = \{A \mid AA^* = E\}$ — *унитарная группа.*
9. $\mathbf{SU}_n(\mathbb{C})$ — *специальная унитарная группа* (подгруппа унитарной группы, составленная из матриц, определитель которых равен единице).
10. $\mathbf{Sp}_{2n}(F) = \left\{A \mid AJA^T = J\right\}$, где J — блочнодиагональная матрица, состоящая из блоков $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, в каноническом виде, — *симплектическая группа.*

Задача 3. *Вычислить порядки* $\mathbf{GL}_n(\mathbb{Z}_p)$, $\mathbf{SL}_n(\mathbb{Z}_p)$, $\mathbf{D}_n(\mathbb{Z}_p)$, $\mathbf{B}_n(\mathbb{Z}_p)$, $\mathbf{U}_n(\mathbb{Z}_p)$, *где* p — *простое.*

Задача 4. *Доказать, что если* $A \in \mathbf{Sp}_{2n}(F)$, *то* $\det A = 1$.

2.4. Аффинные преобразования

Полагаем $M \subseteq \mathbb{R}^n$.

1. $\mathrm{Aff}_n(\mathbb{R}^n)$ — преобразования $\mathbb{A}_n$: $x \mapsto Ax + b$, $\det A \neq 0$, $\mathbb{R}^n$ — евклидово аффинное пространство;
2. *группа движений* — группа аффинных преобразований, у которых A ортогональна;
3. $\mathrm{Sym}(M) = \{f$ — движение $\mid f(M) = M\}$ — *группа симметрий*;
4. $\mathrm{Sym}^+(M) = \{f \in \mathrm{Sym}(M) \mid \det A = 1\}$ — *группа вращений.*

Задача 5. *Доказать, что:*

1. *группа симметрий правильного тетраэдра изоморфна* $\mathbf{S}_4$;
2. *группа вращений правильного тетраэдра изоморфна* $\mathbf{A}_4$;
3. *группа вращений куба изоморфна* $\mathbf{S}_4$.

Определение. *Группой диэдра* $\mathbf{D}_n$ называется группа симметрий правильного n-угольника.

Замечание. При любом n $|\mathbf{D}_n| = 2n$: это число складывается из n поворотов и n осевых симметрий. Но $\mathbf{D}_n$ при чётных и нечётных n устроены по-разному. Например, у правильного пятиугольника все оси симметрии проходят через вершину и середины противолежащего ребра. Но у правильного шестиугольника есть оси симметрии, проходящие через противоположные вершины, и оси симметрии, проходящие через середины противоположных сторон.

2.5. Группа кватернионов

Определение. *Группой кватернионов* называется множество $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ с операцией умножения, заданной следующим образом: $i^2 = j^2 = k^2 = -1$, $ij = k, ji = -k$ («по кругу»).

§ 3. Циклические группы

Пусть G — группа, а g — её элемент.

Определение. *Циклической подгруппой* в G, порождённой g, называется подгруппа $\langle g\rangle = \{g^n, n \in \mathbb{Z}\} = \{\ldots, g^{-2}, g^{-1}, g^0 = e, g^1 = g, g^2, \ldots\}$.

Пример 1. $G = (\mathbb{Z}, +)$, $g = 2 \Rightarrow \langle g\rangle = 2\mathbb{Z}$ — чётные числа.

Определение. *Порядок элемента* $g \in G$ — это наименьшее $n \in \mathbb{N}$, такое что $g^n = e$, если такое существует, или ∞, если такого не существует. Порядок элемента g обозначается как $\operatorname{ord}(g)$.

Лемма 1. $\operatorname{ord}(g) = |\langle g\rangle|$.

□ Пусть $n = \operatorname{ord}(g)$ — конечное число. Тогда $e, g, \ldots, g^{n-1}$ попарно различны, так как если $\exists\, m, k : m > k, g^m = g^k$, то $g^{m-k} = e$, а $m - k < n$, что ведёт к противоречию. Таким образом, $e, g, \ldots, g^{n-1} \in \langle g\rangle$.

Возьмём некоторое $m \in \mathbb{Z}$. Тогда, по теореме о делении с остатком, $m = nq + r$, где $0 \leqslant r \leqslant n-1 \Rightarrow g^m = (g^n)^q g^r = e^q g^r = g^r$. Значит, кроме уже перечисленных элементов, в $\langle g\rangle$ ничего нового добавить нельзя $\Rightarrow |\langle g\rangle| = n$.

Если же $\operatorname{ord}(g) = \infty$, то $g^m \neq g^k \ \forall\, k, m : k \neq m \Rightarrow |\langle g\rangle| = \infty$. ■

Определение. Группа G называется *циклической*, если существует такой элемент $g \in G$, что $\langle g\rangle = G$. Такой g называется *порождающим*, или *образующим элементом*.

Пример 2. $G = (\mathbb{Z}, +) \Rightarrow$ порождающие элементы $g = \pm 1$. Больше порождающих в этой группе нет.

Предложение 1.

1. *Если G — бесконечная циклическая группа, то $G \cong (\mathbb{Z}, +)$.*
2. *Если G — конечная циклическая группа, то $G \cong (\mathbb{Z}_n, +)$.*

□ Строим соответствующие изоморфизмы:

1. $g^m \mapsto m$;
2. $g^m \mapsto \overline{r}$, где $m = nq + r$, $0 \leqslant r \leqslant n-1$, $n = |G|$.

■

Задача 6. *Доказать, что* $\operatorname{ord}\left(g^k\right) = \frac{n}{(n,k)}$, *где* $n = \operatorname{ord}(g)$.

Предложение 2. *Имеется биекция между целыми неотрицательными числами и подгруппами в $\mathbb{Z}$:*

$$d \leftrightarrow d\mathbb{Z}.$$

□ Очевидно, что $d\mathbb{Z}$ — подгруппа и что $d\mathbb{Z} = d'\mathbb{Z} \Leftrightarrow d = d'$.

Докажем, что других подгрупп нет. Если произвольная подгруппа $H = \{0\}$, кладём $d = 0$, иначе кладём d равным наименьшему натуральному элементу H. Тогда $d\mathbb{Z} \subseteq H$.

Пусть $m \in H$. Тогда $m = qd + r \Rightarrow r = m - qd \in H$. При этом $r \in \mathbb{Z}$, $0 \leqslant r \leqslant d-1$, то есть либо $r = 0$, либо $r \in \mathbb{N}$. Но мы выбирали d минимальным натуральным элементом $H \Rightarrow r = 0 \Rightarrow H \subseteq d\mathbb{Z} \Rightarrow H = d\mathbb{Z}$. ■

Предложение 3. *Пусть $n \geqslant 2$. Тогда имеется биекция между натуральными делителями n и подгруппами в $\mathbb{Z}_n$:*

$$d \leftrightarrow \left\langle \overline{d} \right\rangle = d\mathbb{Z}_n.$$

В частности, $|d\mathbb{Z}_n| = \frac{n}{d}$.

□ Очевидно, что $d\mathbb{Z}_n$ — подгруппа $\mathbb{Z}_n \ \forall\, d$.

Если $d \mid n$, то $d\mathbb{Z}_n = \left\{\overline{0}, \overline{d}, \overline{2d}, \ldots, \overline{(k-1)\,d}\right\}$, где $k = \frac{n}{d}$. Таким образом, если $d\mathbb{Z}_n = d'\mathbb{Z}_n$, то $d = d'$.

Пусть $H \subseteq \mathbb{Z}_n$ — произвольная подгруппа. Если $H = \{0\}$, то кладём $d = n$. Иначе пусть d соответствует $\overline{d}$ — наименьшему ненулевому вычету в H. Пусть $c = (d, n)$. По лемме о линейном представлении НОД, $\exists\, u, v \in \in \mathbb{Z}:\ c = du + nv \Rightarrow \overline{c} \in H \Rightarrow c = d \Rightarrow d \mid n$.

Пусть $\overline{m} \in H, m = dq + r, 0 \leqslant r \leqslant d-1$. Тогда $\overline{r} = \overline{m} - \overline{d} \cdot \overline{q} \in H \Rightarrow \overline{r} = \overline{0} \Rightarrow H = d\mathbb{Z}_n$. ■

Следствие. Подгруппа циклической группы — циклическая.

Задача 7. *Привести пример коммутативной счётной нециклической группы.*

Конец лекции № 1 от 2 сентября 2013 г. *(к началу)*

Начало лекции № 2 от 4 сентября 2013 г.

§ 4. Смежные классы. Теорема Лагранжа

Пусть G — группа, $H \subseteq G$ — подгруппа.

Определение. *Левым смежным классом* элемента $g \in G$ по подгруппе H называется множество $gH \overset{\text{def}}{=} \overset{\text{def}}{=} \{gh \mid h \in H\}$.

Замечание. g и g' лежат в одном смежном классе $\Leftrightarrow g^{-1}g' \in H$.

Определение. *Правым смежным классом* элемента $g \in G$ по подгруппе H называется множество $Hg \overset{\text{def}}{=} \overset{\text{def}}{=} \{hg \mid h \in H\}$.

Замечание.

1. $\forall\, g, g' \in G$ либо $gH = g'H$, либо $gH \cap g'H = \varnothing$;
2. $\forall\, g \in G\ \ |gH| = |H|$.

Теорема 2 (Лагранжа). *Пусть G — конечная группа, $H \subseteq G$ — подгруппа. Тогда $|H| \,\big|\, |G|$.*

Доказательство этого результата приводилось в первом семестре.

Следствие. $\forall\, g \in G\ \ \operatorname{ord}(g) \mid |G|$.

□ $\operatorname{ord}(g) = |\langle g \rangle|$, дальше пользуемся теоремой Лагранжа. ■

Следствие. Пусть p — простое, $|G| = p$. Тогда $G \cong \mathbb{Z}_p$.

□ $\forall\, g \neq e\ 1 \neq |\langle g \rangle| \mid p \Rightarrow |\langle g \rangle| = p \Rightarrow \langle g \rangle = G$. ■

Определение. *Индекс подгруппы H* в группе G — это число левых смежных классов по этой подгруппе. Для конечных групп G индекс H обозначается как $[G : H]$, потому что как раз равен $\frac{|G|}{|H|}$. Разбиение группы на правые смежные классы может быть устроено по-другому, но их всё равно будет столько же, сколько и левых.

Задача 8. *Доказать, что в произвольной группе G число левых смежных классов по её подгруппе H равно числу правых смежных классов по H.*

Пример 3. Пусть $G = \mathbf{S}_n$, $H = \left\{\left(\begin{smallmatrix} 1 & 2 & \ldots & n \\ 1 & * & \ldots & * \end{smallmatrix}\right)\right\}$, $g = \left(\begin{smallmatrix} 1 & \ldots & j_1 & \ldots & n \\ i_1 & \ldots & 1 & \ldots & * \end{smallmatrix}\right)$. Тогда $gH = \left\{\left(\begin{smallmatrix} 1 & 2 & \ldots & n \\ i_1 & * & \ldots & * \end{smallmatrix}\right)\right\}$, то есть все матрицы такого вида: их $(n-1)!$ — ровно столько же, сколько и всевозможных произведений g и элементов H. А $Hg = \left\{\left(\begin{smallmatrix} 1 & \ldots & j_1 & \ldots & n \\ * & \ldots & 1 & \ldots & * \end{smallmatrix}\right)\right\}$.

Задача 9. *Привести пример конечной группы G и натурального делителя d числа $|G|$, для которых в G не существует подгруппы порядка d.*

§ 5. Нормальная подгруппа. Факторгруппы. Теорема о гомоморфизме

Гомоморфный образ группы
(Путь к победе коммунизма)
Изоморфен факторгруппе
По ядру гомоморфизма.

Неизвестный автор

Определение. Подгруппа $H \subseteq G$ *нормальна*, если $\forall\, g \in G\ gH = Hg$.

Пример 4.

1. Если G абелева, то любая её подгруппа нормальна.
2. $G = \mathbf{S}_n \Rightarrow H = \left\{\left(\begin{smallmatrix} 1 & 2 & \ldots & n \\ 1 & * & \ldots & * \end{smallmatrix}\right)\right\}$ — ненормальная подгруппа.

3. Если G — любая группа, $H \subseteq G$ — подгруппа, $[G : H] = 2$, то H нормальна.

□

- $g \in H \Rightarrow gH = Hg = H$;
- $g \notin H \Rightarrow gH = Hg = G \setminus H$.

■

Замечание. $H \subseteq G$ нормальна $\Leftrightarrow gHg^{-1} = H \ \forall g \in G$. Другими словами, подгруппа нормальна тогда и только тогда, когда она устойчива относительно всех сопряжений. Из этого следует, что для проверки нормальности подгруппы достаточно проверить выполнение условия $gHg^{-1} \subseteq H$. Действительно, домножив это включение на g^{-1} слева и на g справа, получим, что $H \subseteq g^{-1}Hg \ \forall g \in G$. Подставив теперь вместо g g^{-1}, получим и обратное имеющемуся включение.

Лемма 2. *Если $\varphi : G_1 \to G_2$ — гомоморфизм, то $\operatorname{Ker}\varphi \subseteq G_1$ — нормальная подгруппа в G_1.*

□ Проверяем, что $\forall h \in \operatorname{Ker}\varphi, \ \forall g \in G_1 \ ghg^{-1} \in \operatorname{Ker}\varphi$. Действительно,

$$\varphi\left(ghg^{-1}\right) = \varphi(g)\,\varphi(h)\,\varphi\left(g^{-1}\right) = \varphi(g)\,e_2\varphi\left(g^{-1}\right) = \varphi(g)\,\varphi(g)^{-1} = e_2.$$

■

Задача 10. *Привести пример гомоморфизма $\varphi : G_1 \to G_2$, для которого $\operatorname{Im}\varphi \subseteq G_2$ — ненормальная подгруппа.*

Определение. Пусть G — группа, $H \subseteq G$ — нормальная подгруппа. Обозначим через ${}^{G}\!/_{H}$ (читается «G по H») множество левых смежных классов: ${}^{G}\!/_{H} = \{gH \mid g \in G\}$. Операцию умножения на ней зададим так: $(gH)(g'H) = (gg')H = gg'H$. С такой операцией ${}^{G}\!/_{H}$ называется *факторгруппой*.

Видно, что элементы факторгруппы — подмножества G. Также видно, что определённая нами операция умножения обладает необходимыми свойствами:

- ассоциативностью: $((gH)(g'H))(g''H) = (gH)((g'H)(g''H)) = gg'g''H$;
- нейтральным элементом $eH = H$;
- обратным элементом $g^{-1}H$ для gH.

Но корректно ли определена операция умножения? Это могло бы быть неверно, если бы мы не потребовали от H нормальности.

Теорема 3. *Умножение в факторгруппе определено корректно: $\forall g, g' \in G, \ \forall h, h' \in H \ (gH)(g'H) = (ghH)(g'h'H)$.*

□ $(gg')^{-1} ghg'h' \in H \Leftrightarrow (g')^{-1} g^{-1} ghg' \in H \Leftrightarrow (g')^{-1} hg' \in H \Leftrightarrow g'h(g')^{-1} \in H \Leftrightarrow H$ нормальна. ■

Также нужно проверить корректность определения обратного элемента.

Теорема 4. *Обратный элемент в факторгруппе определено корректно, то есть $\forall g \in G, \ \forall h \in H \ g^{-1}H = (gh)^{-1}H$.*

□ $g^{-1}H = (gh)^{-1}H \Leftrightarrow \left(g^{-1}\right)^{-1}(gh)^{-1} \in H \Leftrightarrow gh^{-1}g^{-1} \in H$, в силу нормальности H. ■

Замечание. Для любой нормальной подгруппы $H \subseteq G$ отображение $\pi : G \to {}^{G}\!/_{H}$, $g \mapsto gH$, является гомоморфизмом.

□ $\pi(gg') = gg'H$, $\pi(g)\,\pi(g') = (gH)(g'H) = gg'H \Rightarrow \pi(gg') = \pi(g)\,\pi(g')$. ■

Видно, что $\operatorname{Ker}\pi = H$. Отсюда можно сделать вывод, что любая нормальная подгруппа реализуется как ядро какого-то гомоморфизма.

Теорема 5 (о гомоморфизме). *Пусть $\varphi : G_1 \to G_2$ — гомоморфизм. Тогда $\operatorname{Im}\varphi \cong {}^{G_1}\!/_{\operatorname{Ker}\varphi}$.*

□ Определим отображение ψ: ${}^{G_1}\!/_{\operatorname{Ker}\varphi} \to \operatorname{Im}\varphi$ следующим образом:

$$\psi(g \operatorname{Ker}\varphi) = \varphi(g).$$

Проверим, что ψ — изоморфизм.

- Корректность: если $g^{-1}g' \in \operatorname{Ker}\varphi$, то $\varphi\left(g^{-1}g'\right) = e_2 \Leftrightarrow \varphi(g) = \varphi(g')$.
- Сюръективность очевидна.
- Инъективность: $\varphi(g) = \psi(g \operatorname{Ker}\varphi) = \psi(g' \operatorname{Ker}\varphi) = \varphi(g') \Leftrightarrow \varphi\left(g^{-1}g'\right) = e_2 \Leftrightarrow g \operatorname{Ker}\varphi = g' \operatorname{Ker}\varphi$.

- Гомоморфность: $\psi\left((g\operatorname{Ker}\varphi)\,(g'\operatorname{Ker}\varphi)\right)=\psi\left(gg'\operatorname{Ker}\varphi\right)=\varphi\left(gg'\right)=\varphi\left(g\right)\varphi\left(g'\right)=\psi\left(g\operatorname{Ker}\varphi\right)\cdot\psi\left(g'\operatorname{Ker}\varphi\right)$.

Итак, ψ — корректно определённый биективный гомоморфизм, то есть изоморфизм. ■

Таким образом, если $H\subseteq G$ — нормальная подгруппа и мы хотим понять, что собой представляет ${}^{G}\!/_{H}$, то для этих целей хорошо найти гомоморфизм $\varphi: G\to G_2$, где G_2 — какая-то известная группа, а $\operatorname{Ker}\varphi=H$. Тогда ${}^{G}\!/_{H}\cong\operatorname{Im}\varphi$, по теореме о гомоморфизме.

Пример 5. (Во всех примерах мы хотим описать, что такое ${}^{G}\!/_{H}$.)

1. Для $G=\mathbb{Z}$, $H=n\mathbb{Z}$ построим гомоморфизм $\varphi: G\to\mathbb{Z}_n$, $k\mapsto k+n\mathbb{Z}\Rightarrow\operatorname{Ker}\varphi=n\mathbb{Z}\Rightarrow{}^{G}\!/_{H}\cong\mathbb{Z}_n$.
2. Для $G=(\mathbb{R},+)$, $H=(\mathbb{Z},+)$ гомоморфизм определим как $\varphi\colon\mathbb{R}\to\mathbb{C}^{\times}$, $a\to e^{2\pi ia}\Rightarrow\operatorname{Im}\varphi=S^1\overset{\text{def}}{=}\{z\in\mathbb{C}\mid|z|=1\}$ — единичная окружность на комплексной плоскости с центром в начале координат $\Rightarrow{}^{G}\!/_{H}\cong S^1$.
3. Для $G=\mathbf{GL}_n\left(F\right)$, $H=\mathbf{SL}_n\left(F\right)$, где F — поле, построим гомоморфизм $\varphi:\mathbf{GL}_n\left(F\right)\to F^{\times}$, $A\mapsto\det A\Rightarrow$ $\Rightarrow\operatorname{Ker}\varphi=H$.

$$\forall\,a\neq0\ \exists\begin{pmatrix}a&0&\cdots&0\\0&1&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&1\end{pmatrix}\Rightarrow\operatorname{Im}\varphi=F^{\times}\Rightarrow{}^{G}\!/_{H}\cong F^{\times}.$$

Задача 11. *Пусть $G=\left(\mathbb{R}^2,+\right)$, $H=\left(\mathbb{Z}^2,+\right)$. Доказать, что ${}^{G}\!/_{H}$ изоморфна тору, и ввести на торе умножение.*

§ 6. Группы автоморфизмов

Пусть G — группа, $\operatorname{Aut}\left(G\right)$ — множество её автоморфизмов. Оно несёт каноническую структуры группы, на ней можно задать следующую операцию:

$$\varphi,\varphi'\in\operatorname{Aut}\left(G\right)\Rightarrow\varphi\circ\varphi'\in\operatorname{Aut}\left(G\right).$$

Необходимые свойства: ассоциативность верна для композиции любых отображений, в том числе и автоморфизмов; нейтральный элемент — тождественное отображение; обратный элемент — φ^{-1} (доказывалось в теореме 1).

Предложение 4.

1. $\operatorname{Aut}\left(\mathbb{Z}\right)\cong\mathbb{Z}_2$;
2. $\operatorname{Aut}\left(\mathbb{Z}_n\right)\cong\mathbb{Z}_n^{\times}$.

Конец лекции № 2 от 4 сентября 2013 г. (к началу)

Начало лекции № 3 от 9 сентября 2013 г.

□ Пусть $G=\langle g\rangle$. Тогда любой гомоморфизм $\varphi: G\to G_2$ однозначно определяется образом образующего элемента $\varphi\left(g\right)\in G_2$. В самом деле, $\varphi\left(g^m\right)=\varphi\left(g\right)^m\ \forall\,m\in\mathbb{Z}$.

Пусть $\varphi: G\to G$ — изоморфизм. Тогда, из его сюръективности, $\exists\,k\colon\varphi\left(g\right)=g^k$, и это порождающий элемент G.

1. У $\mathbb{Z}$ всего два порождающих. Для каждого из них есть гомоморфизм:
   - $\varphi_1: 1\mapsto1$ ($\varphi_1=\mathrm{id}$);
   - $\varphi_2: 1\mapsto-1$ ($\varphi_2=-\mathrm{id}$).

   Это автоморфизмы $\Rightarrow\left|\operatorname{Aut}\left(\mathbb{Z}\right)\right|=2\Rightarrow$ по следствию 4 из теоремы Лагранжа, $\operatorname{Aut}\left(\mathbb{Z}\right)\cong\mathbb{Z}_2$.
2. В $\mathbb{Z}_n$ порождающие — это $\overline{k}\colon\ (k,n)=1$.

   Построим $\varphi_{\overline{k}}\colon\overline{1}\mapsto\overline{k}$, $\overline{m}\mapsto\overline{km}$. Это отображение из множества в само себя сюръективно, то есть и биективно. Значит, это автоморфизм.

   Проверим, что отображение $\overline{k}\mapsto\varphi_{\overline{k}}$ сохраняет операцию. Действительно,

   $$\varphi_{\overline{s}}\left(\varphi_{\overline{k}}\left(\overline{m}\right)\right)=\overline{skm}=\varphi_{\overline{sk}}\left(\overline{m}\right).$$

   Значит, $\operatorname{Aut}\left(\mathbb{Z}_n\right)\cong\mathbb{Z}_n^{\times}$.

■

Задача 12. *Показать на примере, что $\mathbb{Z}_n^\times$ не всегда является циклической группой.*

Определение. Пусть G — произвольная группа, $g \in G$. *Внутренним автоморфизмом* группы G, определяемым g, называется отображение $i_g : G \to G,\ a \mapsto gag^{-1}$.

Проверим, что это автоморфизм:

$$i_g(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = i_g(a)\, i_g(b);$$

обратное к нему существует, это $i_{g^{-1}}$.

Множество всех внутренних автоморфизмов группы G обозначается как $\operatorname{Int}(G)$.

Лемма 3.

1. *Отображение $i\colon G \to \operatorname{Int}(G)$, $g \mapsto i_g$, является гомоморфизмом групп.*
2. $\operatorname{Int}(G) \subseteq \operatorname{Aut}(G)$ *— нормальная подгруппа.*

□

1. $i_{gh}(a) = gha(gh)^{-1} = ghah^{-1}g^{-1} = i_g(i_h(a)) = (i_g \circ i_h)(a)$, то есть операция сохраняется.
2. Поскольку $\operatorname{Int}(G) = \operatorname{Im} i \subseteq \operatorname{Aut}(G)$, то это подгруппа.

   Для проверки нормальности возьмём произвольные $\varphi \in \operatorname{Aut}(G)$ и $i_g \in \operatorname{Int}(G)$ и сопряжём их:

   $\left(\varphi i_g \varphi^{-1}\right)(a) = (\varphi i_g)\left(\varphi^{-1}(a)\right) = \varphi\left(g\varphi^{-1}(a)\, g^{-1}\right) = \varphi(g)\, a\varphi\left(g^{-1}\right) = \varphi(g)\, a\varphi(g)^{-1} = i_{\varphi(g)}(a)$.

   Таким образом, $\varphi i_g \varphi^{-1} \in \operatorname{Int}(G) \Rightarrow \operatorname{Int}(G) \subseteq \operatorname{Aut}(G)$ — нормальная подгруппа.

■

Определение. *Центром группы G* называется множество $Z(G) \stackrel{\text{def}}{=} \{g \in G \mid gg' = g'g \,\forall\, g' \in G\}$ всех элементов группы, коммутирующих со всеми элементами группы.

Ясно, что G абелева $\Leftrightarrow G = Z(G)$.

Лемма 4.

1. $Z(G) \subseteq G$ *— нормальная подгруппа.*
2. $i_g = \mathrm{id} \Leftrightarrow g \in Z(G)$.

□

1. То, что $Z(G)$ — подгруппа, следует из определения. Проверим нормальность.

   $\forall\, g \in Z(G), g' \in G\ g'g\left(g'\right)^{-1} = gg'\left(g'\right)^{-1} = g \in Z(G)$.
2. Проверим, что $i_g(a) = a\ \ \forall\, a \in G$:

   $g \in Z(G) \Leftrightarrow ga = ag \,\forall\, a \in G \Leftrightarrow gag^{-1} = a\ \ \forall\, a \in G \Leftrightarrow i_g(a) = a \,\forall\, a \in G$.

■

В частности, $\operatorname{Int}(G) = \{e\} \Leftrightarrow G$ абелева.

Предложение 5. *Для любой группы G $\operatorname{Int}(G) \cong {}^{G}\!/_{Z(G)}$.*

□ Расмотрим гомоморфизм $i\colon G \to \operatorname{Aut}(G)$, $g \mapsto i_g$. Тогда $\operatorname{Im} i = \operatorname{Int}(G)$, $\operatorname{Ker} i = Z(G)$, по лемме 4. По теореме 5 о гомоморфизме, $\operatorname{Im} i = \operatorname{Int}(G) \cong {}^{G}\!/_{\operatorname{Ker} i} = {}^{G}\!/_{Z(G)}$. ■

Пример 6.

1. $Z(\mathbf{S}_n) = \begin{cases} \mathbf{S}_n, & n \leqslant 2, \\ \{e\}, & n \geqslant 3. \end{cases}$

   Позже этот факт будет доказан.

   Задача 13. *Доказать, что* $Z(\mathbf{A}_n) = \begin{cases} \mathbf{A}_n, & n \leqslant 3, \\ \{e\}, & n \geqslant 4. \end{cases}$
2. $Z(\mathbf{GL}_n(\mathbb{C})) = \{\lambda E \mid \lambda \in \mathbb{C},\ \lambda \neq 0\} = \{\lambda E \mid \lambda \in \mathbb{C}^\times\}$.

   Задача 14. *Найти* $Z(\mathbf{SL}_n(\mathbb{C}))$.

3. $Z(\mathbf{D}_n) = \begin{cases} \pm e, & n = 2k, \\ e, & n = 2k+1. \end{cases}$
4. $Z(Q_8) = \{\pm 1\}$.

Задача 15. *Найти все группы G, для которых $\mathrm{Aut}(G)$ тривиальна (то есть $\mathrm{Aut}(G) = \{e\}$).*

§ 7. Классы сопряжённости

Определение. Пусть G — группа. Элементы $a, b \in G$ называются *сопряжёнными*, если $\exists\, g \in G$: $a = gbg^{-1}$.
Обозначение. $a \sim b$.
Классом сопряжённости элемента $a \in G$ называется множество $C_G(a) \stackrel{\text{def}}{=} \{b \in G \mid a \sim b\}$.

Лемма 5.

1. *Отношение сопряжённости есть отношение эквивалентности.*
2. $C_G(a) = \{a\} \Leftrightarrow a \in Z(G)$.

□

1. Отношение сопряжённости обладает следующими свойствами:
   - Рефлексивность: $a = eae^{-1} \Rightarrow a \sim a$.
   - Симметричность: $a = gbg^{-1} \Leftrightarrow b = g^{-1}ag$.
   - Транзитивность: $(a = gbg^{-1},\ b = hch^{-1} \Rightarrow a = ghch^{-1}g^{-1} = ghc(gh)^{-1}) \Rightarrow (a \sim b,\ b \sim c \Rightarrow a \sim c)$.

   Таким образом, это отношение эквивалентности.
2. $C_G(a) = \{a\} \Leftrightarrow gag^{-1} = a\, \forall\, g \in G \Leftrightarrow a \in Z(G)$.

■

Лемма 6. $b \in C_G(a) \Rightarrow \mathrm{ord}(b) = \mathrm{ord}(a)$.

□ Пусть $b = gag^{-1}$, $a^n = e$. Тогда $b^n = \left(gag^{-1}\right)^n = ga^ng^{-1} = gg^{-1} = e$ и наоборот (из симметричности сопряжённости) $\Rightarrow$ минимальные показатели совпадают. ■

Определение. *Централизатором* элемента $a \in G$ называется множество $Z_G(a) \stackrel{\text{def}}{=} \{g \in G \mid ga = ag\}$.
Ясно, что $Z_G(a) \subseteq G$ — подгруппа, но не обязательно нормальная.

Предложение 6. *Пусть G — конечная группа, $a \in G$. Тогда $|C_G(a)| = \frac{|G|}{|Z_G(a)|}$. В частности, $|C_G(a)| \,\big|\, |G|$.*

□ Пусть ${}^{G}\!/_{Z_G(a)}$ — множество левых смежных классов (это не факторгруппа! $Z_G(a)$ не обязательно нормальна). Достаточно установить биекцию ${}^{G}\!/_{Z_G(a)} \to C_G(a)$.
Определим отображение ${}^{G}\!/_{Z_G(a)} \to C_G(a)$, $gZ_G(a) \mapsto gag^{-1}$. Проверим:

1. корректность: $h \in Z_G(a) \Rightarrow ghZ_G(a) \mapsto (gh)a(gh)^{-1} = ghah^{-1}g^{-1} = gahh^{-1}g^{-1} = gag^{-1} \leftarrow\!\shortmid gZ_G(a)$;
2. сюръективность: по определению;
3. инъективность: $gag^{-1} = g'a(g')^{-1} \Leftrightarrow ag^{-1}g' = g^{-1}g'a \Leftrightarrow g^{-1}g' \in Z_G(a) \Leftrightarrow g' \in gZ_G(a)$.

■

Пример 7.

1. $G = \mathbf{S}_n$.

   Определение. *Циклической структурой* подстановки $a \in \mathbf{S}_n$ назовём неупорядоченное разбиение n: $n = k_1 + \ldots + k_s$, где $k_1, \ldots, k_s$ — длины независимых циклов a.

   Пример 8. $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 1 & 2 & 6 \end{pmatrix} = (134)(25)(6) \in \mathbf{S}_6 \Rightarrow$ циклическая структура a имеет вид $6 = 3 + 2 + 1$.

   Предложение 7. $C_{\mathbf{S}_n}(a) = \{b \in \mathbf{S}_n \mid$ *циклическая структура b = циклическая структура a*$\}$.

□ Пусть $a = (i_1 \dots i_{k_1}) \dots (j_1 \dots j_{k_s})$ — разложение a в независимые циклы, $g = \begin{pmatrix} 1 & 2 & \cdots & n \\ g(1) & g(2) & \cdots & g(n) \end{pmatrix}$.

Тогда рассмотрим gag^{-1}: $g(i_r) \overset{g^{-1}}{\longmapsto} i_r \overset{a}{\longmapsto} i_p \overset{g}{\longmapsto} g(i_p)$, где $r, p \in \{1, \dots, k_1\}$, $p \equiv r+1 \pmod{k_1} \Rightarrow$ $\Rightarrow g(i_1 \dots i_{k_1}) g^{-1} = (g(i_1) \dots g(i_{k_1})) \Rightarrow$ циклическая структура сохраняется, и за счёт выбора g можем получить таким образом любую подстановку той же циклической структуры. ■

Следствие. $Z(\mathbf{S}_n) = \begin{cases} \mathbf{S}_n, & n \leqslant 2, \\ \{e\}, & n \geqslant 3. \end{cases}$

□ При $n \geqslant 3$ любой класс сопряжённости, кроме $n = 1 + \dots + 1$, содержит не менее двух элементов. ■

Задача 16. *Описать классы сопряжённости в* $\mathbf{A}_5$.

2. $G = \mathbf{GL}_n(\mathbb{C})$. Из линейной алгебры известно, что две матрицы сопряжены, если они задают один и тот же линейный оператор в разных базисах. Значит, $C_{\mathbf{GL}_n(\mathbb{C})}(A) = \{B \mid J(B) = J(A)\}$, где $J(\cdot)$ — жорданова нормальная форма матрицы.

   Задача 17. *Описать классы сопряжённости в* $\mathbf{SL}_n(\mathbb{C})$.

3. $G = \mathbf{D}_n$ — группа диэдра; $|\mathbf{D}_n| = 2n$.

   Предложение 8. *Классы сопряжённости в* $\mathbf{D}_n$ *описываются следующим образом:*

   - $n = 2k$:

Число элементов	1	1	2	2	$\cdots$	k	k
Представители	e	$R(\pi)$	$R\left(\frac{\pi}{k}\right)$	$R\left(\frac{(k-1)\pi}{k}\right)$	$\cdots$	S_1	S_2

   - $n = 2k+1$:

Число элементов	1	2	$\cdots$	$2k+1$
Представители	e	$R(\varphi)$	$\cdots$	S

   □ Заметим, что $Z(R(\varphi)) \supset \{\text{повороты}\} \Rightarrow |Z(R(\varphi))| \geqslant n \Rightarrow |C(R(\varphi))| \leqslant \frac{2n}{n} = 2$.

   Для симметрий: $|Z(S)| \geqslant 2 \Rightarrow$ повороты $\sim$ только повороты ($|C(S)| \leqslant n$), симметрии $\sim$ только симметрии.

   Остаётся заметить, что $R_\varphi S_v R_{\varphi^{-1}} = S_{R_\varphi(v)}$, $SR_\varphi S = R_{-\varphi}$. ■

4. **Задача 18.** *Доказать, что классы сопряжённости в* Q_8 — $\{\pm 1\}$, $\{\pm i\}$, $\{\pm j\}$, $\{\pm k\}$.

Конец лекции № 3 от 9 сентября 2013 г. *(к началу)*

Начало лекции № 4 от 16 сентября 2013 г.

§ 8. Прямое произведение групп

8.1. Конструкция внешнего прямого произведения

Пусть $G_1, \dots, G_k$ — произвольные группы. Определим на $G_1 \times \dots \times G_k = \{(g_1, \dots, g_k) \mid g_i \in G_i\}$ операцию $(g_1, \dots, g_k)(g'_1, \dots, g'_k) \overset{\text{def}}{=} (g_1 g'_1, \dots, g_k g'_k)$ (именно в этом порядке). Это корректно определённая бинарная операция, её ассоциативность очевидна, нейтральный элемент $e = (e_1, \dots, e_k)$ и обратный к $g = (g_1, \dots, g_k)$ элемент $g^{-1} = (g_1^{-1}, \dots, g_k^{-1})$ предъявляются непосредственно. Значит, мы определили группу. Если $G_1, \dots, G_k$ конечны, то $|G_1 \times \dots \times G_k| = |G_1| \cdot \dots \cdot |G_k|$.

Заметим, что G_i изоморфна подгруппе $\{(e_1, \dots, e_{i-1}, g_i, e_{i+1}, \dots, e_k) \mid g_i \in G_i\} \subseteq G_1 \times \dots \times G_k$ (соответствующий изоморфизм — $g_i \overset{\varphi}{\longmapsto} (e_1, \dots, e_{i-1}, g_i, e_{i+1}, \dots, e_k)$), и эта подгруппа нормальна.

Замечание. Пусть $\{G_i \mid i \in I\}$ — произвольное (то есть не обязательно конечное) семейство групп. Тогда аналогично определяется их *прямое произведение* $\prod\limits_{i \in I} G_i = \{(g_i,\, i \in I)\}$.

Прямая сумма $\bigoplus\limits_{i \in I} G_i \subseteq \prod\limits_{i \in I} G_i$ — подгруппа, состоящая из наборов, в которых лишь конечное число элементов отлично от нейтральных e_i. Если $|I| < \infty$, то $\bigoplus\limits_{i \in I} G_i = \prod\limits_{i \in I} G_i$.

В дальнейшем будем работать с конечными семействами групп (то есть $|I| < \infty$), значок произведения $\prod$ будем использовать в общих случаях, а значок суммы $\bigoplus$ — для абелевых групп.

Задача 19. *Доказать, что* $Z(G_1 \times \dots \times G_k) = Z(G_1) \times \dots \times Z(G_k)$.

8.2. Внутреннее прямое произведение как свойство группы

Пусть G — произвольная группа, $H_1, \dots, H_k \subseteq G$ — подгруппы.

Определение. Группа G называется *прямым произведением* $H_1, \dots, H_k$, если:

1. $h_i h_j = h_j h_i \; \forall\, h_i \in H_i,\ h_j \in H_j$ при $i \neq j$;
2. $\forall\, g \in G \; \exists!$ запись вида $g = h_1 \dots h_k$, где $h_i \in H_i$.

Предложение 9. *Пусть $H_1 \times \dots \times H_k$ понимается как внешнее произведение групп, а G — их внутреннее произведение. Тогда отображение $H_1 \times \dots \times H_k \to G$, $(h_1, \dots, h_k) \mapsto h_1 \dots h_k$, является изоморфизмом групп.*

Замечание. *Сразу оговоримся, что в бесконечном случае предложение не имеет смысла: не определено бесконечное произведение $h_1 h_2 h_3 \dots$*

□ Биективность отображения следует из определения прямого произведения, точнее, из его второго пункта.
Проверим сохранение операции:

$$\begin{array}{ccccc} (h_1, \dots, h_k) & \cdot & (g_1, \dots, g_k) & = & (h_1 g_1, \dots, h_k g_k) \\ \downarrow & & \downarrow & & \downarrow \\ h_1 \dots h_k & \cdot & g_1 \dots g_k & \overset{?}{=} & h_1 g_1 \dots h_k g_k \end{array}$$

По условию, g_i коммутирует с h_j при $i \neq j$. Тогда, путём перестановок соседних множителей поставив в левом произведении g_1 после h_1, g_2 после h_2 и так далее, получим требуемое. ■

Следствие. Если G — прямое произведение подгрупп $H_1, \dots, H_k$, то $H_1, \dots, H_k$ нормальны в G.

Лемма 7. *Если $H_1,\ H_2 \lhd G$, $H_1 \cap H_2 = \{e\}$, то $h_1 h_2 = h_2 h_1 \; \forall\, h_1 \in H_1,\ h_2 \in H_2$.*

□ $\underbrace{h_1 \overbrace{h_2 h_1^{-1}}^{\in H_1} h_2^{-1}}_{\in H_2} \in H_1 \cap H_2 = \{e\} \Rightarrow h_1 h_2 h_1^{-1} h_2^{-1} = e \Rightarrow h_1 h_2 = h_2 h_1.$ ■

Предложение 10. *Группа G является прямым произведением подгрупп $H_1,\ H_2 \Leftrightarrow$ выполняются следующие условия:*

1. *H_1 и H_2 нормальны;*
2. *$H_1 \cap H_2 = \{e\}$;*
3. *$G = H_1 H_2$, то есть $\forall\, g \in G \; \exists\, h_1 \in H_1,\ h_2 \in H_2$: $g = h_1 h_2$.*

□

- $\boxed{\Rightarrow}$
  1. Из последнего следствия.
  2. Пусть $H_1 \cap H_2 \neq \{e\}$, то есть $\exists\, h \neq e$: $h \in H_1 \cap H_2$. Тогда, с одной стороны, $h = he$, где $h \in H_1$, $e \in H_2$, а с другой, $h = eh$, где $e \in H_1$, $h \in H_2$, что противоречит единственности разложения.
  3. По определению прямого произведения.
- $\boxed{\Leftarrow}$

  По лемме 7, из условий 1 и 2 следует, что $h_1 h_2 = h_2 h_1 \; \forall\, h_1 \in H_1,\ h_2 \in H_2$.

  Если $h_1 h_2 = g_1 g_2$, то $g_1^{-1} h_1 = g_2 h_2^{-1} \in H_1 \cap H_2 = \{e\} \Rightarrow g_1^{-1} h_1 = g_2 h_2^{-1} = e \Rightarrow g_1 = h_1,\ g_2 = h_2 \Rightarrow$ разложение единственно.

■

Замечание. Если в предложении 10 рассматривать, например, три подгруппы, то обобщение условий 1 и 3 очевидно, но записать условие 2 в виде $H_1 \cap H_2 = H_2 \cap H_3 = H_3 \cap H_1 = \{e\}$ будет неправильно.

Пример 9.

1. $\mathbf{V}_4 = \langle (12)(34) \rangle \times \langle (13)(24) \rangle$.
2. $\mathbb{C}^\times = \mathbb{R}^\times_{>0} \times S^1$, $z = |z|(\cos\varphi + i \sin\varphi)$.

3. $\mathbf{D}_n(F) = \left\{ \begin{pmatrix} * & 0 & \cdots & 0 \\ 0 & * & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & * \end{pmatrix} \right\} \cong \underbrace{F^\times \times \ldots \times F^\times}_{n}$.

Задача 20. *Привести пример сюръективного гомоморфизма $\varphi\colon G_1 \to G_2$: $G_1 \ncong \operatorname{Ker}\varphi \times G_2$.*

Предложение 11 (факторизация по сомножителям). *Пусть $G_1, \ldots, G_k$ — группы, H_i — нормальная подгруппа в G_i $\forall\, i \in \{1, \ldots, k\}$. Тогда:*

1. $H_1 \times \ldots \times H_k \lhd G_1 \times \ldots \times G_k$;
2. $\left.{}^{G_1 \times \ldots \times G_k}\right/_{H_1 \times \ldots \times H_k} \cong \left.{}^{G_1}\right/_{H_1} \times \ldots \times \left.{}^{G_k}\right/_{H_k}$.

□

1. То, что это подгруппа, и её нормальность проверяется непосредственно.
2. Установим изоморфизм: $(g_1, \ldots, g_k)(H_1 \times \ldots \times H_k) \leftrightarrow (g_1 H_1, \ldots, g_k H_k)$. То, что это изоморфизм, проверятся, опять же, непосредственно.

■

Пример 10. Если $G = G_1 \times G_2$, то $\left.{}^{G}\right/_{G_1} \cong G_2$.

Пример 11. $\left.{}^{\mathbb{R}^2}\right/_{\mathbb{Z}^2} = \left.{}^{\mathbb{R}\oplus\mathbb{R}}\right/_{\mathbb{Z}\oplus\mathbb{Z}} \cong \left.{}^{\mathbb{R}}\right/_{\mathbb{Z}} \oplus \left.{}^{\mathbb{R}}\right/_{\mathbb{Z}} = S^1 \oplus S^1$, что изоморфно тору. Фактически здесь изложено решение задачи 11.

Задача 21. *Верно ли, что* диагональ $\Delta G \overset{\text{def}}{=} \{(g, g) \mid g \in G\} \subseteq G \times G$ *— нормальная подгруппа?*

Замечание. Не любая (нормальная) подгруппа в $G_1 \times G_2$ имеет вид $H_1 \times H_2$, где $H_1 \subseteq G_1$, $H_2 \subseteq G_2$ — (нормальные) подгруппы.

Задача 22. *Привести пример, соответствующий замечанию.*

Предложение 12. *Пусть n, m, $k \in \mathbb{N}$, $n = mk$. Тогда $\mathbb{Z}_n \cong \mathbb{Z}_m \oplus \mathbb{Z}_k$*[2)] $\Leftrightarrow (m, k) = 1$.

□

- $\boxed{\Leftarrow}$

  Рассмотрим $(\overline{1}, \underline{1})$, где первая единица из $\mathbb{Z}_m$, а вторая — из $\mathbb{Z}_k$. $\exists\, s$ (например, $s = mk$): $s(\overline{1}, \underline{1}) = (\overline{0}, \underline{0}) \Rightarrow$ $\Rightarrow m \mid s$, $k \mid s \Rightarrow n = mk \mid s \Rightarrow \operatorname{ord}(\overline{1}, \underline{1}) = n \Rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_k$ циклическая.

- $\boxed{\Rightarrow}$

  Пусть, от противного, $(m, k) = d > 1$. Тогда $\forall\, (\overline{r}, \overline{q}) \in \mathbb{Z}_m \oplus \mathbb{Z}_k$ имеем $\frac{n}{d}(\overline{r}, \overline{q}) = (\overline{0}, \underline{0})$, так как $m \mid \frac{n}{d}$, $k \mid \frac{n}{d} \Rightarrow \operatorname{ord}(\overline{r}, \overline{q}) \leqslant \frac{n}{d} \Rightarrow$ группа не циклическая (нет элементов порядка n). Противоречие.

■

Пример 12. $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$, $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong \mathbf{V}_4$.

§ 9. Свободные абелевы группы

Пусть A — произвольная абелева группа.

Определение. *Подгруппой кручения*, или *периодической частью* (англ. *torsion subgroup*) группы A называется множество $T(A) = \{a \in A \mid \operatorname{ord}(a) < \infty\}$.

Пример 13. Если $|A| < \infty$, то $T(A) = A$.

Лемма 8. *$T(A)$ — подгруппа в A.*

□ Если $n = \operatorname{ord}(a)$, $m = \operatorname{ord}(b)$, то $nm(a + b) = 0 \Rightarrow \operatorname{ord}(a + b) < \infty$. ■

Замечание. В неабелевой группе элементы конечного порядка не всегда образуют подгруппу.

Задача 23. *Привести пример, соответствующий замечанию.*

Определение. Группа A называется *группой без кручения*, если $T(A) = \{0\}$.

Пример 14. $A = (\mathbb{Z}, +)$. Для элементов $a_1, \ldots, a_n \in A$ и $k_1, \ldots, k_n \in \mathbb{Z}$ можно определить *линейную комбинацию* $k_1 a_1 + \ldots + k_n a_n \in A$. Если $k_i < 0$, то $k_i a_i \overset{\text{def}}{=} (-k_i)(-a_i)$.

[2)] Группы здесь заведомо абелевы.

Определение. Группа A называется *конечнопорождённой*, если $\exists\, a_1, \ldots, a_n \in A$: $\forall\, a \in A$ $a = k_1 a_1 + \ldots + k_n a_n$ для некоторых $k_1, \ldots, k_n \in \mathbb{Z}$. Такой набор элементов $\{a_1, \ldots, a_n\}$ называется *системой порождающих*, или *образующих*.

Пример 15.

1. Любая конечная группа A конечнопорождена.
2. $\mathbb{Z}^n = \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{n} = \{(c_1, \ldots, c_n) \mid c_i \in \mathbb{Z}\}$. Её системой порождающих будет

$$\{e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)\}.$$

Задача 24. *Доказать, что группы $(\mathbb{Q}, +)$ и $(\mathbb{Q}^\times, \times)$ не конечнопорождены (хотя и счётны, а нетрудно видеть, что любая конечнопорождённая группа счётна).*

Определение. Система порождающих $\{a_1, \ldots, a_n\}$ группы A называется *базисом* в A, если $\forall\, a \in A$ запись $a = k_1 a_1 + \ldots + k_n a_n$ единственна.

Определение. Группа A, обладающая базисом, называется *свободной*.

Конец лекции № 4 от 16 сентября 2013 г. *(к началу)*

Начало лекции № 5 от 18 сентября 2013 г.

Пример 16.

1. Если $T(A) \neq \{0\}$, то A не свободна. В самом деле, если $0 \neq a \in T(A)$, $\operatorname{ord}(a) = m$, то $a = k_1 a_1 + \ldots + k_n a_n$. Тогда, с одной стороны, $0 = 0a_1 + \ldots + 0a_n$, с другой, $0 = mk_1 a_1 + \ldots + mk_n a_n\, (= ma) \Rightarrow$ противоречие с единственностью представления. В частности, свободные группы бесконечны.
2. $\mathbb{Z}^n$ свободна, её базис $\{e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)\}$ называется *стандартным*.
3. Элементы $a_1 = 2$ и $a_2 = 3$ порождают $\mathbb{Z}$, но из них нельзя составить базис.

Задача 25. *Приведите пример бесконечной конечнопорождённой, но не свободной абелевой группы.*

Предложение 13. *Все базисы свободной абелевой группы A содержат одно и то же число элементов.*

□ Пусть $\{e_1, \ldots, e_n\}$ и $\{e'_1, \ldots, e'_m\}$ — базисы в A, $m > n$. Выразим элементы второго базиса через элементы первого: $e'_i = \sum\limits_{j=1}^{n} c_{ji} e_j$, $C = (c_{ij}) \in \operatorname{Mat}_{n,m}(\mathbb{Z})$.

По основной лемме о линейной зависимости, применённой над полем $\mathbb{Q}$, столбцы C линейно зависимы $\Rightarrow$ $\Rightarrow$ $\exists\, \lambda_i = \frac{p_i}{q_i} \in \mathbb{Q}$, не все равные нулю: $\sum\limits_i \frac{p_i}{q_i} c_{ji} = 0\, \forall\, j$. Домножив это равенство на $d = [q_1, \ldots, q_m]$, получим $\sum\limits_i d_i e'_i = \sum\limits_i d_i \sum\limits_j c_{ji} e_j = \sum\limits_j \left(\sum\limits_i d_i c_{ji}\right) e_j = \sum\limits_j 0 e_j = 0$, где $d_i \in \mathbb{Z}$. Так как не все d_i равны нулю, получаем противоречие с тем, что $\{e'_1, \ldots, e'_m\}$ — базис в A. ■

Определение. Число элементов в базисе A называется *рангом* A, который обозначается $\operatorname{rk} A$. $\operatorname{rk}\{0\} \stackrel{\text{def}}{=} 0$.

Пример 17. $\operatorname{rk} \mathbb{Z}^n = n$.

Лемма 9. *Свободная абелева группа A ранга n изоморфна $\mathbb{Z}^n$.*

□ Если $\{e_1, \ldots, e_n\}$ — базис в A, то $a = k_1 e_1 + \ldots + k_n e_n \leftrightarrow (k_1, \ldots, k_n) \in \mathbb{Z}^n$. ■

Предложение 14. *Пусть $\{e_1, \ldots, e_n\}$ — базис в A, $e'_1 = \sum\limits_i c_{i1} e_i$, $\ldots$, $e'_n = \sum\limits_i c_{in} e_i$, $c_{ij} \in \mathbb{Z}$, $C = (c_{ij}) \in$ $\in \operatorname{Mat}_n(\mathbb{Z})$. Тогда $\{e'_1, \ldots, e'_n\}$ — базис в $A \Leftrightarrow \det C = \pm 1$.*

□ $\begin{pmatrix} e'_1 & \cdots & e'_n \end{pmatrix} = \begin{pmatrix} e_1 & \cdots & e_n \end{pmatrix} C$.

Заметим, что $\{e'_1, \ldots, e'_n\}$ является базисом $\Leftrightarrow$ $\{e_1, \ldots, e_n\}$ выражается через $\{e'_1, \ldots, e'_n\}$ (линейная независимость $e'_1, \ldots, e'_n$ вытекает из основной леммы о линейной зависимости) $\Leftrightarrow$ $\exists\, B = (b_{ij}) \in \operatorname{Mat}_n(\mathbb{Z})$: $\begin{pmatrix} e_1 & \cdots & e_n \end{pmatrix} =$ $= \begin{pmatrix} e'_1 & \cdots & e'_n \end{pmatrix} B = \begin{pmatrix} e_1 & \cdots & e_n \end{pmatrix} CB \Leftrightarrow CB = E$ (из единственности представления $\{e_1, \ldots, e_n\}$) $\Leftrightarrow$ C^{-1} существует и целочисленна.

Если $\det C = \pm 1$, то $C^{-1} = \frac{1}{\det C} \begin{pmatrix} C_{11} & \cdots & C_{n1} \\ \vdots & \ddots & \vdots \\ C_{1n} & \cdots & C_{nn} \end{pmatrix}$, где C_{ij} — алгебраическое дополнение к C $\Rightarrow$ C^{-1} целочисленна.

Обратно, пусть $\det C = d \neq \pm 1$. Тогда $\det C^{-1} = \frac{1}{\det C} = \frac{1}{d} \notin \mathbb{Z}$. ■

Пример 18. $A = \mathbb{Z}^2$, $e_1' = 2e_1 + 3e_2$, $e_2' = e_1 + e_2 \Rightarrow C = \begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix}$, $\det C = -1 \Rightarrow \{e_1', e_2'\}$ — базис.

Теорема 6. *Всякая подгруппа B свободной абелевой группы A ранга n является свободной абелевой группой ранга $\leqslant n$.*

□ Доказываем индукцией по n.

1. $n = 0 \Rightarrow$ очевидно.
2. Пусть $n > 0$, $\{e_1, \ldots, e_n\}$ — базис в A. Рассмотрим подгруппу $A_1 = \{k_1 e_1 + \ldots + k_{n-1} e_{n-1}\} \subseteq A$. По предположению индукции, $B_1 = B \cap A_1$ ($\operatorname{rk} A_1 = n - 1$) свободна и имеет ранг $m \leqslant n - 1$.

   Пусть теперь $\{f_1, \ldots, f_m\}$ — базис в B_1. Рассмотрим последние координаты всех элементов из B в базисе $\{e_1, \ldots, e_n\}$. Они образуют подгруппу в $\mathbb{Z}$. По предложению 2, она имеет вид $d\mathbb{Z}$, $d \in \mathbb{Z}_{\geqslant 0}$. Если $d = 0$, то последняя координата всегда равна нулю $\Rightarrow B = B_1$ и всё доказано. Если $d > 0$, то рассмотрим вектор $f_{m+1} \in B$ с последней координатой d. Тогда $\forall\, b \in B\, \exists\, s \in \mathbb{Z}$: $b - s f_{m+1} \in B_1 \Rightarrow \{f_1, \ldots, f_m, f_{m+1}\}$ порождают $B \Rightarrow \{f_1, \ldots, f_m, f_{m+1}\}$ — базис B: через них, как показано, всё выражается, $\{f_1, \ldots, f_m\}$ линейно независимы (так как были выбраны базисом) и имеют нулевую последнюю координату, а f_{m+1} имеет ненулевую последнюю координату, поэтому он линейно независим со всеми остальными.

■

Замечание. Если для конечного векторого пространства $U \subseteq V$, $\dim U = \dim V \Rightarrow U = V$, то для свободной абелевой группы $B \subseteq A$, $\operatorname{rk} B = \operatorname{rk} A \not\Rightarrow B = A$. Например, $A = \mathbb{Z}$, $B = d\mathbb{Z}$, $\operatorname{rk} \mathbb{Z} = \operatorname{rk} d\mathbb{Z} = 1$.

В дальнейшем нашей целью станет описать подгруппы в $\mathbb{Z}^n$.

Определение. *Целочисленные элементарные преобразования строк матриц*:

1. прибавление к строке другой, умноженной на целое число;
2. перестановка двух строк;
3. умножение строки на ± 1 (из соображений обратимости разрешены только эти два числа).

Для столбцов аналогично.

Определение. Матрица $C = (c_{ij}) \operatorname{Mat}_{n,m}(F)$ называется *диагональной*, если $c_{ij} = 0\, \forall\, i \neq j$.

Обозначение. $c_{ii} = u_i$, $i \in \{1, \ldots, p = \min\{m, n\}\} \Rightarrow C = \operatorname{diag}(u_1, \ldots, u_p)$.

Предложение 15. *Любую целочисленную матрицу целочисленными элементарными преобразованиями её строк и столбцов можно привести к виду* $\operatorname{diag}(u_1, \ldots, u_p)$, *где* $u_i \geqslant 0\ \forall\, i \in \{1, \ldots, p\}$, $u_i \mid u_{i+1}\, \forall\, i \in \{1, \ldots, p-1\}$.

□ Пусть $C \in \operatorname{Mat}_{n,m}(\mathbb{Z})$. Если $C = 0$, то всё верно.

Пусть $C \neq 0$. Переставляя строки и столбцы, считаем, что $c_{11} \neq 0$. Умножая первую строку на ± 1, считаем, что $c_{11} > 0$. Хотим уменьшить c_{11}, оставляя его положительным.

Сначала передвигаемся по первому столбцу матрицы. Если $c_{11} \nmid c_{i1}$ для некоторого $i \in \{2, \ldots, n\}$, то, по теореме о делении с остатком, $c_{i1} = c_{11} q + r$, где $0 < r < c_{11}$. Вычтя из i-й строки первую q раз, получим r на месте c_{i1}. Поменяв теперь местами i-ю и первую строки, получим r на месте c_{11} и c_{11} на месте c_{i1}. Поскольку значение в левом верхнему углу (бывшее c_{11}) уменьшается и остаётся положительным, то процесс надо будет повторить конечное число раз, и мы добьёмся того, что $c_{11} \mid c_{i1}\, \forall\, i \in \{2, \ldots, n\}$. Совершая теперь то же самое со строкой, получим, что $c_{11} \mid c_{1j}\, \forall\, j \in \{2, \ldots, m\}$.

Перейдём теперь к элементам других строк и столбцов. Пусть $\exists\, i \in \{2, \ldots, n\}$, $j \in \{2, \ldots, m\}$: $c_{11} \nmid c_{ij}$. Так как $c_{11} \mid c_{i1}$, то, вычтя нужное количество раз первую строку из i-й, получим $c_{i1} = 0$. Прибавим к первой строке i-ю и повторим вышеописанный процесс уменьшения c_{11}. Аналогично видим, что процесс рано или поздно завершится, и мы получим, что $c_{11} \mid c_{ij}\, \forall\, i \in \{2, \ldots, n\}$, $j \in \{2, \ldots, m\}$.

Обнулим теперь все элементы первого столбца и первой строки, кроме c_{11}, вычитаниями первого столбца или строки из остальных нужное количество раз. Поскольку все элементы матрицы делятся на c_{11}, то подобные элементарные преобразования эту делимость не устранят. Таким образом, получится матрица вида

$$\begin{pmatrix} c_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & c_{11} C_1 & \\ 0 & & & \end{pmatrix},$$

к которой можно применить принцип математической индукции и получить $\begin{pmatrix} c_{11} & 0 & \cdots & 0 \\ 0 & c_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \ddots \end{pmatrix}$. ■

Пример 19. $\begin{pmatrix}2&0\\0&3\end{pmatrix} \longrightarrow \begin{pmatrix}2&2\\0&3\end{pmatrix} \longrightarrow \begin{pmatrix}2&-1\\0&3\end{pmatrix} \longrightarrow \begin{pmatrix}1&-1\\3&3\end{pmatrix} \longrightarrow \begin{pmatrix}1&0\\3&6\end{pmatrix} \longrightarrow \begin{pmatrix}1&0\\0&6\end{pmatrix}$.

Теорема 7 (о согласованных базисах). *Пусть A — свободная группа ранга n и $B \subseteq A$ — подгруппа ранга $m \leqslant n$. Тогда существует базис $\{e_1, \ldots, e_n\}$ в A и такие $u_1, \ldots, u_m \in \mathbb{N}$, что $\{u_1 e_1, \ldots, u_m e_m\}$ — базис в B и $u_i \mid u_{i+1} \, \forall\, i \in \{1, \ldots, m-1\}$.*

Конец лекции № 5 от 18 сентября 2013 г. *(к началу)*

Начало лекции № 6 от 23 сентября 2013 г.

□ Пусть $\{\widetilde{e_1}, \ldots, \widetilde{e_n}\}$ — базис в A, $\left\{\widetilde{f_1}, \ldots, \widetilde{f_m}\right\}$ — базис в B. Тогда $\begin{pmatrix}\widetilde{f_1} & \cdots & \widetilde{f_m}\end{pmatrix} = \begin{pmatrix}\widetilde{e_1} & \cdots & \widetilde{e_n}\end{pmatrix} C$, где $C \in \mathrm{Mat}_{n,m}(\mathbb{Z})$, $\operatorname{rk} C = m$.

Введём элементарные преобразования над базисом:

1. прибавление к одному базисному вектору другого, умноженного на целое число (но не самого себя!);
2. перестановка двух базисных векторов;
3. умножение базисного вектора на ± 1.

Ясно, что такие преобразования оставляют базис базисом. Что при них происходит с C? Преобразования базиса B есть в точности элементарные преобразования столбцов C, а преобразования базиса A есть в точности элементарные преобразования строк C. Таким образом, мы можем, по предложению 15, привести C к виду $\operatorname{diag}(u_1, \ldots, u_m)$, где $u_i \in \mathbb{N}$ ($u_i \neq 0$, так как $\operatorname{rk} C = m$) и $u_i \mid u_{i+1}$. Значит, в новых базисах $\{e_1, \ldots, e_n\}$ и $\{f_1, \ldots, f_m\}$ мы имеем $f_1 = u_1 e_1, \ldots, f_m = u_m e_m$. ■

Определение. Числа $u_1, \ldots, u_m$ называются *инвариантными множителями* подгруппы $B \subseteq A$.

Рассмотрим факторгруппу ${}^{A}\!/_{B}$: ${}^{A}\!/_{B} = {}^{\langle e_1\rangle \oplus \ldots \oplus \langle e_n\rangle}\!/_{\langle f_1\rangle \oplus \ldots \oplus \langle f_m\rangle} \cong {}^{\langle e_1\rangle}\!/_{\langle u_1 e_1\rangle} \oplus \ldots \oplus {}^{\langle e_m\rangle}\!/_{\langle u_m e_m\rangle} \oplus {}^{\langle e_{m+1}\rangle}\!/_{\langle 0\rangle} \oplus \ldots \oplus \oplus {}^{\langle e_n\rangle}\!/_{\langle 0\rangle} \cong {}^{\mathbb{Z}}\!/_{u_1\mathbb{Z}} \oplus \ldots \oplus {}^{\mathbb{Z}}\!/_{u_m\mathbb{Z}} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \cong \mathbb{Z}^{n-m} \oplus \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m}$, по предложению 11 о факторизации по сомножителям. Тем самым доказано

Предложение 16. *Факторгруппа свободной абелевой группы по произвольной подгруппе изоморфна $\mathbb{Z}^r \oplus \oplus \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m}$, где $u_i \in \mathbb{N}$, $u_i \mid u_{i+1}$, $r \in \mathbb{Z}_{\geqslant 0}$.*

Следствие. Если $\operatorname{rk} A = \operatorname{rk} B$, то $u_1 u_2 \ldots u_n = \left|{}^{A}\!/_{B}\right| = [A : B]$. В частности, это произведение не зависит от выборов согласованных базисов.

Предложение 17 (универсальное свойство свободных абелевых групп). *Пусть A — свободная абелева группа с базисом $\{e_1, \ldots, e_n\}$, D — произвольная абелева группа, $d_1, \ldots, d_n \in D$ — произвольные элементы. Тогда $\exists!$ гомоморфизм $\varphi\colon A \to D$, $\varphi(e_i) = d_i \, \forall\, i \in \{1, \ldots, n\}$.*

□ $\forall\, a \in A \; a = k_1 e_1 + \ldots + k_n e_n$. Тогда положим $\varphi(a) = k_1 \varphi(e_1) + \ldots + k_n \varphi(e_n)$. Это гомоморфизм, что проверяется очевидным образом. ■

Следствие. Для любой конечнопорождённой абелевой группы D существует сюръективный гомоморфизм $\varphi\colon A \to D$ для некоторой свободной абелевой группы A.

□ Пусть $d_1, \ldots, d_n$ — порождающие элементы группы D. Тогда положим $A = \mathbb{Z}^n$ и определим φ условием $\varphi(e_i) = d_i$, где $\{e_1, \ldots, e_n\}$ — стандартный базис в $\mathbb{Z}^n$. Тогда φ сюръективен, так как $d_1, \ldots, d_n$ — порождающие. ■

§ 10. Структура абелевых групп

Следствие 9 позволяет описать все конечнопорождённые абелевы группы.

Теорема 8. *Любая конечнопорождённая абелева группа изоморфна $\mathbb{Z}^r \oplus \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m}$, где $u_i \in \mathbb{N}$, $u_i \mid u_{i+1}$, $r \in \mathbb{Z}_{\geqslant 0}$.*

□ Пусть D — конечнопорождённая абелева группа, $\varphi\colon \mathbb{Z}^n \twoheadrightarrow$ [3] D — сюръективный гомоморфизм. Тогда, по теореме 5 о гомоморфизме, $D \cong {}^{\mathbb{Z}^n}\!/_{B}$, где $B = \operatorname{Ker}\varphi$. По предложению 16, факторгруппа свободной абелевой группы имеет требуемый вид. ■

Разберёмся с конечными абелевыми группами.

Определение. Пусть p — простое. Группа A называется *p-примарной*, если $|A| = p^k$ для некоторого $k \in \mathbb{Z}_{\geqslant 0}$. A называется *примарной*, если она p-примарна для некоторого p.

Теорема 9. *Любая конечная абелева группа A изоморфна прямой сумме примарных циклических групп:*

$$A \cong \mathbb{Z}_{p_1^{k_{11}}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{k_{1r_1}}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{k_{sr_s}}}; \qquad (*)$$

[3] Такой «двухголовой» стрелкой обозначаются сюръективные отображения.

такое разложение единственно с точностью до порядка слагаемых.

□ Из теоремы 8 мы знаем, что

$$A \cong \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m}. \qquad (**)$$

Можно считать, что $u_i \geqslant 2$. Если $u_i = p_{i_1}^{k_{i_1}} \ldots p_{i_q}^{k_{i_q}}$, то $\mathbb{Z}_{u_i} \cong \mathbb{Z}_{p_{i_1}^{k_{i_1}}} \oplus \ldots \oplus \mathbb{Z}_{p_{i_q}^{k_{i_q}}} \Rightarrow A$ разлагается в прямую сумму примарных циклических групп.

Теперь докажем единственность разложения. Определим подгруппу $\mathrm{Tor}_p(A) \stackrel{\text{def}}{=} \{a \in A \mid \exists k \in \mathbb{N}\colon p^k a = 0\} = \{a \in A \mid \exists s\colon \mathrm{ord}(a) = p^s\}$. В разложении $(*)$ $\mathrm{Tor}_{p_1}(A) \cong \mathbb{Z}_{p_1^{k_{11}}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{k_{1r_1}}} \Rightarrow A = \mathrm{Tor}_{p_1}(A) \oplus \ldots \oplus \mathrm{Tor}_{p_s}(A)$. Остаётся доказать, что разложение $\mathrm{Tor}_p(A)$ в прямую сумму циклических подгрупп однозначно.

Далее считаем, что $A = \mathrm{Tor}_p(A)$ и $|A| = p^k$, где $k = k_1 + \ldots + k_r$. Будем вести индукцию по k.

1. $k = 0 \Rightarrow |A| = p^0 = 1 \Rightarrow A = \{0\}$, разложение однозначно.
2. Пусть $k \geqslant 1$. Рассмотрим подгруппу $pA = \{pa \mid a \in A\} \subseteq A$. Тогда $pA \cong p\mathbb{Z}_{p^{k_1}} \oplus \ldots \oplus p\mathbb{Z}_{p^{k_r}} \cong \mathbb{Z}_{p^{k_1-1}} \oplus \ldots \oplus \mathbb{Z}_{p^{k_r-1}}$. В частности, если $k_i = 1$, то соответствующее слагаемое исчезает. По предположению индукции, применённому к pA, числа $k_1 - 1, \ldots, k_s - 1$ определены однозначно при $k_i \geqslant 2$, а число единиц $(k_j = 1)$ восстанавливается как $k - \sum\limits_{k_i \geqslant 2} k_i$.

■

Замечание. Сами циклические слагаемые в разложении $(*)$ определены неоднозначно.

Пример 20. $\mathbf{V}_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$;
$\mathbf{V}_4 = \langle (12)(34) \rangle \oplus \langle (13)(24) \rangle = \langle (12)(34) \rangle \oplus \langle (14)(23) \rangle$.

Инвариантность инвариантных множителей — как их восстановить по разложению $(*)$?

Пример 21. $A = \mathbb{Z}_{2^3} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$;
$A = \mathbb{Z}_{2^3 \cdot 3^2 \cdot 5 = u_3} \oplus \mathbb{Z}_{2^2 \cdot 3 = u_2} \oplus \mathbb{Z}_{2^2 = u_1}$.

Задача 26. *Перечислить с точностью до изоморфизма все абелевы группы порядка 36.*

Решение. $36 = 2^2 \cdot 3^2$.

- $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2} \cong \mathbb{Z}_{36}$;
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2}$;
- $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$;
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_6$.

■

Конец лекции № 6 от 23 сентября 2013 г. *(к началу)*

Начало лекции № 7 от 30 сентября 2013 г.

Задача 27 (обратная теорема Лагранжа). *Пусть A — абелева группа, $|A| = n$, $d \mid n$. Тогда $\exists$ подгруппа $B \subseteq A$: $|B| = d$.*

Определение. *Экспонентой*, или *показателем* конечной группы G (не обязательно абелевой) называется наименьшее общее кратное порядков её элементов.

Обозначение. $\exp(G)$.

Пример 22.

1. $\exp(\mathbb{Z}_n) = n$;
2. $\exp(\mathbb{Z}_2 \oplus \mathbb{Z}_2) = 2$;
3. $\exp(\mathbf{S}_3) = 6$.

Лемма 10.

1. $\forall g \in G\ g^{\exp(G)} = e$;

2. $\exp(G) \mid |G|$.

□

1. $\forall g \in G\ \mathrm{ord}(g) \mid \exp(G)$, по определению экспоненты $\Rightarrow g^{\exp(G)} = e$.

2. По теореме 2 Лагранжа, $\forall\, g \in G \ \operatorname{ord}(g) \,\big|\, |G| \Rightarrow \exp(G) = \operatorname{НОК}(\operatorname{ord}(g),\, g \in G) \,\big|\, |G|$.

■

Предложение 18. *Пусть A — конечная абелева группа. Тогда её экспонента равна её последнему инвариантному множителю.*

□ По теореме 8, $A \cong \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m}$, где $u_i \,\big|\, u_{i+1} \,\forall\, i \in \{1, \ldots, m-1\}$. Тогда $\forall\, a \in A$: $a = (\overline{a_1}, \ldots, \overline{a_m})$ $\operatorname{ord}(a) = \operatorname{НОК}(\operatorname{ord}(\overline{a_i}),\, i \in \{1, \ldots, m\})$. Так как $\operatorname{ord}(\overline{a_i}) \,\big|\, |\mathbb{Z}_{u_i}| = u_i$, а u_m делится на все u_i, то $\operatorname{ord}(a)$ является делителем u_m. Таким образом, $\exp(A) \,\big|\, u_m$. С другой стороны, $\operatorname{ord}(\overline{0}, \ldots, \overline{0}, \overline{1}) = u_m \Rightarrow \exp(A) = u_m$. ■

Следствие.

1. В конечной абелевой группе A существует элемент a: $\operatorname{ord}(a) = \exp(A)$.
2. A — циклическая $\Leftrightarrow |A| = \exp(A)$.

Предложение 19. *Любая конечная подгруппа мультипликативной группы поля является циклической.*

□ Пусть F — поле, $F^\times = F \setminus \{0\}$ — мультипликативная группа поля, $A \subseteq F^\times$ — конечная подгруппа, $m = \exp(A)$. Тогда, по лемме 10, $a^m = 1 \,\forall\, a \in A$. Но уравнение $x^m - 1 = 0$ имеет в поле $\leqslant m$ корней, по теореме Безу $\Rightarrow |A| \leqslant m$. С другой стороны, $m \,\big|\, |A|$, по той же лемме $\Rightarrow m = |A| \Leftrightarrow A$ — циклическая, по следствию из предложения 18. ■

Следствие. Если поле F конечно, то $F^\times$ — циклическая.

Пример 23. $\mathbb{Z}_p^\times$ — циклическая группа порядка $p - 1$.

Теорема 10. *Пусть A — конечнопорождённая абелева группа. Тогда разложение $A \cong \mathbb{Z}^r \oplus \mathbb{Z}_{p_1^{k_{11}}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{k_{sr_s}}}$ единственно с точностью до порядка слагаемых.*

□ Заметим, что $\operatorname{Tor}(A) = \mathbb{Z}_{p_1^{k_{11}}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{k_{sr_s}}} \Rightarrow$ конечные циклические слагаемые определены однозначно, по теореме 9.

Далее, $A/\operatorname{Tor}(A) \cong \mathbb{Z}^r$, по теореме 11 о факторизации по слагаемым $\Rightarrow r = \operatorname{rk}\left(A/\operatorname{Tor}(A)\right)$, но ранг абелевой группы определён корректно и от разложения не зависит. ■

Задача 28. *Доказать, что любая подгруппа и любая факторгруппа конечнопорождённой абелевой группы конечнопорождена.*

§ 11. Порождающие элементы

Пусть G — произвольная группа, $S \subseteq G$ — подмножество.

Определение. Подгруппа в G называется *порождённой подмножеством* S, если эта группа есть множество элементов вида $g_{i_1}^{\varepsilon_1} \ldots g_{i_k}^{\varepsilon_k}$, где $g_{i_j} \in S$, $\varepsilon_j \in \{\pm 1\}$.

Обозначение. $\langle S \rangle$.

Это подгруппа, так как $\left(g_{i_1}^{\varepsilon_1} \ldots g_{i_k}^{\varepsilon_k}\right)\left(g_{j_1}^{\tau_1} \ldots g_{j_s}^{\tau_s}\right) \in \langle S \rangle$, $\left(g_{i_1}^{\varepsilon_1} \ldots g_{i_k}^{\varepsilon_k}\right)^{-1} = g_{i_k}^{-\varepsilon_k} \ldots g_{i_1}^{-\varepsilon_1} \in \langle S \rangle$. Легко заметить, что это наименьшая подгруппа в G, содержащая S.

Пример 24. $S = \{a, b\} \Rightarrow \langle S \rangle = \left\{a^{k_1} b^{k_2} a^{k_3} b^{k_4} \ldots \mid k_i \in \mathbb{Z}\right\}$.

Определение. Группа G *порождена множеством* S, если $G = \langle S \rangle$.

Вспомним из первого курса, что группа подстановок $\mathbf{S}_n$ порождается транспозициями (ij) и даже транспозициями вида $(12), (13), \ldots, (1n)$ или $(12), (23), \ldots, ((n-1)\, n)$.

Задача 29. *Доказать, что группа $\mathbf{S}_n$ порождается (12) и $(12 \ldots n)$.*

Предложение 20. *Группа $\mathbf{A}_n$ порождается:*

1. *парами транспозиций;*
2. *тройными циклами (то есть циклами длины 3);*
3. *парами независимых транспозиций при $n \geqslant 5$.*

□

1. $\forall\, \sigma \in \mathbf{S}_n$ $\sigma = \tau_1 \ldots \tau_k$, где τ_i — транспозиция. Если σ чётна, то $k = 2s \Rightarrow \sigma = (\tau_1 \tau_2) \ldots (\tau_{2s-1} \tau_{2s})$.
2. Выразим пары транспозиций через тройные циклы:

$$(ij)\,(ij) = e, \qquad (ij)\,(jk) = (ijk), \qquad (ij)\,(kl) = (ijk)\,(jkl).$$

3. Выразим пару зависимых транспозиций через пары независимых транспозиций:

$$(ij)(jk) = ((ij)(lm))((jk)(lm)), \qquad l, m \notin \{i, j, k\}.$$

■

Замечание. При $n = 4$ пары независимых транспозиций порождают $\mathbf{V}_4 \neq \mathbf{A}_4$.

Пример 25. $\mathbf{D}_n = \left\langle R\left(\frac{2\pi}{n}\right), S\right\rangle$, где S — любая симметрия. В самом деле, в $\left\langle R\left(\frac{2\pi}{n}\right), S\right\rangle$ лежат все повороты (группа поворотов — циклическая и порождается $R\left(\frac{2\pi}{n}\right)$) и как минимум ещё один элемент, то есть больше половины элементов $\Rightarrow$ по теореме 2 Лагранжа, $\left\langle R\left(\frac{2\pi}{n}\right), S\right\rangle = \mathbf{D}_n$.

Задача 30. *Найти минимальную систему порождающих группы* Q_8.

Предложение 21. *Пусть* F *— поле. Тогда:*

1. *группа* $\mathbf{GL}_n(F)$ *порождается элементарными матрицами;*
2. *группа* $\mathbf{SL}_n(F)$ *порождается элементарными матрицами первого типа, то есть матрицами вида* $E + cE_{ij}$, $i \neq j$.

□

1. Пусть $A \in \mathbf{GL}_n(F)$. Её методом Гаусса, применяя элементарные преобразования строк, можно привести к ступенчатому виду. Но поскольку невырожденность матрицы при таких преобразованиях не меняется, то матрица будет иметь не просто ступенчатый, а верхнетреугольный вид. Дальнейшими преобразованиями можно получить диагональ, состоящую из единиц, а с её помощью — единичную матрицу. Вспомним теперь, что этим преобразованиям соответствуют некоторые элементарные матрицы $U_1, \ldots, U_r$: $U_r \ldots U_1 A = E \Rightarrow A = U_1^{-1} \ldots U_r^{-1}$, при этом известно, что обратные к элементарным матрицам — элементарные. Значит, A представима в виде произведения элементарных матриц.
2. Требуется доказать, что $A \in \mathbf{SL}_n(F)$ может быть приведена к единичной матрице с использованием элементарных преобразований строк только первого типа.

   В предыдущем пункте в приведении к ступенчатому виду, а также при переходе от матрицы с единичной диагональю к единичной матрице используются только нужные преобразования. Как можно разобраться с переходом от ступенчатого вида к матрице с единичной диагональю? Формально описывать это не будем, рассмотрим пример:

$$\begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \to \begin{pmatrix} 2 & 0 \\ 2 & \frac{1}{2} \end{pmatrix} \to \begin{pmatrix} 1 & -\frac{1}{4} \\ 2 & \frac{1}{2} \end{pmatrix} \to \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

   Последний диагональный элемент в любом случае будет единицей, так как $\det A = 1$.

■

§ 12. Коммутант

Пусть G — произвольная группа.

Определение. *Коммутатором* двух элементов $x, y \in G$ называется $[x, y] \stackrel{\text{def}}{=} xyx^{-1}y^{-1} \in G$.

Легко заметить, что:

1. $[x, y] = e \Leftrightarrow x$ и y коммутируют;
2. $xy = [x, y]\, yx$, поэтому говорят, что $[x, y]$ — *корректирующий член.*

Определение. *Коммутантом*, или *производной подгруппой* группы G называется подгруппа $G' \subseteq G$ (иногда $[G, G]$), порождённая всеми коммутаторами в G.

Конец лекции № 7 от 30 сентября 2013 г. *(к началу)*

Начало лекции № 8 от 2 октября 2013 г.

Замечание.

1. $e = [x, x]$;
2. $[x, y]^{-1} = \left(xyx^{-1}y^{-1}\right)^{-1} = yxy^{-1}x^{-1} = [y, x]$.

Отсюда соблазнительно сделать вывод, что, поскольку нейтральный элемент — коммутатор и обратный к коммутатору — коммутатор, все коммутаторы сами по себе уже образуют подгруппу в G. Но не факт, что произведение коммутаторов — коммутатор.

Задача 31. *Привести пример группы G и элементов $x, y, z, t \in G$: $[x, y]\,[z, t]$ — не коммутатор никаких двух элементов G.*

Замечание. $G' = \{e\} \Leftrightarrow G$ абелева.

Пример 26. $G = \mathbf{S}_n \Rightarrow [\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ — чётная $\Rightarrow G' \subseteq \mathbf{A}_n$. С другой стороны, $\mathbf{A}_n$, по предложению 20, порождается тройными циклами, которые, в свою очередь, представимы как коммутаторы: $(ijk) = (ij)\,(ik)\,(ij)\,(ik) = (ij)\,(ik)\,(ij)^{-1}\,(ik)^{-1} = [(ij), (ik)] \Rightarrow \mathbf{A}_n \subseteq G' \Rightarrow \mathbf{A}_n = G'$.

Предложение 22. *Пусть G — произвольная группа. Тогда:*

1. *$G' \triangleleft G$;*
2. *G/G' абелева;*
3. *если $N \triangleleft G$, то G/N абелева $\Leftrightarrow G' \subseteq N$;*
4. *если $G' \subseteq K \subseteq G$, K — подгруппа, то $K \triangleleft G$.*

□ Доказывать будем только общие факты 3 и 4, из которых сразу следуют 2 и 1, соответственно.

3. $\forall g, h \in G\ (gN)\,(hN) = (hN)\,(gN) \Leftrightarrow (gN)\,(hN)\,(gN)^{-1}\,(hN)^{-1} = \left(ghg^{-1}h^{-1}N\right) = eN \Leftrightarrow ghg^{-1}h^{-1} \in N \Leftrightarrow$ N содержит все коммутаторы $\Leftrightarrow G' \subseteq N$.
4. Если $g \in G$, $k \in K$, то $gkg^{-1} = gkg^{-1}k^{-1}k = [g, k]\,k$. Так как $[g, k] \in K$, $k \in K$, то $gkg^{-1} \in K \Rightarrow K \triangleleft G$.

■

Лемма 11. *Пусть $\varphi\colon G_1 \to G_2$ — гомоморфизм. Тогда $\varphi(G_1') \subseteq G_2'$. Если φ сюръективен, то $\varphi(G_1') = G_2'$.*

□ $\varphi([x, y]) = \varphi\left(xyx^{-1}y^{-1}\right) = \varphi(x)\,\varphi(y)\,\varphi\left(x^{-1}\right)\varphi\left(y^{-1}\right) = \varphi(x)\,\varphi(y)\,\varphi(x)^{-1}\,\varphi(y)^{-1} = [\varphi(x), \varphi(y)] \in G_2' \Rightarrow$
$\Rightarrow \varphi(G_1') \subseteq G_2'$.
Если φ сюръективен и $a, b \in G_2$, то $\exists x, y \in G_1$: $a = \varphi(x)$, $b = \varphi(y)$. Тогда $[a, b] = [\varphi(x), \varphi(y)] = \varphi([x, y]) \in$
$\in \varphi(G_1') \Rightarrow G_2' \subseteq \varphi(G_1')$. ■

Определение. Пусть G — группа. Тогда подгруппа $H \subseteq G$ называется *характеристической*, если она устойчива относительно всех автоморфизмов, то есть $\forall \varphi \in \mathrm{Aut}(G)\ \varphi(H) = H$.

Замечание. Любая характеристическая подгруппа нормальна, так как нормальность, по определению, — устойчивость относительно внутренних автоморфизмов.

Задача 32. *Привести пример нормальной подгруппы, не являющейся характеристической.*

Замечание. Для проверки того, что $H \subseteq G$ — характеристическая подгруппа, достаточно убедиться, что $\forall \varphi \in \mathrm{Aut}(G)\ \varphi(H) \subseteq H$. В самом деле, воспользуемся этим включением для автоморфизма φ^{-1}: $\varphi^{-1}(H) \subseteq H \Rightarrow$
$\Rightarrow \varphi\left(\varphi^{-1}(H)\right) = H \subseteq \varphi(H) \Rightarrow \varphi(H) = H$.

Задача 33. *Привести пример группы G, подгруппы $H \subseteq G$ и $\varphi \in \mathrm{Aut}(G)$, для которых $\varphi(H) \subsetneq H$.*

Пример 27. $Z(G) \subseteq G$ — характеристическая подгруппа. В самом деле, надо доказать, что $\forall b \in G$, $\varphi \in$
$\in \mathrm{Aut}(G)$, $a \in Z(G)$ $\varphi(a)\,b = b\varphi(a)$. Поскольку φ — биекция, то $\exists c \in G$: $b = \varphi(c) \Rightarrow \varphi(a)\,\varphi(c) = \varphi(ac) =$
$= \varphi(ca) = \varphi(c)\,\varphi(a) \Rightarrow \varphi(Z(G)) \subseteq Z(G)\ \forall \varphi \in \mathrm{Aut}(G) \Rightarrow$ по последнему замечанию, $\varphi(Z(G)) = Z(G)$.

Предложение 23. *Коммутант группы — это её характеристическая подгруппа.*

□ Достаточно проверить, что $\forall \varphi \in \mathrm{Aut}(G)\ \varphi([x, y]) \in G'$.
$\varphi([x, y]) = [\varphi(x), \varphi(y)] \in G'$. ■

Замечание. Если $H \subseteq G$ — подгруппа, то $H' \subseteq G'$.

Лемма 12. $\mathbf{A}_n' = \begin{cases} e, & n \leqslant 3, \\ \mathbf{V}_4, & n = 4, \\ \mathbf{A}_n, & n \geqslant 5. \end{cases}$

□ При $n \leqslant 3$ $\mathbf{A}_n$ абелева.
При $n = 4$ $\mathbf{V}_4 \triangleleft \mathbf{A}_4$, $\left|\mathbf{A}_4/\mathbf{V}_4\right| = \frac{12}{4} = 3$ — простое число $\Rightarrow \mathbf{A}_4/\mathbf{V}_4 \cong \mathbb{Z}_3 \Rightarrow \mathbf{A}_4/\mathbf{V}_4$ — абелева $\Rightarrow \mathbf{A}_4' \subseteq \mathbf{V}_4$. С другой стороны, $\mathbf{A}_4' \neq \{e\}$, так как $\mathbf{A}_4$ не абелева. Но $\mathbf{A}_4$ состоит из двух классов сопряжённости $\Rightarrow$ в $\mathbf{V}_4$ нет собственных подгрупп, нормальных в $\mathbf{A}_4 \Rightarrow \mathbf{A}_4' = \mathbf{V}_4$.

При $n \geqslant 5$, применяя вышеописанные рассуждения к произвольной четвёрке индексов i, j, k, l, увидим, что любая пара независимых транспозиций лежит в $\mathbf{A}'_n$. По предложению 20, такие пары порождают $\mathbf{A}_n$. Значит, $\mathbf{A}'_n = \mathbf{A}_n$. ■

Лемма 13. $\mathbf{D}'_n = \begin{cases} \left\langle R\left(\frac{2\pi}{n}\right)\right\rangle, & n = 2s+1, \\ \left\langle R\left(\frac{2\pi}{s}\right)\right\rangle, & n = 2s. \end{cases}$

□ Коммутаторы вращений тривиальны.
$R(\varphi) S_v R(-\varphi) S_v = S_{R(\varphi)v} S_v = R(2\varphi)$.
$S_1 S_2 S_1 S_2 = R(2\varphi) R(2\varphi) = R(4\varphi)$, где φ — угол между осями симметрий.
Таким образом, $\mathbf{D}'_n = \left\{R\left(2 \cdot \frac{2\pi k}{n}\right)\right\}_{k=0}^{n-1} = \begin{cases} \left\langle R\left(\frac{2\pi}{n}\right)\right\rangle, & n = 2s+1, \\ \left\langle R\left(\frac{2\pi}{s}\right)\right\rangle, & n = 2s. \end{cases}$ ■

Задача 34. *Найти коммутант* Q_8.

Лемма 14. *Пусть* F *— поле,* $|F| \geqslant 4$. *Тогда* $\mathbf{SL}_n(F)' = \mathbf{SL}_n(F)$.

□ Пусть $n = 2$. Тогда

$$\left[\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c\left(\lambda^2 - 1\right) \\ 0 & 1 \end{pmatrix}.$$

Выберем $\lambda \notin \{-1, 0, 1\}$. Тогда $\lambda^2 - 1 \neq 0$, и за счёт выбора c получим, что все матрицы вида $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ являются коммутаторами. Аналогичное рассуждение проводится для нижнетреугольных матриц. Получается, что все элементарные матрицы первого типа лежат в коммутанте.

При $n > 2$ применим это соображение в двумерном пространстве $\langle e_i, e_j \rangle$ и получим, что матрицы вида $\begin{pmatrix} 1 & & & \\ 0 & 1 & & * \\ & & \ddots & \\ 0 & 0 & & 1 \end{pmatrix}$, где звёздочка стоит на месте (i, j), будут коммутаторами. Получается, что все элементарные матрицы первого типа лежат в коммутанте.

По пункту 2 предложения 21, такие элементарные матрицы порождают $\mathbf{SL}_n(F) \Rightarrow \mathbf{SL}_n(F) \subseteq \mathbf{SL}_n(F)' \Rightarrow$ $\Rightarrow \mathbf{SL}_n(F) = \mathbf{SL}_n(F)'$. ■

Лемма 15. *Пусть* F *— поле,* $|F| \geqslant 4$. *Тогда* $\mathbf{GL}_n(F)' = \mathbf{SL}_n(F)$.

□ $\det[A, B] = \det\left(ABA^{-1}B^{-1}\right) = 1 \Rightarrow \mathbf{GL}_n(F)' \subseteq \mathbf{SL}_n(F)$. С другой стороны, $\mathbf{SL}_n(F)' = \mathbf{SL}_n(F) \subseteq$ $\subseteq \mathbf{GL}_n(F)'$. Значит, $\mathbf{GL}_n(F)' = \mathbf{SL}_n(F)$. ■

§ 13. Разрешимые группы

Определение. *Кратный коммутант* $G^{(k)}$ группы G определим индуктивно:

1. $G^{(1)} = G'$;
2. $G^{(k)} = \left(G^{(k-1)}\right)'$.

Удобно считать, что $G^{(0)} = G$.

Предложение 24. *Пусть* G *— произвольная группа,* H_1 *— характеристическая подгруппа в* G, H_2 *— характеристическая подгруппа в* H_1. *Тогда* H_2 *— характеристическая подгруппа в* G.

□ $\forall \varphi \in \mathrm{Aut}(G)\ \varphi(H_1) = H_1 \Rightarrow \exists \psi = \varphi\big|_{H_1} : H_1 \to H_1,\ \psi(H_2) = H_2,\ \psi \in \mathrm{Aut}(H_1) \Rightarrow \varphi(H_2) = \psi(H_2) = H_2$.
■

Следствие. $G^{(k)} \lhd G$. Более того, $G^{(k)}$ — характеристическая подгруппа в G.

Задача 35. *Привести пример* $H_2 \subseteq H_1 \subseteq G$: $H_1 \lhd G$, $H_2 \lhd H_1$, $H_2 \not\lhd G$.

Определение. Группа G *разрешима*, если $\exists k \in \mathbb{N}$: $G^{(k)} = \{e\}$. В этом случае $G \supset G' \supset G^{(2)} \supset \ldots \supset G^{(k)} = \{e\}$, $G^{(i)}/G^{(i+1)}$ абелева. Наименьшее такое $k \in \mathbb{N}$ называется *ступенью разрешимости* G, то есть говорят, что группа G разрешима ступени k.

Конец лекции № 8 от 2 октября 2013 г. *(к началу)*

Начало лекции № 9 от 7 октября 2013 г.

Замечание. Разрешимые группы ступени 1 — абелевы группы.

Пример 28.

0. $G = \mathbf{S}_3 \Rightarrow G' = \mathbf{A}_3 \Rightarrow G^{(2)} = \mathbf{A}_3' = \{e\} \Rightarrow G$ разрешима ступени 2.
1. $G = \mathbf{S}_4 \Rightarrow G' = \mathbf{A}_4 \Rightarrow G^{(2)} = \mathbf{A}_4' = \mathbf{V}_4 \Rightarrow G^{(3)} = \mathbf{V}_4' = \{e\} \Rightarrow G$ разрешима ступени 3.
2. $G = \mathbf{S}_n$, $n \geqslant 5 \Rightarrow G' = \mathbf{A}_n \Rightarrow G^{(k)} = \mathbf{A}_k \,\forall\, k \geqslant 2 \Rightarrow G$ неразрешима. Аналогично для $G = \mathbf{A}_n$, $n \geqslant 5$.
3. $G = \mathbf{D}_n \Rightarrow G' \subseteq R$ — группа поворотов, которая есть абелева циклическая $\Rightarrow G^{(2)} = \{e\} \Rightarrow G$ разрешима ступени 2.
4. **Задача 36.** *Доказать, что Q_8 разрешима.*
5. $G = \mathbf{GL}_n(F)$ или $G = \mathbf{SL}_n(F)$, $|F| \geqslant 4 \Rightarrow G' = \mathbf{SL}_n(F) \Rightarrow G^{(k)} = \mathbf{SL}_n(F) \,\forall\, k \geqslant 2 \Rightarrow G$ неразрешима.

Имеем $G \supseteq G' \supseteq G^{(2)} \supseteq \ldots$ Если G разрешима, то цепочка оборвётся: $G \supseteq G' \supseteq G^{(2)} \supseteq \ldots \supseteq G^{(k)} = \{e\}$. Такая цепочка называется *производным рядом*. Также знаем, что ${}^{G^{(i)}}\!/_{G^{(i+1)}}$ абелева $\forall\, i$.

Предложение 25. *Пусть в группе G $\exists$ ряд подгрупп $G \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_s = \{e\}$, $G_{i+1} \lhd G_i$, ${}^{G_i}\!/_{G_{i+1}}$ абелева $\forall\, i$. Тогда G разрешима.*

□ Достаточно доказать, что $G^{(i)} \subseteq G_i \,\forall\, i$. Воспользуемся индукцией по n.

1. $i = 0 \Rightarrow G^{(0)} = G = G_0$.
2. Пусть $G^{(i)} \subseteq G_i$. Проверим, что $G^{(i+1)} \subseteq G_{i+1}$. Так как, по предположению индукции, ${}^{G_i}\!/_{G_{i+1}}$ абелева, то, по пункту 3 предложения 22, $G_i' \subseteq G_{i+1}$. Но $G^{(i+1)} = \left(G^{(i)}\right)' \subseteq G_i' \subseteq G_{i+1}$.

■

Лемма 16.

1. *Подгруппа разрешимой группы разрешима.*
2. *Факторгруппа разрешимой группы разрешима.*

□

1. Пусть $H \subseteq G$ — подгруппа. Тогда $H' \subseteq G', \ldots, H^{(i)} \subseteq G^{(i)} \,\forall\, i$. Поскольку $\exists\, k \in \mathbb{N}$: $G^{(k)} = \{e\}$, то $H^{(k)} = \{e\}$.
2. Пусть $N \lhd G$, $F = {}^{G}\!/_{N}$. По лемме 11, для сюръективного гомоморфизма $\pi\colon G \twoheadrightarrow F$, $g \mapsto gN$, имеем $F' = \pi(G'), \ldots, F^{(i)} = \pi\left(G^{(i)}\right) \,\forall\, i$. Поскольку $\exists\, k \in \mathbb{N}$: $G^{(k)} = \{e\}$, то $F^{(k)} = \pi\left(G^{(k)}\right) = \pi(\{e\}) = \{eN\} \Rightarrow F$ разрешима.

■

Предложение 26. *Пусть G — группа, $N \lhd G$, N разрешима, $F = {}^{G}\!/_{N}$ разрешима. Тогда G разрешима.*

□ По предположению, $\exists\, k \in \mathbb{N}$: $\left({}^{G}\!/_{N}\right)^{(k)} = \{eN\}$.

$[gN, hN] = (gN)(hN)(gN)^{-1}(hN)^{-1} = ghg^{-1}h^{-1}N$.

Рассмотрим проекцию $\pi\colon G \to {}^{G}\!/_{N}$, $g \mapsto gN$. Тогда $\pi(G') = \left({}^{G}\!/_{N}\right)', \ldots, \pi\left(G^{(k)}\right) = \left({}^{G}\!/_{N}\right)^{(k)} = \{eN\} \Rightarrow$
$\Rightarrow G^{(k)} \subseteq N$.

С другой стороны, так как N разрешима, то $\exists\, s \in \mathbb{N}$: $N^{(s)} = \{e\} \Rightarrow \left(G^{(k)}\right)^{(s)} = G^{(k+s)} \subseteq N^{(s)} = \{e\} \Rightarrow$
$\Rightarrow \left(G^{(k)}\right)^{(s)} = \{e\} \Rightarrow G$ разрешима. ■

Задача 37. *Может ли ступень разрешимости G быть меньше суммы ступеней разрешимости N и F?*

Замечание. Предложение 26 даёт ещё одно доказательство предложения 25.

Предложение 27. *Пусть F — поле, $\mathbf{B}_n(F)$ — группа невырожденных верхнетреугольных матриц над F. Тогда $\mathbf{B}_n(F)$ разрешима.*

□ Доказательство проведём индукцией по n.

1. $n = 1 \Rightarrow \mathbf{B}_1(F) \cong F^\times$. Так как $F^\times$ абелева, то $\mathbf{B}_1(F)$ разрешима.
2. Пусть $n > 1$. Построим гомоморфизм $\varphi\colon \mathbf{B}_n(F) \to \mathbf{B}_{n-1}(F)$, где у матрицы A вычёркивается последний столбец и последняя строка. Очевидно, что он сюръективен. Тогда, по теореме 5 о гомоморфизме, ${}^{\mathbf{B}_n(F)}\!/_{\operatorname{Ker}\varphi} \cong \mathbf{B}_{n-1}(F)$. По предположению индукции, ${}^{\mathbf{B}_n(F)}\!/_{\operatorname{Ker}\varphi}$ разрешима $\Rightarrow$ по предложению 26, достаточно доказать, что $\operatorname{Ker}\varphi$ разрешима.

$\operatorname{Ker}\varphi = \left\{ \begin{pmatrix} 1 & \cdots & 0 & c_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & c_{n-1} \\ 0 & \cdots & 0 & c_n \end{pmatrix} \right\}$. Рассмотрим гомоморфизм $\psi\colon \operatorname{Ker}\varphi \to F^\times$, $C \mapsto \det C$. Тогда ${}^{\operatorname{Ker}\varphi}\!/_{\operatorname{Ker}\psi} \cong$ $\cong \operatorname{Im}\psi$ абелева, $\operatorname{Ker}\psi = \left\{ \begin{pmatrix} 1 & \cdots & 0 & c_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & c_{n-1} \\ 0 & \cdots & 0 & 1 \end{pmatrix} \right\}$ абелева $\Rightarrow$ по предложению 26, $\operatorname{Ker}\varphi$ разрешима $\Rightarrow \mathbf{B}_n(F)$ разрешима.

■

§ 14. Простые группы

Определение. Группа G *проста*, если в ней нет нетривиальных нормальных подгрупп[4)].

Теорема 11. *Пусть G — конечная группа. Тогда $\exists$ ряд подгрупп $G \supset H_1 \supset H_2 \supset \ldots \supset H_k = \{e\}$, такой что $H_{i+1} \lhd H_i$, ${}^{H_i}\!/_{H_{i+1}}$ проста $\forall i$. Такой ряд называется* композиционным.

□ Доказательство снова ведём индукцией по n.

1. $|G| = 1 \Rightarrow G = \{e\}$.
2. Пусть $|G| > 1$, $H \subsetneq G$ — нормальная подгруппа наибольшего порядка.

Лемма 17. ${}^{G}\!/_{H}$ *проста.*

□ Пусть, от противного, $N \lhd {}^{G}\!/_{H}$ нетривиальна, $\pi\colon G \to {}^{G}\!/_{H}$. Тогда $\pi^{-1}(N) \lhd G$, $H \subsetneq \pi^{-1}(N) \neq G$ (так как N нетривиальна) $\Rightarrow \pi^{-1}(N)$ — нормальная подгруппа порядка $> |H|$. Это противоречит изначальному предположению, что H имеет наибольший порядок из нормальных подгрупп G. ■

Положим теперь $H_1 = H$. Тогда $|H_1| < |G|$ и, по предположению индукции, $\exists$ ряд $H_1 \supset H_2 \supset \ldots \supset H_s = \{e\}$: $H_{i+1} \lhd H_i$, ${}^{H_i}\!/_{H_{i+1}}$ проста $\forall i$. Итак, получился ряд $G \supset H_1 \supset H_2 \supset \ldots \supset H_s = \{e\}$: $H_{i+1} \lhd H_i$, ${}^{H_i}\!/_{H_{i+1}}$ проста $\forall i$.

■

Определение. Пусть $N \lhd G$, $F = {}^{G}\!/_{N}$. Тогда говорят, что G — *расширение* группы N с помощью подгруппы F.

Здесь имеем цепочку гомоморфизмов: $N \overset{i}{\hookrightarrow} G \overset{\pi}{\longrightarrow} {}^{G}\!/_{N} = F$.

Следствие. Любая конечная группа G получается цепочкой расширений при помощи простых групп.

Ставим задачей классификацию конечных групп, которая распадётся на два этапа:

1. классификация конечных простых групп;
2. классификация расширений.

Замечание. Композиционный ряд из теоремы 11 для данной группы G не единственнен, но, по теореме Жордана — Гёльдера, доказательство которой приведено в этом курсе не будет, длина всех таких рядов одинакова, и набор простых факторгрупп $\left\{ {}^{G}\!/_{H_1}, {}^{H_1}\!/_{H_2}, \ldots, {}^{H_{k-1}}\!/_{H_k} \right\}$ определён однозначно с точностью до порядка.

Пример 29. Не всегда тем, что G — расширение N с помощью F, G определяется однозначно. Например, пусть $N \cong \mathbb{Z}_3$, $F \cong \mathbb{Z}_2$. Тогда:

1. $N = \mathbb{Z}_3$, $F = \mathbb{Z}_2 \Rightarrow G = \mathbb{Z}_3 \oplus \mathbb{Z}_2$ — абелева;
2. $N = \mathbf{A}_3 \cong \mathbb{Z}_3$, $F = {}^{\mathbf{S}_3}\!/_{\mathbf{A}_3} \cong \mathbb{Z}_2 \Rightarrow G = S_3$ — неабелева.

Конец лекции № 9 от 7 октября 2013 г. *(к началу)*

Начало лекции № 10 от 14 октября 2013 г.

Лемма 18. *Абелева группа A проста $\Leftrightarrow A \cong \mathbb{Z}_p$, где p — простое.*

[4)] Тривиальные нормальные подгруппы — $\{e\}$ и G. Конечно, в этом определении можно уловить связь с определением простого числа.

□ В A любая подгруппа нормальна. Простота A в этом случае означает отсутствие нетривиальных подгрупп (не только нормальных, а вообще). Но $\forall\, 0 \neq a \in A$ рассмотрим циклическую подгруппу $\langle a \rangle$. Из вышеизложенного, $\langle a \rangle = A \Rightarrow A$ — циклическая. Предложения 2 и 3 описывали все подгруппы циклических групп. Нетривиальных подгрупп нет, что равносильно тому, что $A \cong \mathbb{Z}_p$. ■

Замечание. Если G — простая неабелева, то $Z(G) = \{e\}$, $G' = G$.

Задача 38. *Привести пример конечной группы G, у которой $Z((G)) = \{e\}$, $G' = G$, но G не проста.*

Теорема 12. *Группа $\mathbf{A}_n$ проста $\forall\, n \geqslant 5$.*

□ (Доказательство приводится по Винбергу.)

Если $N \lhd \mathbf{A}_n$, то N есть объединение классов сопряжённости в $\mathbf{A}_n$.

Лемма 19. *Если $\sigma \in \mathbf{A}_n$ и в разложение σ на независимые циклы входит либо цикл чётной длины, либо два цикла одинаковой нечётной длины, то $C_{\mathbf{A}_n}(\sigma) = C_{\mathbf{S}_n}(\sigma) = \{\tau \in \mathbf{S}_n \mid \tau$ и σ имеют одинаковую циклическую структуру$\}$.*

□ Ясно, что $C_{\mathbf{A}_n}(\sigma) \subseteq C_{\mathbf{S}_n}(\sigma)$. Второе равенство доказывалось в предложении 7. Осталось доказать обратное включение, то есть что если τ сопряжена σ в $\mathbf{S}_n$, то они сопряжены в $\mathbf{A}_n$.

Пусть $\tau = j\sigma j^{-1}$, $j \in \mathbf{S}_n$. Если j чётная, то всё доказано. Пусть j нечётная. Рассмотрим $\beta \in \mathbf{S}_n$: в первом случае β положим равной указанному циклу чётной длины, во втором если $(i_1 \dots i_q)(j_1 \dots j_q)$ — два независимых цикла нечётной длины q в σ, то $\beta \stackrel{\text{def}}{=} (i_1 j_1) \dots (i_q j_q)$. Тогда β нечётна, $\beta\sigma = \sigma\beta$. Значит, $j\beta \in \mathbf{A}_n$ и $(j\beta)\,\sigma\,(j\beta)^{-1} = j\beta\sigma\beta^{-1}j^{-1} = j\sigma\beta\beta^{-1}j^{-1} = j\sigma j^{-1} = \tau \Rightarrow \sigma$ и τ сопряжены в $\mathbf{A}_n$. ■

Пусть $N \lhd \mathbf{A}_n$, $e \neq \sigma \in N$, $\operatorname{ord}(\sigma) = m = pk$, p — простое. Тогда $\operatorname{ord}(\sigma^k) = p$. Заменив σ на σ^k, можно считать, что $\operatorname{ord}(\sigma) = p \Rightarrow \sigma$ есть произведение независимых циклов длины p.

1. $p \geqslant 5 \Rightarrow \sigma = (i_1 \dots i_p)\,\sigma_1$, где $\sigma_1 = e$ или раскладывается в произведение других независимых циклов длины p. Тогда $\sigma' = (i_1 i_2 i_3)\,\sigma\,(i_1 i_2 i_3)^{-1} = (i_2 i_3 i_1 i_4 \dots i_p)\,\sigma_1 \in N \Rightarrow \sigma'\sigma^{-1} = (i_1 i_2 i_4) \in N$. Пользуясь леммой 19 при $q = 1$, получаем, что все тройные циклы лежат в $N \Rightarrow N = \mathbf{A}_n$, по предложению 20.
2. $p = 3$. Если $\sigma = (i_1 i_2 i_3)$, то опять в N лежат все тройные циклы, и $N = \mathbf{A}_n$. Пусть $\sigma = (i_1 i_2 i_3)(j_1 j_2 j_3)\,\sigma_1$. Тогда $\sigma' = (i_1 j_1)(i_2 j_2)\,\sigma\,(i_2 j_2)(i_1 j_1) = (i_1 i_2 j_3)(j_1 j_2 i_3)\,\sigma_1 \in N \Rightarrow \sigma'\sigma^{-1} = (i_1 j_1)(i_3 j_3) \in N \Rightarrow$ по лемме 19, все пары независимых транспозиций лежат в $N \Rightarrow$ по предложению 20, $N = \mathbf{A}_n$.
3. $p = 2 \Rightarrow \sigma = (i_1 i_2)(i_3 i_4)\,\sigma_1$. Пусть $\sigma' = (i_1 i_2 i_3)\,\sigma\,(i_1 i_2 i_3)^{-1} = (i_2 i_3)(i_1 i_4)\,\sigma_1 \in N \Rightarrow \sigma'\sigma^{-1} = (i_1 i_3)(i_2 i_4) \in$ $\in N \Rightarrow$ все пары независимых транспозиций лежат в $N \Rightarrow N = \mathbf{A}_n$.

■

Материал, изложенный начиная отсюда и до конца параграфа, не требуется сдавать на экзамене.

Группа $\mathbf{SL}_n(F)$, вообще говоря, не проста: $Z(\mathbf{SL}_n(F)) \supseteq \{\lambda E \mid \lambda^n = 1\}$. Оказывается, группа $\mathbf{PSL}_n(F) \stackrel{\text{def}}{=} {}^{\mathbf{SL}_n(F)}\!/_{Z(\mathbf{SL}_n(F))}$ — *специальная проективная группа* — проста, кроме случаев $n = 2$, $F = \mathbb{Z}_2$ и $F = \mathbb{Z}_3$. Таким образом, для конечных полей мы получаем много конечных простых групп.

Попытки завершить классификацию простых групп предпринимались в 1981, 1983 (Дэниелом Горенштейном) и 2004 (Майклом Ашбахером) годах. Последняя считается успешной, но только предположительно: в общей сложности работа потребовала 10 тысяч страниц текста в сотнях научных журналов и труда около сотни авторов на протяжении всей второй половины XX века. Итак, классификация конечных простых групп выглядит следующим образом:

- $\mathbb{Z}_p$, p — простое;
- $\mathbf{A}_n$, $n \geqslant 5$;
- некоторые группы матриц над конечными полями (*группы типа Ли*);
- 26 *спорадических простых групп*. Первые пять были открыты Эмилем Матьё в 1860 году и имеют порядки от 7920 до 244823040, остальные 21 — в 1965–1975 годах. Самые большие порядки из них имеют *Бэйби-Монстр* ($2^{41} \cdot 3^{13} \cdot \ldots \cdot 47$) и *Монстр* ($2^{46} \cdot 3^{20} \cdot 5^9 \cdot \ldots \cdot 71$).

§ 15. Действия групп

В этом параграфе в качестве групп рассматриваются группы симметрий или группы преобразований (абстрактная теория группы появилась только в первой половине XX века).

Определение. Пусть G — произвольная группа, X — произвольное множество. *Действием* группы G на множестве X называется гомоморфизм $\alpha\colon G \to S(X)$, где $S(X)$ — группа биекций на X.

Например, если X конечно, $|X| = n$, то $S(X) \cong \mathbf{S}_n$.

Почему мы называем это действием? Элемент $g \in G$ действует на $x \in X$: $x \mapsto \alpha(g)(x)$.

Другая, эквивалентная точка зрения: действие — это отображение $G \times X \to X$, $(g, x) \mapsto g \cdot x = gx$, удовлетворяющее условиям:

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

Задача 39. *Проверить, что второй пункт не влечёт за собой первый.*

Задача 40. *Проверить эквивалентность таких определений действия.*

Решение. Приведём наброски решения. Если $\alpha\colon G \to S\,(X)$, то положим $(g, x) \mapsto \alpha\,(g)\,(x)$.

Обратно, если задано отображение $G \times X \to X$, то для любого фиксированного $g \in G$ отображение $\alpha_g\colon X \to X$, $x \mapsto gx$, обратимо (рассмотреть $\alpha_{g^{-1}}$) $\Rightarrow$ биекция $\Rightarrow$ гомоморфизм $\alpha\colon G \to S\,(X)$, $g \mapsto \alpha_g$. ■

Пример 30. Группа $\mathbf{S}_n$ действует на $\{1, \ldots, n\}$, $\sigma i = \sigma\,(i)$. Здесь $\alpha = \mathrm{id}$.

Определение. *Орбитой* точки $x \in X$ называется множество $Gx \stackrel{\text{def}}{=} \{gx \mid g \in G\} \subseteq X$.

Задача 41. *Доказать, что для данного действия $G \times X \to X$ отношение на X «лежать в одной орбите» является отношением эквивалентности, то есть X распадается на непересекающиеся орбиты.*

Определение. *Стабилизатором* (*стационарной подгруппой*, *подгруппой изотропии*) точки $x \in X$ называется множество $\mathrm{St}\,(x) \stackrel{\text{def}}{=} \{g \in G \mid gx = x\}$.

Ясно, что $\mathrm{St}\,(x)$ — подгруппа в G.

Определение. Действие *транзитивно*, если $\forall\, x, y \in X\ \exists\, g \in G\colon y = gx$ ($\Leftrightarrow X$ — это одна орбита).

Определение. Действие *свободно*, если $gx = x$ для некоторого $x \in X$ влечёт $\mathrm{St}\,(x) = \{e\}$ ($\Leftrightarrow g = e$).

Определение. Действие *эффективно*, если $gx = x \,\forall\, x \in X$ влечёт $g = e$ ($\alpha\colon G \to S\,(X)$ инъективно).

Определение. *Ядро неэффективного действия* $\mathrm{Ker}\,\alpha = \{g \in G \mid gx = x \,\forall\, x \in X\} \lhd G$.

Обозначение. G действует на $X \Leftrightarrow G : X$ или $G \curvearrowright X$.

Пример 31.

1. $G = \mathbf{SO}_n\,(\mathbb{R}) \curvearrowright \mathbb{R}^n = X$, $(A, v) \mapsto Av$. Орбиты этого движения в случае $n = 2$ — концентрические окружности с центром в начале координат (а также сама точка начала координат, считающаяся окружностью с нулевым радиусом). В общем случае это сферы с центром в начале координат, а также сама точка начала координат.

   Стабилизатор ненулевого вектора $\mathrm{St}\,(v) \cong \mathbf{SO}_{n-1}\,(\mathbb{R})$ — все специальные ортогональные преобразования в ортогональной плоскости к v. Если же $v = 0$, то $\mathrm{St}\,(v) = \mathbf{SO}_n\,(\mathbb{R})$.

   Действие не транзитивно, не свободно (хотя при $n = 2$ очень к этому близко), эффективно.

Конец лекции № 10 от 14 октября 2013 г. (к началу)

Начало лекции № 11 от 16 октября 2013 г.

2. $G = \mathbf{S}_n \curvearrowright \{1, \ldots, n\} = X$, $i \mapsto \sigma\,(i)$.

   Действие транзитивно.

   $\mathrm{St}\,(i) \cong \mathbf{S}_{n-1} \Rightarrow$ действие не свободно при $n \geqslant 3$.

   Действие эффективно.

3. $G = \mathbf{GL}_n\,(F)$ или $\mathbf{SL}_n\,(F)$ $(n \geqslant 2) \curvearrowright F^n = X$, $(A, v) \mapsto Av$.

   Орбиты: $F^n \setminus \{0\}$ и $\{0\}$.

   Задача 42. *Доказать, что:*

   а. $G = \mathbf{B}_n\,(F) = \left\{ \begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & * \end{pmatrix} \right\} \curvearrowright F^n = X$ *имеет* $n + 1$ *орбиту;*

   б. $G = \mathbf{D}_n\,(F) = \left\{ \begin{pmatrix} * & 0 & \cdots & 0 \\ 0 & * & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & * \end{pmatrix} \right\} \curvearrowright F^n = X$ *имеет* 2^n *орбит.*

   В обоих случаях описать орбиты.

4. $\sigma \in \mathbf{S}_n$, $G = \langle\sigma\rangle \curvearrowright \{1, \ldots, n\} = X$.

   Орбиты соответствуют независимым циклам в разложении σ.

   Действие транзитивно $\Leftrightarrow \sigma$ — цикл длины n.

   Задача 43. *Когда это действие свободно?*

5. $G = \mathbf{GL}_n(\mathbb{C}) \curvearrowright \mathrm{Mat}_n(\mathbb{C}) = X$, $(g, M) \mapsto gMg^{-1}$.

   Орбиты — матрицы одного оператора в разных базисах: $GM = \{M' \mid J(M') = J(M)\}$, где $J(M)$ — жорданова нормальная форма M.

   $\mathrm{St}(M) = Z_{\mathbf{GL}_n(\mathbb{C})}(M)$ [5] $= \{g \mid gM = Mg\}$.

6. $G = \mathbf{GL}_n(F) \curvearrowright \mathrm{Mat}_n(F) = X$, $(g, M) \mapsto gMg^T$.

   Орбиты GM — матрицы одной билинейной формы.

   Если $F = \mathbb{C}$, а $\mathrm{Mat}_n(\mathbb{C})$ заменить на $\mathrm{Sym}_n(\mathbb{C})$ — пространство симметрических матриц, то в этой ситуации орбит будет $n + 1$, и орбита будет определяться рангом соответствующей симметрической билинейной формы: вспомним, что матрица симметрической билинейной формы имеет канонический вид

$$\begin{pmatrix} 1 & \cdots & 0 & \\ \vdots & \ddots & \vdots & 0 \\ 0 & \cdots & 1 & \\ & 0 & & 0 \end{pmatrix},$$

   где количество единиц r есть ранг формы, и эту матрицу и можем принять представителем орбиты.

Три важных действия $G \curvearrowright G$:

1. левые сдвиги: $(g, x) \mapsto gx$;
2. правые сдвиги: $(g, x) \mapsto xg^{-1}$ [6];
3. сопряжения: $(g, x) \mapsto gxg^{-1}$.

Действия 1 и 2 транзитивны: $x \overset{g=yx^{-1}}{\longmapsto} y$ для действия 1, аналогично для действия 2.
Действия 1 и 2 свободны: $\mathrm{St}(x) = \{g \in G \mid gx = x\} = \{e\}$.
Действия 1 и 2 эффективны.
Орбиты действия 3 — классы сопряжённости $C_G(x)$, стабилизатор $\mathrm{St}(x) = Z_G(x)$ — централизатор.
Пусть G нетривиальна. Тогда действие 3 не транзитивно, не свободно, не эффективно: $\operatorname{Ker}\alpha = \bigcap\limits_{x \in X} \mathrm{St}(x) = Z(G)$.

Теорема 13 (Кэли). *Любая конечная группа изоморфна некоторой подгруппе группы $\mathbf{S}_n$, где n — порядок группы.*

□ Рассмотрим $G \curvearrowright G$ левыми сдвигами. Оно определяет гомоморфизм $\alpha\colon G \to S(G) \cong \mathbf{S}_n$. Действие свободно $\Rightarrow$ эффективно $\Rightarrow \alpha$ инъективно $\Rightarrow$ по теореме 5 о гомоморфизме, $G \cong \alpha(G) \subseteq \mathbf{S}_n$. ■

Несложно такой изоморфизм построить и вручную: $G = \{g_1, g_2, \ldots, g_n\}$, $g \to \sigma \Rightarrow G = \{gg_1, gg_2, \ldots, gg_n\} = \{g_{\sigma(1)}, g_{\sigma(2)}, \ldots, g_{\sigma(n)}\} \Rightarrow \sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$.

Определение. Подгруппы H_1, $H_2 \subseteq G$ *сопряжены*, если $\exists\, g \in G$: $gH_1g^{-1} = H_2$.

Лемма 20. *Пусть $G \curvearrowright X$, $x, y \in X$ лежат в одной G-орбите. Тогда $\mathrm{St}(x)$ и $\mathrm{St}(y)$ сопряжены.*

□ По условию, $\exists\, g \in G$: $gx = y$. Тогда $h = \mathrm{St}(y) \Leftrightarrow hy = y \Leftrightarrow h(gx) = gx \Leftrightarrow g^{-1}hgx = x \Leftrightarrow g^{-1}hg \in \mathrm{St}(x) \Leftrightarrow$
$\Leftrightarrow \mathrm{St}(x) = g^{-1}\,\mathrm{St}(y)\,g \Leftrightarrow \mathrm{St}(y) = g\,\mathrm{St}(x)\,g^{-1}$. ■

Замечание. Обратное утверждение к лемме 20 неверно.

Определение. Пусть $G_1 \curvearrowright X_1$, $G_2 \curvearrowright X_2$ — два действия. Они называются *изоморфными*, если существует изоморфизм $\varphi\colon G_1 \to G_2$ и биекция $f\colon X_1 \to X_2$, такие что одно действие переходит в другое, то есть $f(gx) = \varphi(g)\,f(x)$ $\forall\, x \in X_1, g \in G_1$:

$$\begin{array}{ccc} x & \longrightarrow & gx \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\ f(x) & \longrightarrow & \varphi(g)\,f(x) \end{array}$$

[5] Здесь централизатор немного не в том смысле, в котором мы его понимаем, поскольку M не обязательно лежит в $\mathbf{GL}_n(\mathbb{C})$. Но суть остаётся прежней.

[6] Есть аксиома из определения действия, что $g(hx) = (gh)x$. В этом случае $xh^{-1}g^{-1} = x(gh)^{-1}$.

Пусть G — группа, $H \subseteq G$ — подгруппа. Тогда G действует на ${}^{G}\!/_{H}$ (множество левых смежных классов, а не факторгруппа: H не обязательно нормальна):

$$G \times {}^{G}\!/_{H} \to {}^{G}\!/_{H}, \quad (g, g_1H) \mapsto gg_1H.$$

Это действие транзитивно: $g_1H \overset{g=g_2g_1^{-1}}{\longmapsto} g_2H$.

Замечание. Иногда ${}^{G}\!/_{H}$ называют *однородным пространством* группы G.

Предложение 28. *Пусть группа G транзитивно действует на X, $x_0 \in X$, $H = \mathrm{St}(x_0)$. Тогда действие $G \curvearrowright X$ изоморфно $G \curvearrowright {}^{G}\!/_{H}$.*

□ Положим $\varphi = \mathrm{id}$, $f\colon {}^{G}\!/_{H} \to X$, $g_1H \mapsto g_1x_0$.
Проверим, корректно ли определено f, то есть что $g_1x_0 = g_1hx_0$. Это следует из того, что $h \in H$.
Сюръективность f следует из транзитивности действия.
Проверим теперь инъективность: $g_1x_0 = g_2x_0 \Leftrightarrow g_2^{-1}g_1x_0 = x_0 \Leftrightarrow g_2^{-1}g_1 \in H \Leftrightarrow g_2H = g_1H$.
Остаётся понять, что отображение переводит одно действие в другое: $f(gg_1H) = gg_1x_0 = gf(g_1H)$. ■

Предложение 29. *Пусть G — конечная группа, $G \curvearrowright X$. Тогда $\forall x \in X\ |Gx| = \frac{|G|}{|\mathrm{St}(x)|}$.*

□ Группа G действует на орбите Gx транзитивно. Значит, по предложению 28, есть биекция $f\colon Gx \leftarrow {}^{G}\!/_{\mathrm{St}(x)} \Rightarrow |Gx| = \left|{}^{G}\!/_{\mathrm{St}(x)}\right| = \frac{|G|}{|\mathrm{St}(x)|}$, из доказательства теоремы 2. ■

Замечание. Предложение 6 говорило, что $|C_G(a)| = \frac{|G|}{|Z_G(a)|}$. Это как раз частный случай предложения 29.

Теорема 14 (формула Бернсайда). *Пусть G — конечная группа, X — конечное множество, $G \curvearrowright X$. Тогда число орбит этого действия равно $\frac{1}{|G|}\sum\limits_{g\in G}|X^g|$, где $X^g \overset{\text{def}}{=} \{x \in X \mid gx = x\}$.*

□ Рассмотрим $M = \{(g, x) \mid gx = x\}$. Тогда $|M| = \sum\limits_{g\in G}|X^g|$. С другой стороны, если зафиксировать x, то $|M| = \sum\limits_{x\in X}|\mathrm{St}(x)| = \sum\limits_{x\in X}\frac{|G|}{|Gx|} = |G|\sum\limits_{x\in X}\frac{1}{|Gx|}$. Нетрудно заметить, что для каждой орбиты обратная величина к её порядку войдёт в сумму столько раз, сколько элементов в орбите, то есть сумма просто будет равна числу орбит. Приравняв две полученные мощности M, получим требуемое. ■

Пример 32. У действия сопряжениями число классов сопряжённости равно $\frac{1}{|G|}\sum\limits_{g\in G}|Z_G(g)|$.

§ 16. p-группы

Определение. Пусть p — простое число. Конечная группа G называется *p-группой*, если $|G| = p^k$, $k \in \mathbb{Z}_{\geqslant 0}$.

Пример 33.

1. $|\mathbf{D}_4| = 2^3 \Rightarrow \mathbf{D}_4$ — 2-группа.
2. $|Q_8| = 2^3 \Rightarrow Q_8$ — 2-группа.

Теорема 15.

1. *Нетривиальная p-группа имеет нетривиальный центр.*
2. *Любая p-группа разрешима.*

□

1. $|G| = p^k$, $G = \bigsqcup C_G(g) \Rightarrow |G| = \sum|C_G(g)|$. Но $|C_G(g)| = \frac{|G|}{|Z_G(g)|} = p^l$, $l \leqslant k$. При этом $|C_G(g)| = 1 \Leftrightarrow g \in Z(G)$. Поэтому $p^k = |G| = |Z(G)| + \sum\limits_{l_i>0}p^{l_i} \Rightarrow p \,\big|\, |Z(G)| \Rightarrow |Z(G)| \neq 1 \Rightarrow Z(G) \neq \{e\}$.
2. Индукцией по k.
   а. При $k = 0$ $|G| = 1 \Rightarrow G = \{e\} \Rightarrow G$ разрешима.
   б. Пусть $k > 0$. Тогда $Z(G) \neq \{e\}$, $Z(G) \triangleleft G \Rightarrow \left|{}^{G}\!/_{Z(G)}\right| = p^l < p^k$. По предположению индукции, ${}^{G}\!/_{Z(G)}$ разрешима. А сам $Z(G)$ абелев, в частности, разрешим. По предложению 26, G разрешима.

■

Конец лекции № 11 от 16 октября 2013 г. (к началу)

Начало лекции № 12 от 21 октября 2013 г.

Лемма 21. *Пусть G — некоммутативная группа. Тогда ${}^{G}\!/_{Z(G)}$ — не циклическая.*

□ Пусть ${}^{G}\!/_{Z(G)}$ — циклическая. Тогда $\exists a \in G$: ${}^{G}\!/_{Z(G)} = \langle aZ(G)\rangle$. Отсюда $\forall g \in G\ g = a^k z$, где $k \in \mathbb{Z}$, $z \in Z(G)$. Но $\left(a^{k_1} z_1\right)\left(a^{k_2} z_2\right) = a^{k_1+k_2} z_1 z_2 = \left(a^{k_2} z_2\right)\left(a^{k_1} z_1\right)$, поскольку $z_1, z_2 \in Z(G)$, и их можно переставлять как угодно. Получаем противоречие с некоммутативностью группы. ■

Теорема 16. *Группа порядка p^2 абелева.*

□ Пусть $|G| = p^2$. Каким может быть $|Z(G)|$?

1. $|Z(G)| = 1 \Rightarrow$ противоречие с пунктом 1 теоремы 15.
2. $|Z(G)| = p \Rightarrow \left|{}^{G}\!/_{Z(G)}\right| = p \Rightarrow$ по следствию из теоремы 2 Лагранжа, ${}^{G}\!/_{Z(G)}$ — циклическая $\Rightarrow$ противоречие с леммой 21.
3. $|Z(G)| = p^2 \Rightarrow G = Z(G) \Rightarrow G$ абелева.

■

Следствие. Если $|G| = p^2$, то либо $G \cong \mathbb{Z}_{p^2}$, либо $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$.

Пример 34. Приведём пример некоммутативной подгруппы. Пусть $G = \mathbf{U}_n(\mathbb{Z}_p) = \left\{ \begin{pmatrix} 1 & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \right\}, * \in \mathbb{Z}_p$.

Тогда, например, при $n = 3$ $H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}_p \right\}$ — некоммутативная подгруппа порядка p^3.

§ 17. Теоремы Силова

Петер Людвиг Мейделль Сюлов (более известен как *Силов*) — норвежский математик, профессор университета Осло. Свои теоремы опубликовал в 1872 году.

Определение. Пусть G — конечная группа, p — простое число. Тогда $|G| = p^k m$, где $k \in \mathbb{Z}_{\geqslant 0}$, $(m, p) = 1$. *Силовской p-подгруппой в G* называется подгруппа H порядка p^k.

Пример 35. $G = \mathbf{S}_4 \Rightarrow |G| = 24 = 2^3 \cdot 3$

- $p = 2 \Rightarrow |H| = 8 \Rightarrow H \cong \mathbf{D}_4$.
- $p = 3 \Rightarrow |H| = 3$. Например, $H = \langle(123)\rangle$.
- $p \geqslant 5 \Rightarrow |H| = 1 \Rightarrow H = \{e\}$.

Теорема 17 (первая теорема Силова). *В любой конечной группе G для любого простого p силовская p-подгруппа существует.*

□ Доказательство проведём индукцией по порядку группы. Будем считать, что $k \geqslant 1$ (иначе $H = \{e\}$).

Случай 1: $G = A$ — абелева. Тогда $H = \mathrm{Tor}_p(A)$.

Случай 2: в G существует нетривиальный[7)] класс сопряжённости $C_G(g)$, такой что $(|C_G(g)|, p) = 1$. Тогда условие $|G| = |C_G(g)|\,|Z_G(g)|$ влечёт, что $p^k \,\big|\, |Z_G(g)|$. Но поскольку $|Z_G(g)| < |G|$, из нетривиальности класса сопряжённости $C_G(g)$, то, по предположению индукции, $\forall p$ в $Z_G(g)$ существует силовская p-подгруппа H. При этом, так как $p^k \,\big|\, |Z_G(g)|$ и на большие степени p $|Z_G(g)|$ делиться не может, то $|H| = p^k$. Тогда H — силовская p-подгруппа в G.

Случай 3: $\forall C_G(g)$: $|C_G(g)| \neq 1$ $p \,\big|\, |C_G(g)|$. Тогда $|G| = |Z(G)| + ps$, где $s \in \mathbb{N}$. Отсюда $p \,\big|\, |Z(G)|$. Если $|Z(G)| = p^l r$, где $l \geqslant 1$, $(r, p) = 1$, то, по предположению индукции, в $Z(G)$ существует силовская p-подгруппа H_1: $|H_1| = p^l$. Эта подгруппа центральна $\Rightarrow H_1 \lhd G \Rightarrow \left|{}^{G}\!/_{H_1}\right| = p^{k-l} m < p^k m = |G| \Rightarrow$ по предположению индукции, в ${}^{G}\!/_{H_1}$ существует силовская p-подгруппа H_2: $|H_2| = p^{k-l}$.

Пусть $\pi\colon G \to {}^{G}\!/_{H_1}$ — гомоморфизм проекции. Тогда $\pi^{-1}(H_2) = H$ — подгруппа, порядок которой равен числу смежных классов, умноженному на количество элементов в этих смежных классах, то есть $|H| = |H_2|\,|H_1| = p^{k-l} p^l = p^k \Rightarrow H$ — силовская p-подгруппа в G. ■

[7)] То есть $|C_G(g)| \neq 1$.

Замечание. Первая теорема Силова 17 — это частичное обращение теоремы 2 Лагранжа.

Теорема 18 (вторая теорема Силова).

1. *Любая p-подгруппа в G содержится в некоторой силовской p-подгруппе.*
2. *Все силовские p-подгруппы сопряжены.*

□

1. Пусть $H \subseteq G$ — силовская p-подгруппа, $H_1 \subseteq G$ — p-подгруппа. Рассмотрим действие $H_1 \curvearrowright {}^{G}\!/_{H}$ умножениями слева. Число элементов любой нетривиальной H_1-орбиты делится на p, а $\left|{}^{G}\!/_{H}\right| = m$, где $|G| = p^k m$, $(m, p) = 1$. Получается, существует тривиальная H_1-орбита, то есть неподвижная точка данного движения, то есть $\exists\, gH \in {}^{G}\!/_{H}$: $h_1 gH = gH \,\forall\, h_1 \in H_1 \Leftrightarrow g^{-1} h_1 g \in H \,\forall\, h_1 \in H_1 \Leftrightarrow H_1 \subseteq gHg^{-1}$. Но $\left|gHg^{-1}\right| = |H| = p^k \Rightarrow gHg^{-1}$ — тоже силовская.
2. Будем теперь считать, что H_1 — тоже силовская. Вышеприведённые рассуждения показывают, что $\exists\, g \in G$: $H_1 \subseteq gHg^{-1}$. Но $|H_1| = p^k \Rightarrow H_1 = gHg^{-1}$.

■

Следствие. Пусть $H \subseteq G$ — силовская p-подгруппа. Тогда $H \lhd G \Leftrightarrow H$ — единственная силовская p-подгруппа.

Определение. Пусть G — группа, $H \subseteq G$ — подгруппа. *Нормализатором* подгруппы H в G называется множество $N_G(H) \stackrel{\text{def}}{=} \{g \in G \mid gHg^{-1} = H\}$. При этом $H \lhd N_G(H)$.

Теорема 19 (третья теорема Силова). *Если за n_p обозначить число силовских p-подгрупп в G, то $n_p \equiv 1 \pmod p$ и $n_p \,\big|\, m$, где m — индекс силовской p-подгруппы ($|G| = p^k m$, $(m, p) = 1$).*

□ Рассмотрим $G \curvearrowright M$, где M — множество всех силовских p-подгрупп, сопряжениями: $(g, H) \mapsto gHg^{-1}$. По второй теореме Силова 18, это действие транзитивно. Значит, $n_p = \frac{|G|}{|\mathrm{St}(H)|} = \frac{|G|}{|N_G(H)|}$. Но $H \subseteq N_G(H) \Rightarrow$
$\Rightarrow p^k \,\big|\, |N_G(H)| \Rightarrow n_p = \frac{p^k m}{p^k r} \,\big|\, m$.

Зафиксируем некоторую силовскую p-подгруппу $H_0 \subseteq G$ и ограничим $G \curvearrowright M$ на H_0, то есть $H_0 \times M \to M$, $(h_0, H) \mapsto h_0 H h_0^{-1}$. Это действие имеет неподвижную точку H_0. Покажем, что других неподвижных точек нет. Если $h_0 H h_0^{-1} = H \,\forall\, h_0 \in H_0$, то есть H — неподвижная точка, то $H_0 \subseteq N_G(H)$. Но и $H \subseteq N_G(H)$. Применяя вторую теорему Силова 18 к $N_G(H)$, получаем, что H и H_0 сопряжены и в G, и в $N_G(H)$. Но $H \lhd N_G(H)$, а нормальная подгруппа сопряжена только самой себе $\Rightarrow H_0 = H$. Длина любой нетривиальной H_0-орбиты в M делится на $p \Rightarrow n_p = |M| = 1 + ps \equiv 1 \pmod p$. ■

Следствие. Группа G порядка pq, где p, q — простые, $p > q$, разрешима ступени $\leqslant 2$.

□ Пусть $H \subseteq G$ — силовская p-подгруппа. Поскольку $n_p \equiv 1 \pmod p$, $n_p \,\big|\, q$, то $n_p = 1 \Rightarrow H \lhd G$. Но $|H| = p \Rightarrow H \cong \mathbb{Z}_p$; $\left|{}^{G}\!/_{H}\right| = q \Rightarrow {}^{G}\!/_{H} \cong \mathbb{Z}_q \Rightarrow G$ разрешима ступени $\leqslant 2$. ■

Задача 44. *Доказать, что все группы порядка < 60 разрешимы*[8)].

Пример 36. Пусть $|G| = 15 = 5 \cdot 3$. Тогда G — циклическая, в частности, абелева.

□ Пусть H_3 и H_5 — силовские 3- и 5-подгруппы в G. Тогда $n_3 \equiv 1 \pmod 3$, $n_3 \,\big|\, 5 \Rightarrow n_3 = 1$. Аналогично $n_5 = 1$. Значит, $H_3, H_5 \lhd G$. Далее, $H_3 \cap H_5 = \{e\}$ (в этом можно убедиться с помощью теоремы 2 Лагранжа или рассмотрения порядков элементов в H_3 и H_5). По лемме 7, $h_3 h_5 = h_5 h_3 \,\forall\, h_3 \in H_3, h_5 \in H_5 \Rightarrow H_3 \times H_5 \hookrightarrow G$, но $|H_3 \times H_5| = |G| = 15 \Rightarrow G \cong H_3 \times H_5$. $H_3 \cong \mathbb{Z}_3$, $H_5 \cong \mathbb{Z}_5 \Rightarrow G \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$. ■

Конец лекции № 12 от 21 октября 2013 г. *(к началу)*

[8)] Дальше, конечно, хуже: группа $\mathbf{A}_5$ имеет порядок 60, проста и неразрешима.

Начало лекции № 13 от 28 октября 2013 г.

II. Теория представлений

§ 1. Основные понятия

Зафиксируем поле F, векторное пространство V над F и группу G.

Определение. *Представлением* группы G в пространстве V называется гомоморфизм $\rho\colon G \to \mathbf{GL}(V)$. Число $n = \dim V$ называется *размерностью* представления, а V — *пространством* представления. $\{\rho(g) \mid g \in G\} \subseteq \subseteq \mathbf{GL}(V)$ — подгруппа, изоморфная ${}^{G}\!/_{\operatorname{Ker}\rho}$, — называется подгруппой *операторов* представления.

Представление $\rho\colon G \to \mathbf{GL}(V)$ определяет действие $G \times V \to V$, $(g, v) \mapsto \rho(g)\, v$. Таким образом, представления — это линейные действия.

Пример 1. Для любой группы G существует *тривиальное* представление $\rho\colon G \to \mathbf{GL}(V)$, $\rho(g) = E \ \forall\, g \in G$.

Определение. Представление $\rho\colon G \to \mathbf{GL}(V)$ называется *точным*, если $\operatorname{Ker}\rho = \{e\}$ ($\Leftrightarrow$ соответствующее действие эффективно).

Определение. Представления $\rho_1\colon G \to \mathbf{GL}(V)$ и $\rho_2\colon G \to \mathbf{GL}(W)$ группы G над полем F называются *эквивалентными*, или *изоморфными*, если существует изоморфизм $\varphi\colon V \to W$, такой что $\varphi(\rho_1(g)\, v) = \rho_2(g)\, \varphi(v)$:

$$\begin{array}{ccc} v & \xrightarrow{\rho_1(g)} & \rho_1(g)\, v \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi} \\ \varphi(v) & \xrightarrow{\rho_2(g)} & \rho_2(g)\, \varphi(v) \end{array} \qquad \forall\, v \in V,\ g \in G.$$

Отсюда автоматически $\dim V = \dim W$.

Попробуем всё то же самое описать на матричном языке. Зафиксируем базис $\{e_1, \ldots, e_n\} \subseteq V$. Он определяет отождествления $V \leftrightarrow F^n$, $\mathbf{GL}(V) \leftrightarrow \mathbf{GL}_n(F)$. Тогда для представления $\rho\colon \mathbf{GL}_n(F)$ $\rho(g)$ — невырожденная матрица размера $n \times n$ над F $\forall\, g \in G$.

В определении эквивалентности представлений есть изоморфизм $\varphi\colon V \cong F^n \to W \cong F^n$. Он задаётся невырожденной матрицей S размера $n \times n$ над F и условие $\varphi(\rho_1(g)\, v) = \rho_2(g)\, \varphi(v)$ перепишется как $S\rho_1(g)\, v = \rho_2(g)\, Sv \Leftrightarrow \rho_1(g)\, v = S^{-1}\rho_2(g)\, Sv \,\forall\, g \in G, v \in V \Leftrightarrow \rho_1(g) = S^{-1}\rho_2(g)\, S \,\forall\, g \in G \Leftrightarrow \rho_2(g) = S\rho_1(g)\, S^{-1} \,\forall\, g \in G$. Итак, представления ρ_1 и ρ_2 эквивалентны $\Leftrightarrow$ $\forall\, g \in G$ матрицы $\rho_1(g)$ и $\rho_2(g)$ — матрицы одного оператора в базисах, соответственно, $\{e_1, \ldots, e_n\}$ и $\{e'_1, \ldots, e'_n\}$, где $e'_i = Se_i$:

$$\{\rho_1(g) \mid g \in G\} \xleftrightarrow[\text{с помощью } S]{\text{сопряжение}} \{\rho_2(g) \mid g \in G\}.$$

В частности, $\operatorname{tr} S^{-1}AS = \operatorname{tr} A$, $\det S^{-1}AS = \det A \Rightarrow$ числа $\operatorname{tr}\rho(g)$ и $\det\rho(g)$ не меняются, если заменить представления на эквивалентные.

Определение. *Инвариантным подпространством* представления $\rho\colon G \to \mathbf{GL}(V)$ называется подпространство $U \subseteq V$, такое что $\rho(g)\, U \subseteq U \,\forall\, g \in G$.

Пример 2. Одномерное подпространство $U = \langle v \rangle$ инвариантно $\Leftrightarrow$ v — общий собственный вектор для всех операторов представления.

Определение. Если $U \subseteq V$ — инвариантное подпространство, то определено *подпредставление* $\rho\big|_U(g) : G \to \mathbf{GL}(U)$, $g \mapsto \rho(g)\big|_U$.

На матричном языке: если $\{e_1, \ldots, e_n\}$ — такой базис в V, что $\{e_1, \ldots, e_k\}$ — базис в U, то $\forall\, g \in G$ $\rho(g) = \left(\begin{array}{c|c} A & B \\ \hline 0 & C \end{array}\right)$, $\rho\big|_U(g) = A \in \mathbf{GL}_k(F)$.

У любого представления есть *тривиальные* инвариантные подпространства $U = \{0\}$ и $U = V$.

Определение. Представление $\rho\colon G \to \mathbf{GL}(V)$ называется *неприводимым*, если у него нет нетривиальных инвариантных подпространств.

Пример 3. Любое одномерное представление неприводимо.

§ 2. Примеры представлений

1. $G = (\mathbb{Z}, +)$. Представление $\rho\colon G \to \mathbf{GL}_n(F)$ однозначно определено матрицей $A = \rho(1) \in \mathbf{GL}_n(F)$, при этом A можно выбирать любой. Тогда $\rho(k) = A^k$. Два таких представления ρ и ρ' эквивалентны $\Leftrightarrow A = \rho(1)$ и $A' = \rho'(1)$ сопряжены.

2. $G = (\mathbb{Z}_n, +)$. Представление $\rho\colon G \to \mathbf{GL}_n(F)$ однозначно определено матрицей $A = \rho\left(\overline{1}\right) \in \mathbf{GL}_n(F)$, но теперь подходят только такие A, что $A^n = E$.

3. Пусть G — конечная группа, F — поле. Построим векторное пространство V_G с базисом $\{e_g \mid g \in G\}$ над полем F. Определим *регулярное* представление группы G $\rho = r\colon G \to \mathbf{GL}(V_G)$, $\rho(g)(e_h) = e_{gh}\,\forall\, g, h \in G$. Проверка того, что это гомоморфизм, то есть что $\rho(g_1)\,\rho(g_2) = \rho(g_1 g_2)$, очевидна.

   Инвариантная прямая $U = \left\langle \sum\limits_{h\in G} e_h \right\rangle\colon \rho(g) \sum\limits_{h\in G} e_h = \sum\limits_{h\in G} e_{gh} = \sum\limits_{h\in G} e_h$.

   Инвариантная гиперплоскость $W = \left\{ \sum\limits_{n\in G} x_n e_n \mid \sum\limits_{n\in G} x_n = 0 \right\}$.

   Предложение 1. *Регулярное представление точно.*

   □ Если $\rho(g) = E$, то $\rho(g)\,e_h = e_{gh} = e_h\,\forall\, g, h \in G \Rightarrow g = e$. ■

   Следствие. Любая конечная группа G реализуется как подгруппа в $\mathbf{GL}_n(F)$ для любого поля F, $n = |G|$. Образ G в $\mathbf{GL}_n(F)$ запишется $(0,1)$-матрицами (то есть матрицами только из нулей и единиц).

4. $G = \mathbf{S}_n$. Определим *мономиальное* представление $\rho\colon \mathbf{S}_n \to \mathbf{GL}_n(F)$ формулой $\rho(\sigma)(e_i) = e_{\sigma(i)}\,\forall\,\sigma \in \mathbf{S}_n, i \in$ $\in \{1, \ldots, n\}$. Например, при $n = 2$ $g = e \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $g = (12) \mapsto \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$; при $n = 3$ $g = (132) \mapsto \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)$.

   Инвариантная прямая $U = \langle e_1 + \ldots + e_n \rangle$.

   Инвариантная гиперплоскость $W = \left\{ \sum\limits_{i=1}^{n} x_i e_i \mid \sum\limits_{i=1}^{n} x_i = 0 \right\}$.

   Определение. Подпредставление мономиального представления группы $\mathbf{S}_n$ в гиперплоскости W назовём *каноническим* представлением $\mathbf{S}_n$: $\rho\colon \mathbf{S}_n \to \mathbf{GL}_{n-1}(F)$.

   Напомним, что характеристикой поля называется число $\operatorname{char} F = \begin{cases} p, & \exists\, p : \underbrace{1 + \ldots + 1}_{p} = 0, \\ 0, & \text{иначе.} \end{cases}$

   Известно, что если характеристика поля положительна, то это простое число.

   Теорема 1. *Пусть $n \geqslant 3$. Тогда каноническое представление неприводимо $\Leftrightarrow (\operatorname{char} F, n) = 1$ или $\operatorname{char} F = 0$.*

   □

   - $\boxed{\Rightarrow}$
     Пусть $\operatorname{char} F = p \,\big|\, n$. Тогда $\underbrace{1 + \ldots + 1}_{n} = 0 \Rightarrow$ прямая $U = \langle e_1 + \ldots + e_n \rangle \subseteq W$. С другой стороны, $\dim W \geqslant 2 \Rightarrow U$ — нетривиальное инвариантное подпространство $\Rightarrow$ представление приводимо.
   - $\boxed{\Leftarrow}$
     Пусть $p \nmid n$ или $\operatorname{char} F = 0$. Предположим, что $0 \neq w \in W$ лежит в инвариантном подпространстве $W_1 \subseteq W$. Надо доказать, что $W_1 = W$. Пусть $w = \sum\limits_{i=1}^{n} x_i e_i$. Так как $w \in W$, то $\sum\limits_{i=1}^{n} x_i = 0 \Rightarrow \exists\, k \neq$ $\neq l$: $x_k \neq x_l$ (иначе $\sum\limits_{i=1}^{n} x_i = n x_1 = 0$, $n \neq 0 \Rightarrow x_1 = 0 \Rightarrow w = 0$). Тогда вектор $\rho((kl))\,w - w =$ $= (x_l - x_k)\,e_k + (x_k - x_l)\,e_l \in W_1$. Домножим на $(x_l - x_k)^{-1}$ (так как $x_l \neq x_k$) $\Rightarrow e_k - e_l \in W_1 \Rightarrow$ для подстановки σ: $\sigma(k) = 1$, $\sigma(l) = i$ $\rho(\sigma)(e_k - e_l) = e_1 - e_i \in W_1\,\forall\, i \in \{2, \ldots, n\}$.
     Заметим, что если $\sum\limits_{i=1}^{n} y_i = 0$, то $\sum\limits_{i=1}^{n} y_i e_i = \sum\limits_{i=2}^{n} (-y_i)(e_1 - e_i) \Rightarrow W$ порождается векторами $e_1 - e_2$, $e_1 - e_3$, … , $e_1 - e_n \Rightarrow W = W_1 \Rightarrow$ нет нетривиальных инвариантных подпространств.

   ■

Конец лекции № 13 от 28 октября 2013 г. (к началу)

Начало лекции № 14 от 11 ноября 2013 г.

Задача 1. *Задать матрицами каноническое представление* $\mathbf{S}_3$ *в базисе* $\{e_1 - e_2, e_2 - e_3\}$.

5. *Знаковое представление* группы $\mathbf{S}_n$, $n \geqslant 2$: $\rho = \operatorname{sgn}\colon \mathbf{S}_n \to \mathbf{GL}_1(F) \cong F^\times$, $\rho(\sigma) = \begin{cases} 1, & \sigma \text{ чётная}, \\ -1, & \sigma \text{ нечётная}. \end{cases}$

   Представление по построению одномерно и, как следствие, неприводимо; оно тривиально (то есть $\operatorname{Im}\rho = \{1\}$) $\Leftrightarrow \operatorname{char} F = 2$.

6. Пусть $G \subseteq \mathbf{GL}_n(F)$ — подгруппа. Тогда у неё есть *тавтологическое представление* $\rho\colon G \to \mathbf{GL}_n(F)$, $\rho(g) = g\ \forall g \in G$. Представление точно. Также есть *дуальное (двйоственное) представление* $\rho\colon G \to \to \mathbf{GL}_n(F)$, $\rho(g) = \left(g^{-1}\right)^T$[9].

7. Представление $\mathbf{D}_n \to \mathbf{GL}_2(\mathbb{R})$, $g \mapsto$ матрица преобразования $\mathbb{R}^2$, отвечающего симметрии n-угольника. Например, $R(\alpha) \mapsto \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$.

§ 3. Полная приводимость

Определение. Пусть $\rho_1\colon G \to \mathbf{GL}(V_1)$, $\rho_2\colon G \to \mathbf{GL}(V_2)$ — представления над одним и тем же полем F. *Прямой суммой представлений* ρ_1 и ρ_2 называется представление $\rho_1 \oplus \rho_2\colon G \to \mathbf{GL}(V_1 \oplus V_2)$, $(\rho_1 \oplus \rho_2)(g) = \left(\begin{array}{c|c} \rho_1(g) & 0 \\ \hline 0 & \rho_2(g) \end{array}\right)$, или $(\rho_1 \oplus \rho_2)(g)(v_1, v_2) = (\rho_1(g)v_1, \rho_2(g)v_2)$. При этом $\dim(\rho_1 \oplus \rho_2) = \dim\rho_1 + \dim\rho_2$.

Пример 4. Представление ρ изоморфно прямой сумме одномерных представлений $\Leftrightarrow$ в подходящем базисе все операторы представления диагональны, то есть $\rho(g) = \begin{pmatrix} * & 0 & \cdots & 0 \\ 0 & * & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & * \end{pmatrix}\ \forall g \in G$. $V = \langle e_1\rangle \oplus \ldots \oplus \langle e_n\rangle$ — инвариантное подпространство. В этом случае операторы представления попарно коммутируют.

Определение. Представление $\rho\colon G \to \mathbf{GL}(V)$ называется *вполне приводимым*, если оно эквивалентно прямой сумме неприводимых представлений: $\rho \cong \rho_1 \oplus \ldots \oplus \rho_k$.

Пример 5.

1. Неприводимое представление вполне приводимо.
2. ρ тривиально $\Leftrightarrow \rho = \mathrm{id} \oplus \ldots \oplus \mathrm{id}$, где $\mathrm{id}\colon G \to \mathbf{GL}_1(R)$, $g \mapsto 1 \Leftrightarrow \rho$ вполне приводимо.
3. $\rho\colon (\mathbb{Z}, +) \to \mathbf{GL}_2(F)$, $k \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k$.

   Инвариантные подпространства нетривиальны $\Leftrightarrow$ это прямые.

   Поскольку представление циклическое, то инвариантные подпространства достаточно искать относительно $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

   $$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \lambda\begin{pmatrix} x \\ y \end{pmatrix} \Rightarrow \begin{cases} x + y &= \lambda x \\ y &= \lambda y \end{cases}.$$

   Тогда либо $y = 0 \Rightarrow \lambda = 1$, либо $\lambda = 1 \Rightarrow y = 0$. Таким образом, в любом случае $\lambda = 1 \Rightarrow$ инвариантная прямая одна — $\langle e_1\rangle \Rightarrow$ представление приводимо, но не вполне приводимо, так как если бы оно распалось в прямую сумму неприводимых, то эти неприводимые были бы одномерными, но одномерное инвариантное пространство только одно.

4. $\rho\colon (\mathbb{Z}_p, +) \to \mathbf{GL}_2(F)$, $\overline{k} \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k$, p — простое. Пусть $\operatorname{char} F = p$. Тогда $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow$ ρ определено корректно.

   Повторяя рассуждения предыдущего примера, увидим, что инвариантная прямая только одна $\Rightarrow$ ρ не вполне приводимо.

[9] Если взять просто $\rho(g) = g^{-1}$ или $\rho(g) = g^T$, то это не будет гомоморфизмом, так как множители меняются местами; при указанной композиции такая смена мест происходит дважды.

Теорема 2 (Машке). *Пусть G — конечная группа, F — поле,* $\operatorname{char} F = 0$ *или* $\operatorname{char} F = p$, *где* $p \nmid |G|$. *Тогда все представления группы G над полем F вполне приводимы.*

□ Пусть $\rho\colon G \to \mathbf{GL}(V)$ — представление над полем F. Будем вести индукцию по $\dim V$.

1. $\dim V = 1 \Rightarrow \rho$ неприводимо как одномерное представление $\Rightarrow \rho$ вполне приводимо.
2. Пусть $\dim V > 1$. Если ρ неприводимо, то оно вполне приводимо. Пусть ρ приводимо, $U \subsetneq V$ — нетривиальное инвариантное подпространство.

   Шаг 1. Покажем, что существует инвариантное подпространство $W \subseteq V$: $V = U \oplus W$ (W называется в таком случае *инвариантным дополнением*).

   Пусть $W' \subseteq V$ — некоторое дополнительное к U подпространство, то есть $V = U \oplus W'$[10]. Рассмотрим оператор проекции $P'\colon V \to W'$, $P'(u + w') = w' \,\forall\, u \in U, w' \in W'$. Тогда $\operatorname{Ker} P' = U$, $(P')^2 = P'$, $\forall\, v \in V$ $v - P'v \in U$.

   «Усредним» оператор проекции на группе G: $P = \frac{1}{|G|} \sum\limits_{g \in G} \rho(g) P' \rho\left(g^{-1}\right)$[11]. Тогда:

   - P коммутирует со всеми операторами представления: $\rho(h) P = P \rho(h) \,\forall\, h \in G$.

     □
     $$\begin{aligned}\rho(h) P \rho\left(h^{-1}\right) &= \frac{1}{|G|} \sum_{g \in G} \rho(h)\rho(g) P' \rho\left(g^{-1}\right)\rho\left(h^{-1}\right) = \\ &= \frac{1}{|G|} \sum_{g \in G} \rho(hg) P' \rho\left((hg)^{-1}\right) = \\ &= \frac{1}{|G|} \sum_{g \in G} \rho(g) P' \rho\left(g^{-1}\right) = P.\end{aligned}$$
     ■

   - $W = \operatorname{Im} P$ инвариантно.

     □ $\rho(g) w = \rho(g) Pv = P(\rho(g) v) \in \operatorname{Im} P = W \,\forall\, w \in W$. ■

   - $U \subseteq \operatorname{Ker} P$.

     □ $Pu = \frac{1}{|G|} \sum\limits_{g \in G} \rho(g) P' \underbrace{\rho\left(g^{-1}\right) u}_{\in U} = \frac{1}{|G|} \sum\limits_{g \in G} \rho(g) \underbrace{P'u'}_{=0} = 0 \,\forall\, u \in U$. ■

   - $\operatorname{Ker} P \subseteq U$, $P^2 = P$.

     □ $\forall\, v \in V$ $v - Pv = v - \frac{1}{|G|} \sum\limits_{g \in G} \rho(g) P' \rho\left(g^{-1}\right) v = \frac{1}{|G|} \sum\limits_{g \in G} \rho(g) \left(\rho\left(g^{-1}\right) v - P' \rho\left(g^{-1}\right) v\right) \in U$.

     $P \underbrace{(v - Pv)}_{\in U} = 0 = Pv - P^2 v \Rightarrow Pv = P^2 v \,\forall\, v \in V \Rightarrow P^2 = P$.

     $\forall\, v \in \operatorname{Ker} P$ $v - Pv = v - 0 = v \in U \Rightarrow \operatorname{Ker} P \subseteq U$. ■

   - $V = U + W$.

     □ $\forall\, v \in V$ $v = \underbrace{v - Pv}_{\in U} + \underbrace{Pv}_{\in W}$. ■

   - $V = U \oplus W$.

[10] Такое подпространство существует: например, можно взять базис U, дополнить его до базиса V и за W' взять линейную оболочку добавленных базисных векторов.

[11] Использовано предположение, что $\operatorname{char} F \nmid |G|$.

□ $\forall v \in U \cap W\ \exists v_0 \in V$: $v = Pv_0 \Rightarrow 0 = Pv = PPv_0 = P^2v_0 = Pv_0 = v \Rightarrow U \cap W = \{0\} \Rightarrow V = U \oplus W$. ■

Шаг 2. Поскольку $\dim U, \dim W < \dim V$, то, по предположению индукции, $\rho\Big|_U = \rho_1 \oplus \ldots \oplus \rho_k$, $\rho\Big|_W = \rho_{k+1} \oplus \ldots \oplus \rho_n \Rightarrow \rho = \rho_1 \oplus \ldots \oplus \rho_k \oplus \rho_{k+1} \oplus \ldots \oplus \rho_n$.

■

§ 4. Инвариантные формы

Над полями $F = \mathbb{R}, \mathbb{C}$ шаг 1 теоремы 2 Машке можно провести иначе.

Теорема 3. *Пусть $\rho\colon G \to \mathbf{GL}(V)$ — представление конечной группы над полем $\mathbb{R}$ ($\mathbb{C}$). Тогда на пространстве V существует положительно определённая билинейная симметрическая (положительно определённая эрмитова) форма $(\cdot,\cdot)$, для которой $(\rho(h)v_1, \rho(h)v_2) = (v_1, v_2)\ \forall h \in G, v_1, v_2 \in V$.*

□ Пусть $\langle\cdot,\cdot\rangle$ — произвольное скалярное произведение на V. Положим новое скалярное произведение «усреднением» старого: $(v_1, v_2) = \frac{1}{|G|}\sum\limits_{g\in G}\langle\rho(g)v_1, \rho(g)v_2\rangle\ \forall v_1, v_2 \in V$. Тогда:

- $(\cdot,\cdot)$ — симметрическая билинейная (эрмитова) форма.
- $(\cdot,\cdot)$ положительно определено.

  □ $(v,v) = \frac{1}{|G|}\sum\limits_{g\in G}\langle\rho(g)v, \rho(g)v\rangle > 0$. ■

- $(\cdot,\cdot)$ инвариантно.

  □

$$\begin{aligned}(\rho(h)v_1, \rho(g)v_2) &= \frac{1}{|G|}\sum_{g\in G}\langle\rho(g)\rho(h)v_1, \rho(g)\rho(h)v_2\rangle = \\ &= \frac{1}{|G|}\sum_{g\in G}\langle\rho(gh)v_1, \rho(gh)v_2\rangle = \\ &= \frac{1}{|G|}\sum_{g\in G}\langle\rho(g)v_1, \rho(g)v_2\rangle = (v_1, v_2).\end{aligned}$$

  ■

■

Конец лекции № 14 от 11 ноября 2013 г. (к началу)

Начало лекции № 15 от 13 ноября 2013 г.

Теперь можно предъявить другое обоснование шага 1 в доказательстве теоремы 2 Машке. Нужно найти инвариантное дополнение W инвариантного подпространства U в пространстве V. Положим $W = U^\perp \overset{\text{def}}{=} \overset{\text{def}}{=} \{v \in V \mid (v,u) = 0\ \forall u \in U\}$. То, что это дополнение, известно из курса линейной алгебры: $V = U \oplus U^\perp$. Остаётся проверить инвариантность $U^\perp$. Если $v \in U^\perp$, $h \in G$, то $\forall u \in U\ (\rho(h)v, u) = \left(\rho\left(h^{-1}\right)\rho(h)v, \rho\left(h^{-1}\right)u\right) = \left(v, \rho\left(h^{-1}\right)u\right) = 0 \Rightarrow \rho(h)v \in U^\perp$.

Замечание. Пусть G — конечная группа, $\rho\colon G \to \mathbf{GL}(V)$ — представление. Мы доказали, что над $\mathbb{R}$ ($\mathbb{C}$) в подходящем базисе все операторы представления записываются ортогональными (унитарными) матрицами, то есть $AA^T = E$ ($A\overline{A}^T = E$).

Задача 2. *Привести пример представления конечной группы G над $\mathbb{C}$ ($\rho\colon G \to \mathbf{GL}_n(\mathbb{C})$), для которого не существует невырожденной билинейной симметрической формы.*

Задача 3. *Доказать (над $\mathbb{C}$), что если $\mathcal{A}^m = \mathcal{E}$, $m \in \mathbb{N}$, то $\mathcal{A}$ диагонализируем.*

Наша дальнейшая цель — классифицировать неприводимые представления (в основном над $\mathbb{C}$) данной конечной группы.

§ 5. Одномерные представления

Пусть G — произвольная группа, F — произвольное поле, $\rho\colon G \to \mathbf{GL}_1(F) \cong F^\times$ — одномерное представление.

Лемма 1. *Коммутант G лежит в* $\operatorname{Ker}\rho$.

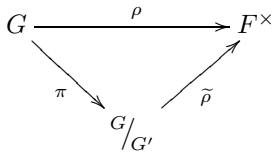
□ Поскольку группа $F^\times$ коммутативна, имеем

$$\rho\left(ghg^{-1}h^{-1}\right) = \rho(g)\,\rho(h)\,\rho\left(g^{-1}\right)\rho\left(h^{-1}\right) = \\ = \rho(g)\,\rho\left(g^{-1}\right)\rho(h)\,\rho\left(h^{-1}\right) = 1.$$

Отсюда $[g,h] \in \operatorname{Ker}\rho\ \forall\, g,h \in G \Rightarrow G' \subseteq \operatorname{Ker}\rho$. ■

Тем самым представление $\rho\colon G \to F^\times$ определяет представление $\widetilde{\rho}\colon {}^{G}\!/_{G'} \to F^\times$, $\widetilde{\rho}(gG') \stackrel{\text{def}}{=} \rho(g)$. Обратно, любое представление $\widetilde{\rho}\colon {}^{G}\!/_{G'} \to F^\times$ определяет представление $\rho\colon G \to F^\times$, $\rho = \widetilde{\rho}\circ\pi$, где π — естественная проекция: $\pi\colon G \to {}^{G}\!/_{G'}$; то есть $\rho(g) = \widetilde{\rho}(gG')$. Тем самым доказана

Теорема 4. *Диаграмма*



определяет биекцию между одномерными представлениями G и одномерными представлениями ${}^{G}\!/_{G'}$.

${}^{G}\!/_{G'}$ — абелева группа, поэтому теперь рассматриваем только их.

Пусть далее G конечна. Тогда ${}^{G}\!/_{G'}$ — конечная абелева группа $\Rightarrow {}^{G}\!/_{G'} \cong \mathbb{Z}_{u_1} \oplus \ldots \oplus \mathbb{Z}_{u_m}$.

Замечание. Одномерные представления эквивалентны $\Leftrightarrow$ они совпадают: $S\rho(g)\,S^{-1} = \rho(g)\ \forall\, g \in G$.

Предложение 2.

1. *Одномерное комплексное представление группы $\mathbb{Z}_u$ имеет вид $\rho_\varepsilon\colon \mathbb{Z}_u \to \mathbb{C}^\times$, $\overline{k} \mapsto \varepsilon^k$, $\varepsilon^u = 1$*[12)].
2. *Конечная абелева группа A имеет ровно $|A|$ одномерных комплексных представлений.*

□

1. $\rho\colon \mathbb{Z}_u \to \mathbb{C}^\times \Rightarrow \rho\left(\overline{1}\right) = \varepsilon$, $\varepsilon^u = 1 \Rightarrow \rho\left(\overline{k}\right) = \varepsilon^k \Rightarrow \rho = \rho_\varepsilon$.

   Обратно, любой ε: $\varepsilon^u = 1$ определяет представление ρ_ε.
2. Мы знаем, что $A \cong \mathbb{Z}_{u_1}\oplus\ldots\oplus\mathbb{Z}_{u_m}$. Пусть $\rho\colon A \to \mathbb{C}^\times$. Тогда $\rho\Big|_{\{0\}\oplus\ldots\oplus\mathbb{Z}_{u_i}\oplus\ldots\oplus\{0\}} : \mathbb{Z}_{u_i} \to \mathbb{C}^\times$ имеет вид ρ_{ε_i}, $\varepsilon_i^{u_i} = 1 \Rightarrow \rho\left(\left(\overline{k_1},\ldots,\overline{k_m}\right)\right) = \rho\left(\left(\overline{k_1},\overline{0},\ldots,\overline{0}\right) + \ldots + \left(\overline{0},\overline{0},\ldots,\overline{k_m}\right)\right) = \rho\left(\left(\overline{k_1},\overline{0},\ldots,\overline{0}\right)\right)\ldots\rho\left(\left(\overline{0},\ldots,\overline{k_m}\right)\right) = \\ = \varepsilon_1^{k_1}\ldots\varepsilon_m^{k_m}$. Таких представлений, как способов выбрать набор из ε, $u_1\ldots u_m = |A|$.

■

Следствие. Пусть G — конечная группа. Тогда число её одномерных представлений равно $\left|{}^{G}\!/_{G'}\right|$.

Пример 6.

1. Опишем одномерные комплексные представления группы диэдра $\mathbf{D}_4$. Поскольку $|\mathbf{D}_4| = 8$, а $\mathbf{D}_4' = \{e, R(\pi)\}$, то $\left|{}^{\mathbf{D}_4}\!/_{\mathbf{D}_4'}\right| = 4 \Rightarrow {}^{\mathbf{D}_4}\!/_{\mathbf{D}_4'} \cong \mathbb{Z}_2\oplus\mathbb{Z}_2$ или ${}^{\mathbf{D}_4}\!/_{\mathbf{D}_4'} \cong \mathbb{Z}_4$. Но $\mathbf{D}_4$ можно породить двумя «соседними» симметриями, которые имеют порядок 2, и $\mathbb{Z}_2\oplus\mathbb{Z}_2$, в отличие от $\mathbb{Z}_4$, тоже порождается элементами порядка 2. Значит, ${}^{\mathbf{D}_4}\!/_{\mathbf{D}_4'} \cong \mathbb{Z}_2\oplus\mathbb{Z}_2$.

   Получаем четыре одномерных представления:

	ρ_1	ρ_2	ρ_3	ρ_4
S_1	1	1	−1	−1
S_2	1	−1	1	−1

2. $G = \mathbf{A}_4 \Rightarrow {}^{G}\!/_{G'} = {}^{\mathbf{A}_4}\!/_{\mathbf{V}_4} \cong \mathbb{Z}_3$ порождается $(123)\,\mathbf{V}_4$. Тут три одномерных представления:

	ρ_1	ρ_2	ρ_3
(123)	1	ε	ε^2

[12)] Видно, что таких представлений u штук, как корней u-й степени из единицы.

Задача 4. *Чему равно число одномерных вещественных представлений:*

1. *группы* $\mathbb{Z}_4$*;*
2. *произвольной конечной группы* A*?*

§ 6. Представления абелевых групп

Основное поле — $\mathbb{C}$.

Теорема 5. *Неприводимое комплексное представление абелевой группы одномерно.*

□ *Шаг 1.* Пусть $\{\mathcal{A}_i \mid i \in I\}$ — набор линейных операторов в комплексном векторном пространстве V, $\dim V < \infty$, и $\mathcal{A}_i\mathcal{A}_j = \mathcal{A}_j\mathcal{A}_i \ \forall i, j \in I$. Тогда у них существует общий собственный вектор, то есть $0 \neq v \in V$: $\mathcal{A}_i v = \lambda_i v$, $\lambda_i \in \mathbb{C}$. Доказывается это индукцией по размерность пространства:

1. Если $\dim V = 1$, то всё ясно.
2. Пусть $\dim V > 1$. Если все $\mathcal{A}_i$ скалярны, то любой вектор будет собственным для всех $\mathcal{A}_i$. Пусть $\mathcal{A}_1$ нескалярен, λ_1 — его собственное значение, $V_{\lambda_1} = \{v \in V \mid \mathcal{A}_1 v = \lambda_1 v\}$. Тогда $\{0\} \neq V_{\lambda_1} \neq V$. Проверим, что V_{λ_1} инвариантно относительно всех $\mathcal{A}_i$. Пусть $v \in V_{\lambda_1}$. Тогда $\mathcal{A}_1\mathcal{A}_i v = \mathcal{A}_i\mathcal{A}_1 v = \mathcal{A}_i\lambda_1 v = \lambda_1(\mathcal{A}_i v) \Rightarrow$ $\Rightarrow \mathcal{A}_i v \in V_{\lambda_1}$. Поскольку $\dim V_{\lambda_1} < \dim V$, то, по предположению индукции, операторы $\mathcal{A}_i$ имеют общий собственный вектор в V_{λ_1}.

Шаг 2. Пусть $\rho\colon A \to \mathbf{GL}(V)$ — неприводимое комплексное представление абелевой группы A. Тогда операторы $\rho(a)$, $a \in A$, коммутируют $\Rightarrow$ они имеют общий собственный вектор $v \in V$. Тогда $U = \langle v \rangle$ — инвариантное подпространство для представления $\rho \Rightarrow V = U$, в силу неприводимости $\rho \Rightarrow \dim V = 1$. ■

Следствие. Любое комплексное представление конечной абелевой группы эквивалентно прямой сумме одномерных.

□ По теореме 2 Машке, представление эквивалентно прямой сумме неприводимых, а по теореме 5, неприводимые одномерны. ■

Задача 5. *Сколько с точностью до эквивалентности двумерных комплексных представлений у группы* $\mathbb{Z}_3 \oplus \mathbb{Z}_3$*?*

Пример 7.

1. Если абелева группа бесконечна, то утверждение следствия неверно. Контрпример: $\rho\colon \mathbb{Z} \to \mathbf{GL}_2(\mathbb{C})$, $k \mapsto$ $\mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k$.
2. Утверждение следствия также неверно над $\mathbb{R}$. Контрпример: $\rho\colon \mathbb{Z}_3 \to \mathbf{GL}_2(\mathbb{R})$, $\overline{k} = \begin{pmatrix} \cos\frac{2\pi k}{3} & \sin\frac{2\pi k}{3} \\ -\sin\frac{2\pi k}{3} & \cos\frac{2\pi k}{3} \end{pmatrix}$.

   Матрица $\begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$ недиагонализируема над $\mathbb{R}$.

Задача 6. *Пусть* $\{\mathcal{A}_i \mid i \in I\}$ *— линейные операторы в комплексном векторном пространстве* V*,* $\mathcal{A}_i\mathcal{A}_j =$ $= \mathcal{A}_j\mathcal{A}_i \ \forall i, j \in I$*. Предположим, что все операторы* $\mathcal{A}_i$ *диагонализируемы. Доказать, что существует базис, в котором все* $\mathcal{A}_i$ *записываются диагональными матрицами.*

Задача 7. *Пусть все неприводимые комплексные представления конечной группы* G *одномерны. Доказать, что* G *абелева.*

Следующая цель — описать неприводимые неодномерные комплексные представления конечных групп, например, $\mathbf{S}_3$ или $\mathbf{S}_4$.

Конец лекции № 15 от 13 ноября 2013 г. *(к началу)*

Начало лекции № 16 от 18 ноября 2013 г.

§ 7. Лемма Шура и усреднение отображений

Пусть $\rho_1\colon G \to \mathbf{GL}(V)$, $\rho_2\colon G \to \mathbf{GL}(W)$ — представления группы G над полем F.

Определение. Линейное отображение $\varphi\colon V \to W$ называется *гомоморфизмом представлений* ρ_1 и ρ_2, если $\varphi(\rho_1(g)\, v) = \rho_2(g)\, \varphi(v) \ \ \forall g \in G$, $v \in V$:

$$\begin{array}{ccc} v & \xrightarrow{\varphi} & \varphi(v) \\ \Big\downarrow{\scriptstyle \rho_1(g)} & & \Big\downarrow{\scriptstyle \rho_2(g)} \\ \rho_1(g)\, v & \xrightarrow{\varphi} & v'. \end{array}$$

Теорема 6 (лемма Шура). *Пусть представления ρ_1 и ρ_2 неприводимы, φ — гомоморфизм ρ_1 и ρ_2. Тогда:*

1. *если $\rho_1 \not\cong \rho_2$, то $\varphi \equiv 0$;*
2. *если $\rho_1 \cong \rho_2$, то либо $\varphi \equiv 0$, либо φ — изоморфизм представлений;*
3. *если $F = \mathbb{C}$, $V = W$, $\rho_1 = \rho_2 = \rho$, то $\varphi = \lambda\mathcal{E}$, где $\lambda \in \mathbb{C}$.*

□ Заметим, что $\operatorname{Ker}\varphi \subseteq V$ и $\operatorname{Im}\varphi \subseteq W$ — инвариантные подпространства. В самом деле:

- если $\varphi(v) = 0$, то $\varphi(\rho_1(g)\,v) = \rho_2(g)\,\varphi(v) = \rho_2(g)\,0 = 0$, то есть $\rho_1(g)\,v \in \operatorname{Ker}\varphi$;
- если $w = \varphi(v)$, то $\rho_2(g)\,w = \rho_2(g)\,\varphi(v) = \varphi(\rho_1(g)\,v)$, то есть $\rho_2(g)\,w \in \operatorname{Im}\varphi$.

Из неприводимости ρ_1 следует, что возможны только два случая.
Случай 1. $\operatorname{Ker}\varphi = V \Rightarrow \varphi \equiv 0$.
Случай 2. $\operatorname{Ker}\varphi = \{0\}$. Поскольку $\dim V = \dim\operatorname{Ker}\varphi + \dim\operatorname{Im}\varphi$, то если $\operatorname{Im}\varphi = \{0\}$, то $\dim V = 0 \Rightarrow V = \{0\} \Rightarrow \varphi \equiv 0$; если же $\operatorname{Im}\varphi \neq 0$, то, из неприводимости ρ_2, $\operatorname{Im}\varphi = W \Rightarrow \varphi\colon V \to W$ — изоморфизм пространств (инъективен в силу тривиальности ядра, сюръективен в силу равенства образа W) $\Rightarrow \varphi$ — изоморфзизм представлений. Таким образом, доказаны пункты 1 и 2.

Докажем пункт 3. Можно считать, что $\varphi \not\equiv 0$. Тогда φ — изоморфизм, по пункту 2, и это линейный оператор $\varphi\colon V \to V$, который имеет ненулевой собственный вектор $v \in V$ с ненулевым собственным значением $\lambda \in \mathbb{C}$ (это следует из невырожденности изоморфизма φ), то есть $\varphi(v) = \lambda v$. Тем самым подпространство собственных векторов $V_\lambda = \{v \in V \mid \varphi(v) = \lambda v\} \neq \{0\}$. Проверим, что оно инвариантно. Действительно, $\varphi(\rho(g)\,v) = \rho(g)\,\varphi(v) = \rho(g)\,\lambda v = \lambda\rho(g)\,v \;\; \forall g \in G$, $v \in V_\lambda$. Поскольку ρ неприводимо, $V_\lambda \neq \{0\}$, то $V_\lambda = V \Rightarrow \varphi = \lambda\mathcal{E}$. ■

Пункт 3 можно переформулировать следующим образом: если линейный оператор $\mathcal{A}$ коммутирует со всеми операторами неприводимого представления и $F = \mathbb{C}$, то $\mathcal{A}$ скалярен.

Задача 8. *Показать на примере, что при $F = \mathbb{R}$ это неверно.*

Следствие. Пусть $\rho_1\colon G \to \mathbf{GL}(V)$ и $\rho_2\colon G \to \mathbf{GL}(W)$ — два неприводимых комплексных представления конечной группы G, $\varphi\colon V \to W$ — произвольное линейное отображение. Тогда для *усреднения* $\widetilde{\varphi} \overset{\text{def}}{=} \frac{1}{|G|}\sum\limits_{g\in G}\rho_2(g)\,\varphi\rho_1\left(g^{-1}\right)$ имеем:

1. если $\rho_1 \not\cong \rho_2$, то $\widetilde{\varphi} \equiv 0$;
2. если $V = W$, $\rho_1 = \rho_2 = \rho$, то $\widetilde{\varphi} = \frac{\operatorname{tr}\varphi}{\dim V}\mathcal{E}$.

□ Проверим, что $\rho_2(h)\,\widetilde{\varphi} = \widetilde{\varphi}\rho_1(h)$. В самом деле, $\rho_2(h)\,\widetilde{\varphi}\rho_1\left(h^{-1}\right) = \frac{1}{|G|}\sum\limits_{g\in G}\rho_2(h)\,\rho_2(g)\,\varphi\rho_1\left(g^{-1}\right)\rho_1\left(h^{-1}\right) = \frac{1}{|G|}\sum\limits_{g\in G}\rho_2(hg)\,\varphi\rho_1\left((hg)^{-1}\right) = \frac{1}{|G|}\sum\limits_{g\in G}\rho_2(g)\,\varphi\rho_1\left(g^{-1}\right) = \widetilde{\varphi}$. Тогда из леммы Шура следует пункт 1.

Для пункта 2 из леммы Шура получаем $\widetilde{\varphi} = \lambda\mathcal{E}$ и $\lambda\dim V = \operatorname{tr}\lambda\mathcal{E} = \operatorname{tr}\widetilde{\varphi} = \frac{1}{|G|}\sum\limits_{g\in G}\operatorname{tr}\left(\rho(g)\,\varphi\rho\left(g^{-1}\right)\right)$. Напомним, что $\operatorname{tr}AB = \operatorname{tr}BA \Rightarrow trCAC^{-1} = \operatorname{tr}A \Rightarrow \frac{1}{|G|}\sum\limits_{g\in G}\operatorname{tr}\left(\rho(g)\,\varphi\rho\left(g^{-1}\right)\right) = \frac{1}{|G|}\sum\limits_{g\in G}\operatorname{tr}\varphi = \operatorname{tr}\varphi \Rightarrow \lambda = \frac{\operatorname{tr}\varphi}{\dim V}$.
■

То же утверждение рассмотрим в матричносм виде. Пусть $\{e_i\}$ — базис V, $\{f_j\}$ — базис W, $\rho_1(g) = (a_{ij}(g))$, $\rho_2(g) = (b_{ij}(g))$, $\varphi = (\varphi_{ij})$. Тогда $\widetilde{\varphi} = (\widetilde{\varphi_{ij}})$,

$$\widetilde{\varphi_{ij}} = \frac{1}{|G|}\sum_{g\in G}\sum_{i',j'} b_{ii'}(g)\,\varphi_{i'j'}a_{j'j}\left(g^{-1}\right). \qquad (*)$$

Возьмём $\varphi = E_{i_0j_0} = \begin{pmatrix} & & \\ & 1 & \\ & & \end{pmatrix}$, где единица стоит на i_0-й строке в j_0-м столбце. Тогда:

1. при $\rho_1 \not\cong \rho_2$ подставим φ в 7 и воспользуемся пунктом 1 следствия:

$$\widetilde{\varphi_{ij}} = \frac{1}{|G|}\sum_{g\in G} b_{ii_0}(g)\,a_{j_0j}\left(g^{-1}\right) = 0 \qquad \forall\, i, i_0, j, j_0; \qquad (**)$$

2. при $V = W$, $\rho_1 = \rho_2 = \rho$ $\operatorname{tr}\varphi = \sum\limits_i \varphi_{ii} = \sum\limits_{i,j} \delta_{ij}\varphi_{ij}$ и $\widetilde{\varphi} = \frac{\operatorname{tr}\varphi}{\dim V}\mathcal{E}$, откуда $\widetilde{\varphi_{ij}} = \delta_{ij}\frac{\operatorname{tr}\varphi}{\dim V} = \frac{\delta_{ij}}{\dim V}\sum\limits_{i',j'}\delta_{i'j'}\varphi_{i'j'}$.

   Сравнивая (∗) и (∗∗), получаем:

$$\frac{1}{|G|}\sum_{g\in G} b_{ii_0}(g)\, a_{j_0 j}\left(g^{-1}\right) = \frac{\delta_{ij}\delta_{i_0 j_0}}{\dim V}\,^{13)}.$$

§ 8. Характеры представлений

Пусть $\rho\colon G \to \mathbf{GL}(V)$ — представление группы G над полем F.

Определение. *Характером представления* ρ называется функция $\chi_\rho\colon G \to F$, $\chi_\rho(g) = \operatorname{tr}\rho(g)$.

Всюду далее полагаем $F = \mathbb{C}$. Если $\lambda_1, \ldots, \lambda_n$ — собственные значения $\rho(g)$ с учётом алгебраической кратности, то $\chi_\rho(g) = \lambda_1 + \ldots + \lambda_n$. Ясно, что если заменить ρ на эквивалентное представление $C\rho C^{-1}$, то, так как при сопряжении след не меняется, не меняется и характер.

Предложение 3.

1. $\chi_\rho(e) = \dim V$;
2. $\chi_\rho\left(h^{-1}gh\right) = \chi_\rho(g)\ \ \forall\, g, h \in G$, *то есть* χ_ρ *постоянна на классах сопряжённости;*
3. *если* $\operatorname{ord}(g) < +\infty$, *то* $\chi_\rho\left(g^{-1}\right) = \overline{\chi_\rho(g)}$;
4. $\chi_{\rho_1\oplus\rho_2} = \chi_{\rho_1} + \chi_{\rho_2}$.

□

1. $\chi_\rho(e) = \operatorname{tr} E = \dim V$.
2. $\chi_\rho\left(h^{-1}gh\right) = \operatorname{tr}\rho\left(h^{-}1\right)\rho(g)\rho(h) = \operatorname{tr}\rho(g) = \chi_\rho(g)$.
3. Если $\lambda_1, \ldots, \lambda_n$ — собственные значения $\rho(g)$, то $\lambda_1^{-1}, \ldots, \lambda_n^{-1}$ — собственные значения $\rho\left(g^{-1}\right)$.

   $\lambda_i^{\operatorname{ord}(g)} = 1 \Rightarrow |\lambda_i| = 1 \Rightarrow \lambda_i^{-1} = \overline{\lambda_i} \Rightarrow \chi_\rho\left(g^{-1}\right)\operatorname{tr}\rho\left(g^{-1}\right) = \sum\limits_{i=1}^n \lambda_i^{-1} = \sum\limits_{i=1}^n \overline{\lambda_i} = \overline{\sum\limits_{i=1}^n \lambda_i} = \overline{\chi_\rho(g)}$.
4. $\operatorname{tr}\begin{pmatrix}\rho_1(g) & 0\\ 0 & \rho_2(g)\end{pmatrix} = \operatorname{tr}\rho_1(g) + \operatorname{tr}\rho_2(g)$.

■

Всюду далее G конечна. Множество всех функций $F(G) = \{f\colon G \to \mathbb{C}\}$ — конечномерное векторное пространство: $(\alpha_1 f_1 + \alpha_2 f_2)(g) \overset{\text{def}}{=} \alpha_1 f_1(g) + \alpha_2 f_2(g)$, базис — $\left\{\delta_h(g) = \begin{cases}1, & h = g,\\ 0, & h \neq g\end{cases} \mid h \in G\right\}$. В частности, $\dim F(G) = |G|$.

Определение. Функция $f \in F(G)$ называется *центральной*, если она постоянна на классах сопряжённости, то есть $f\left(hgh^{-1}\right) = f(g)\ \ \forall\, g, h \in G$. Подпространство центральных функций в $F(G)$ обозначим как $F_C(G)$.

Ясно, что $\chi_\rho \in F_C(G)$.

Пусть $K_1, \ldots, K_r$ — все классы сопряжённости в G. Тогда $\left\{\widetilde{f_i}(g) = \begin{cases}1, & g \in K_i,\\ 0, & g \notin K_i\end{cases} \mid i \in \{1, \ldots, r\}\right\}$ — базис в $F_C(G)$.

Превратим $F(G)$ в эрмитово векторное пространство: $(f_1, f_2) \overset{\text{def}}{=} \frac{1}{|G|}\sum\limits_{g\in G} f_1(g)\,\overline{f_2(g)}$.

Лемма 2. $(\cdot\,,\cdot)$ — *невырожденная эрмитова форма.*

□ Линейность по первому аргументу очевидна.

$(f_2, f_1) = \frac{1}{|G|}f_2(g)\,\overline{f_1(g)} = \overline{(f_1, f_2)} \Rightarrow$ эрмитовость проверена.

Остаётся невырожденность: если f лежит в ядре, надо доказать, что она нулевая. Действительно, $(f, \delta_h) = \frac{1}{|G|}\sum\limits_{g\in G} f(g)\,\overline{\delta_h(g)} = \frac{1}{|G|}f(h) \Rightarrow f \equiv 0$. ■

Теорема 7 (соотношение ортогональности для характеров). *Пусть* ρ_1 *и* ρ_2 — *неприводимые комплексные представления конечной группы* G. *Тогда* $(\chi_{\rho_1}, \chi_{\rho_2}) = \begin{cases}1, & \rho_1 \cong \rho_2,\\ 0, & \rho_1 \ncong \rho_2.\end{cases}$

[13)] На самом деле $(b_{ij}(g))$ и $(a_{ij}(g))$ в этом случае совпадают.

Конец лекции № 16 от 18 ноября 2013 г. (к началу)

Начало лекции № 17 от 25 ноября 2013 г.

□ В наших обозначениях $\chi_{\rho_1}(g) = \sum_j a_{jj}(g)$, $\chi_{\rho_2}(g) = \sum_i b_{ii}(g)$.

Пусть $\rho_1 \not\cong \rho_2$. Подставляя в (∗) (используется неприводимость представлений) $i_0 = i$, $j_0 = j$ и суммируя равенства для всех i и j, получаем $0 = \frac{1}{|G|}\sum_{g\in G}\sum_{i,j} b_{ii}(g)\,a_{jj}\left(g^{-1}\right) = \frac{1}{|G|}\sum_{g\in G}\left(\sum_i b_{ii}(g)\right)\left(\sum_j a_{jj}\left(g^{-1}\right)\right) =$
$= \frac{1}{|G|}\sum_{g\in G}\chi_{\rho_2}(g)\,\chi_{\rho_1}\left(g^{-1}\right) = {}^{14)}\frac{1}{|G|}\sum_{g\in G}\chi_{\rho_2}(g)\,\overline{\chi_{\rho_1}(g)} = (\chi_{\rho_2}, \chi_{\rho_1})$.

Пусть $\rho_1 \cong \rho_2$. Тогда считаем, что $V = W$ и $\rho_1 = \rho_2 = \rho$. Аналогично в (∗∗) подставляя $i_0 = i$, $j_0 = j$ и суммируя равенства для всех i и j, получаем $1 = \frac{\sum_{i,j}\delta_{ij}}{\dim V} = \frac{1}{|G|}\sum_{g\in G}\left(\sum_i b_{ii}(g)\right)\left(\sum_j a_{jj}\left(g^{-1}\right)\right) = \frac{1}{|G|}\sum_{g\in G}\chi_{\rho_2}(g)\,\overline{\chi_{\rho_1}(G)} =$
$= (\chi_{\rho_2}, \chi_{\rho_1})$. ■

Определение. Пусть $\rho\colon G \to \mathbf{GL}(V)$ — представление группы G, $\rho = \rho_1 \oplus \ldots \oplus \rho_k$ — разложение ρ в прямую сумму неприводимых. Тогда *кратностью вхождения* неприводимого представления $\widetilde{\rho}$ в ρ называется число $|\{\rho_i \cong \widetilde{\rho} \mid i \in \{1, \ldots, k\}\}|$.

Теорема 8. *Пусть G — конечная группа, $\rho\colon G \to \mathbf{GL}(V)$ — комплексное представление. Тогда:*

1. *кратность вхождения $\widetilde{\rho}$ в ρ равна $(\chi_\rho, \chi_{\widetilde{\rho}})$. В частности, кратность вхождения не зависит от разложения ρ в прямую сумму неприводимых;*
2. *два комплексных представления $\rho\colon G \to \mathbf{GL}(V)$ и $\rho'\colon G \to \mathbf{GL}(W)$ эквивалентны $\Leftrightarrow \chi_\rho = \chi_{\rho'}$.*

□

1. Мы знаем, что $\rho = \rho_1 \oplus \ldots \oplus \rho_k \Rightarrow \chi_\rho = \chi_{\rho_1} + \ldots + \chi_{\rho_k}$. Тогда $(\chi_\rho, \chi_{\widetilde{\rho}}) = (\chi_{\rho_1}, \chi_{\widetilde{\rho}}) + \ldots + (\chi_{\rho_k}, \chi_{\widetilde{\rho}})$. Это сумма нулей и единиц, причём единицы отвечаю случаю, когда $\rho_i \cong \widetilde{\rho} \Rightarrow$ эта сумма равна кратности вхождения $\widetilde{\rho}$ в ρ.
2. - $\boxed{\Rightarrow}$
   Уже обсуждалось: характер — это, по определению, след, который при переходе к эквивалентному представлению, то есть при сопряжении, не меняется.
   - $\boxed{\Leftarrow}$
   Пусть $\chi_\rho = \chi_{\rho'}$. Тогда, по теоремам 1 и 2 Машке, в разложения ρ и ρ' на неприводимые входят одни и те же слагаемые с одними и теми же кратностями $\Rightarrow \rho \cong \rho_1 \oplus \ldots \oplus \rho_k \cong \rho'$.

■

Следствие. Число (классов эквивалентности) неприводимых комплексных представлений конечной группы G конечно.

□ Попарно ортогональные векторы линейно независимы, что следует из курса линейной алгебры $\Rightarrow$ в конечномерном пространстве таких векторов лишь конечное число $\Rightarrow$ характеров неприводимых представлений конечное число $\Rightarrow$ по пункту 2 теоремы 8, и самих неприводимых представлений конечное число. ■

§ 9. Неприводимые комплексные представления конечных групп

Теорема 9. *Число (классов эквивалентности) неприводимых комплексных представлений конечной группы G равно числу r классов сопряжённости в G.*

Пример 8. Пусть $G = A$ — конечная абелева группа. Все неприводимые комплексные представления одномерны, и их число равно $|A|$. С другой стороны, все классы сопряжённости A одноэлементны, значит, и их число равно $|A|$.

□ Пусть $\rho_1, \ldots, \rho_s$ — все (попарно неэквивалентные) неприводимые комплексные представления группы G. Тогда их характеры $\chi_{\rho_1}, \ldots, \chi_{\rho_s}$ — попарно ортогональные центральные функции на G. Они линейно независимы, и их число не превосходит $\dim F_C(G) = r$. Таким образом, $s \leqslant r$.

[14)] По предложению 3.

Лемма 3. *Пусть $f \in F_C(G)$, $\rho\colon G \to \mathbf{GL}(V)$ — неприводимое представление. Тогда $L_{f,\rho} = L\colon V \to V$, $L = \sum\limits_{h\in G} \overline{f(h)}\rho(h)$, имеет вид $\lambda\mathcal{E}$, где $\lambda = \frac{|G|}{\dim V}(\chi_\rho, f)$.*

□ Получаем $\rho(g) L\rho\left(g^{-1}\right) = \sum\limits_{h\in G} \overline{f(h)}\rho(g)\rho(h)\rho\left(g^{-1}\right) = \sum\limits_{h\in G} \overline{f\left(ghg^{-1}\right)}\rho\left(ghg^{-1}\right) = \sum\limits_{h\in G} \overline{f(h)}\rho(h) = L$. Отсюда $\rho(g) L = L\rho(g) \Rightarrow$ по лемме Шура, $L = \lambda\mathcal{E}$.

Вычисляем след: $\lambda \dim V = \operatorname{tr}\lambda\mathcal{E} = \operatorname{tr} L = \sum\limits_{h\in G} \overline{f(h)} \operatorname{tr}\rho(h) = |G|\,|G|^{-1} \sum\limits_{h\in G} \chi_\rho(h)\,\overline{f(h)} = |G|(\chi_\rho, f) \Rightarrow \lambda = \frac{|G|}{\dim V}(\chi_\rho, f)$. ■

Лемма 4. *Характеры $\chi_{\rho_1}, \ldots, \chi_{\rho_s}$ образуют ортонормированный базис $F_C(G)$.*

□ Эти характеры можно дополнить до ортонормированного базиса $F_C(G)$. Пусть при дополнении до базиса действительно добавляется некоторая функция $f \in F_C(G)$, то есть $(\chi_{\rho_i}, f) = 0\ \forall i \in \{1, \ldots, s\}$. Тогда, по лемме 3, $L_{f,\rho_i} = \frac{|G|}{\dim \rho_i}(\chi_{\rho_i}, f)\,\mathcal{E} = 0$. По теореме 2 Машке, $\rho = m_1\rho_1 \oplus \ldots \oplus m_s\rho_s$, где $m_i \geqslant 0$ — кратности. Тогда $L_{f,\rho} = \bigoplus\limits_i m_i L_{f,\rho_i} = 0$. С другой стороны, применим это к регулярному представлению $\rho\colon G \to \mathbf{GL}(V_G)$, $V_G = \langle e_h \mid h \in G\rangle$, $\rho(g) e_h = e_{gh}$. Тогда $0 = L_{f,\rho}(e_e) = \sum\limits_{h\in G} \overline{f(h)} e_e = \sum\limits_{h\in G} \overline{f(h)} e_h$. Это линейная комбинация базисных векторов V_G, равная нулю $\Rightarrow \overline{f(h)} = 0\ \forall h \in G \Rightarrow f = 0$. ■

Таким образом, по лемме 4, $s = r$. ■

Теорема 10. *Пусть G — конечная группа, $\rho_1, \ldots, \rho_r$ — все её неприводимые представления, $n_i \stackrel{\text{def}}{=} \dim \rho_i$. Тогда:*

1. *кратность вхождения представления ρ_i в регулярное представление ρ равна n_i;*
2. $|G| = \sum\limits_{i=1}^{r} n_i^2$.

□

1. Вычислим характер регулярного представления ρ.

   $\chi_\rho(e) = \dim V_G = |G|$, по построению.

   $\chi_\rho(h)\ \forall h \neq e$, поскольку $\rho(h) e_g = e_{hg} \neq e_g$ (то есть любой базисный вектор перейдёт в другой базисный вектор, что сделает диагональ нулевой).

   Далее, $(\chi_\rho, \chi_{\rho_i}) = \frac{1}{|G|} \sum\limits_{g\in G} \chi_\rho(g)\,\overline{\chi_{\rho_i}(g)} = \frac{1}{|G|}|G|\,\overline{\chi_{\rho_i}(e)} = \overline{n_i} = n_i$, так как $n_i \in \mathbb{Z}_+$. По пункту 1 теоремы 8, кратность вхождения равна n_i.

2. Итак, $\rho = n_1\rho_1 \oplus \ldots \oplus n_r\rho_r$, и $|G| = \chi_\rho(e) = n_1\chi_{\rho_1}(e) + \ldots + n_r\chi_{\rho_r}(e) = n_1 \cdot n_1 + \ldots + n_r \cdot n_r = \sum\limits_{i=1}^{r} n_i^2$.

■

Пример 9. $G = \mathbf{S}_3$.

Одномерных представлений $\left|{}^{\mathbf{S}_3}\!/_{\mathbf{S}_3'}\right| = 2$: id и sgn.

$|\mathbf{S}_3| = 6 = 1^2 + 1^2 + 4 = 1^2 + 1^2 + 2^2$, то есть есть ещё одно двумерное представление. Им оказывается каноническое.

Задача 9. *Доказать, что любое семимерное комплексное представление $\mathbf{S}_3$ обладает инвариантной прямой.*

Пример 10. $G = \mathbf{S}_4$.

Одномерных представлений $\left|{}^{\mathbf{S}_4}\!/_{\mathbf{S}_4'}\right| = 2$: id и sgn.

$|\mathbf{S}_4| = 24 = 1^2 + 1^2 + 22 = 1^2 + 1^2 + 2^2 + 3^2 + 3^2$, то есть ещё одно двумерное и два трёхмерных представления.

Рассмотрим композицию гомоморфизма $\mathbf{S}_4 \to {}^{\mathbf{S}_4}\!/_{\mathbf{S}_4''} = {}^{\mathbf{S}_4}\!/_{\mathbf{V}_4} \cong \mathbf{S}_3$ и канонического представления $\mathbf{S}_3 \to \mathbf{GL}_2(\mathbb{C})$. Такая композиция даст двумерное неприводимое представление $\mathbf{S}_4$.

Остались трёхмерные. Нам известно, что группа симметрий тетраэдра и группа вращений куба изоморфны $\mathbf{S}_4$. Помещаем начало координат в середину тетраэдра (куба), записываем матрицами все симметрии (вращения) и получаем два трёхмерных вещественных, то есть и комплексных, представления. Так как мы знаем

классификацию одномерных и двумерных представлений, у них у всех в ядре лежит $\mathbf{V}_4$. Но в ядре трёхмерных представлений $\mathbf{V}_4$ лежать не может, так как определяет нетривиальные симметрии тетраэдра (вращения куба). Таким образом, построенные трёхмерные представления не могут распасться в сумму неприводимых меньших размерностей, что доказывает их неприводимость. Также они неэквивалентны, так как для представления через тетраэдр определитель равен ± 1, а через куб — 1.

Каноническое представление тоже неприводимо и трёхмерное. Но оказывается, что оно изоморфно представлению через тетраэдр: из теоремы 10 следует, что хотя бы одному из построенных трёхмерных представлений оно должно быть изоморфно, а его определитель равен ± 1.

Конец лекции № 17 от 25 ноября 2013 г. *(к началу)*

Начало лекции № 18 от 27 ноября 2013 г.

III. Кольца и поля

§ 1. Основные определения и примеры

Определение. Множество R с двумя бинарными операциями «$+$» и «$\times$» называется *кольцом*, если:

1. $(R, +)$ — абелева группа (её нейтральный элемент будем обозначать как 0);
2. операции удовлетворяют свойству дистрибутивности:
   - $a(b+c) = ab + ac$ (дистрибутивность слева);
   - $(b+c)a = ba + ca$ (дистрибутивность справа);

   $\forall\, a, b, c \in R$.

В этом курсе добавим ещё два условия:

3. умножение ассоциативно: $a(bc) = (ab)c \ \ \forall\, a, b, c \in R$;
4. $\exists 1 \in R$: $1 \cdot a = a \cdot 1 = a \ \ \forall\, a \in R$.

Таким образом, мы сделали $(R, \times)$ моноидом.

Определение. Кольцо R коммутативно, если $ab = ba \ \ \forall\, a, b \in R$.

Определение. Пусть F — поле. Тогда векторное пространство A над F называется *F-алгеброй*, или просто *алгеброй*, если на A задано билинейное отображение $A \times A \to A$, $(a, b) \mapsto ab$, такое что $(A, +, \times)$ — кольцо.

Пример 1.

1. $R = \mathbb{Z}, \mathbb{Z}_n$ — кольца.
2. Если F — поле, то F, $F[x_1, \ldots, x_n]$, $\mathrm{Mat}_n(F)$ — F-алгебры.
3. Если F — поле, то функции $f\colon M \to F$, где M — произвольное множество, можно складывать и умножать на скаляр ($(\lambda_1 f_1 + \lambda_2 f_2)(m) = \lambda_1 f_1(m) + \lambda_2 f_2(m)$) и перемножать ($(f_1 f_2)(m) = f_1(m) f_2(m)$). Тогда $\mathcal{F}(M, F) \stackrel{\text{def}}{=} \{f\colon M \to F\}$ — F-алгебра.
4. Если R — кольцо (алгебра), то кольцами (алгебрами) являются множества
   - многочленов над R $R[x] = \left\{a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \mid a_i \in R, n \in \mathbb{N}\right\}$;
   - формальных степенных рядов над R $R[[x]] = \left\{a_0 + a_1 x + a_2 x^2 + \ldots \mid a_i \in R\right\}$;
   - матриц над R $\mathrm{Mat}_n(R)$;
   - верхнетреугольных матриц над R $\mathbf{B}_n(R)$;

   при этом $\mathrm{Mat}_n(R)$ — некоммутативное кольцо (алгебра).

Определение.

1. *Делителем нуля* в кольце R называется $0 \neq a \in R$, такой что $\exists\, 0 \neq b \in R$: $ab = 0$ (тогда a — *левый делитель нуля*) или $ba = 0$ (тогда a — *правый делитель нуля*).
2. Элемент $a \in R$ *обратим*, если $\exists\, a^{-1} \in R$: $aa^{-1} = a^{-1}a = 1$.
3. Элемент $0 \neq a \in R$ *нильпотентен*, если $\exists\, n \in \mathbb{N}$: $a^n = 0$.
4. Элемент $a \in R$ *идемпотентен*, если $a^2 = a$. Например, 0, 1 — идемпотенты, и в поле других нет.

Пример 2. Пусть $R = \mathbb{Z}_n$. Оно является полем $\Leftrightarrow$ n — простое.

1. Делителями нуля являются элементы $\overline{k} \in \mathbb{Z}_n$: $\overline{k} \neq \overline{0}$, $(k, n) \neq 1$.
2. Обратимы элементы $\overline{k} \in \mathbb{Z}_n$: $(k, n) = 1$.
3. Пусть $n = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$, Тогда $\overline{k} \in \mathbb{Z}_n$ — нильпотент $\Leftrightarrow$ $\overline{k} \neq \overline{0}$, $p_1 \ldots p_s \,\big|\, k$. Нильпотентов нет $\Leftrightarrow$ $\alpha_i = 1$ $\forall\, i \in \{1, \ldots, s\}$, то есть n *свободно от квадратов*.

4. Общая ситуация с идемпотентами сложнее. Частный случай: $n = 6 \Rightarrow \overline{3}^2 = \overline{3}, \overline{4}^2 = \overline{4} \Rightarrow \overline{3}, \overline{4}$ — идемпотенты.

Определение. Пусть G — группа, F — поле, V_G — векторное пространство над полем F с базисом $\{e_g \mid g \in G\}$. Положим $e_g e_h \stackrel{\text{def}}{=} e_{gh}$ и продолжим это умножение на всё пространство по билинейности. Тем самым получим *групповую алгебру* FG.

FG коммутативна $\Leftrightarrow$ G абелева.

Гипотеза Капланского: в FG нет делителей нуля $\Leftrightarrow$ G — группа без кручения, то есть в G любой ненулевой элемент имеет бесконечный порядок.

Определение. Коммутативное кольцо F называется *полем*, если любой его ненулевой элемент обратим.

Определение. *Подкольцом* R_1 кольца R называется подгруппа R по сложению, такая что $\forall\, a, b \in R_1 \ ab \in \in R_1$. Дополнительно потребуем $1 \in R_1$. Аналогично определяется *подалгебра* (подкольцо и подпространство) и *подполе* (подкольцо F_1: $\forall\, a \in F_1 \ a^{-1} \in F_1$). Если есть поле F и его подполе F_1, то говорят о *расширении полей*.

Пример 3.

1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$, p — простое, — поля.
2. Пусть F — поле. Тогда $F(x) \stackrel{\text{def}}{=} \left\{ \frac{f(x)}{g(x)} \mid f, g \in F[x] \right\}$, где полагаем $\frac{f}{g} = \frac{f_1}{g_1} \Leftrightarrow f g_1 = f_1 g$, — *поле рациональных дробей* над полем F. Отсюда:
3. $\mathbb{Z}_p(x)$ — бесконечное поле характеристики p.
4. $\mathbb{C}(x)$ — поле, строго содержащее $\mathbb{C}$.

Определение. *Прямым произведением колец (алгебр)* R_1 *и* R_2 называется кольцо (алгебра) $R_1 \times R_2 \stackrel{\text{def}}{=} \stackrel{\text{def}}{=} \{(r_1, r_2) \mid r_1 \in R_1, r_2 \in R_2\}$.

Замечание. Но для полей F_1 и F_2 определённое таким образом $F_1 \times F_2$ — не поле, так как в нём есть делители нуля: $(a, 0)(0, b) = (0, 0)$.

Определение. Пусть R — коммутативное кольцо без делителей нуля. Тогда *полем частных* называется $QR \stackrel{\text{def}}{=} \left\{ \frac{r_1}{r_2} \mid r_1, r_2 \in R, r_2 \neq 0 \right\}$, где $\frac{r_1}{r_2} = \frac{r_3}{r_4} \Leftrightarrow r_1 r_4 = r_2 r_3$. Таким образом, $R \hookrightarrow QR$, $r \mapsto \frac{r}{1}$.

Задача 1. *Доказать, что* $a_0 + a_1 x + a_2 x^2 + \ldots \in F[[x]]$ *обратим* $\Leftrightarrow a_0 \neq 0$.

Пример 4. $(1 + x)^{-1} = 1 - x + x^2 - x^3 + x^4 - \ldots + (-1)^n x^n + \ldots$, что проверяется перемножением.

Определение. Пусть F — поле. Тогда $F((x)) \stackrel{\text{def}}{=} \left\{ a_{-k} x^{-k} + \ldots + a_0 + a_1 x + \ldots \mid a_i \in F \ \forall\, i \geqslant -k \right\}$ — поле. $a_{-k} x^{-k} + \ldots + a_0 + a_1 x + \ldots$ обратим, так как $x^k \left(a_{-k} x^{-k} + \ldots + a_0 + a_1 x + \ldots \right) = \underbrace{a_{-k}}_{\neq 0} + a_{-k+1} + \ldots + a_0 x^k + \\ + a_1 x^{k+1} + \ldots$ обратим, по задаче 1. Таким образом, $F(x) \subseteq F((x))$.

§ 2. Идеалы и факторкольца

Определение. Пусть R — кольцо. $I \subseteq R$ называется *идеалом*, если $I \subseteq (R, +)$ — подгруппа и выполняется хотя бы одно из двух условий:

1. $ca \in I \ \ \forall\, c \in R, a \in I$ (тогда I — *левый идеал*);
2. $ac \in I \ \ \forall\, c \in R, a \in I$ (тогда I — *правый идеал*).

Если выполнены оба условия, то идеал называется *двусторонним*.

Пример 5. Пусть $R = \mathrm{Mat}_n(F)$, где F — поле. Тогда $I = \left\{ \begin{pmatrix} * & & 0 \\ * & & \\ * & & \\ * & & \end{pmatrix} \right\}$ — левый, но не правый идеал.

Дальше рассматриваем только двусторонние идеалы, называя их просто идеалами.

Лемма 1. *Пусть* I *— идеал в кольце* R*. Тогда* $I = R \Leftrightarrow I$ *содержит обратимый элемент.*

□

- $\boxed{\Rightarrow}$

  $I = R \Rightarrow 1 \in I$, а 1 — обратимый элемент.

- $\boxed{\Leftarrow}$
  $a \in I \Rightarrow aa^{-1} = 1 \in I \Rightarrow \forall\, c \in R\, c \cdot 1 = c \in I \Rightarrow I = R.$

■

Следствие. В полях нет нетривиальных идеалов.

Определение. Пусть R — коммутативное кольцо. Тогда с каждым набором элементов $\{r_i \mid i \in \mathcal{I}\}$ связан идеал $I = \{h_1 r_{i_1} + \ldots + h_k r_{i_k}\}$. То, что это идеал, очевидно; более того, это наименьший идеал, содержащий все элементы $\{r_i\}$. Если множество $\mathcal{I}$ конечно, то есть набор элементов $\{r_1, \ldots, r_k\}$ конечен, то I обозначают $(r_1, \ldots, r_k)$ и называют идеалом, *порождённым* $\{r_1, \ldots, r_k\}$.

Определение. Идеал I называется *главным*, если $\exists\, r \in I\colon I = (r) = \{hr \mid h \in R\}$.

Определение. Кольцо R называется *кольцом главных идеалов*, если любой идеал в R — главный.

Предложение 1. *Кольца $\mathbb{Z}$ и $F[x]$, где F — поле, — кольца главных идеалов.*

□ Идеал является, в частности, подгруппой, а мы знаем, что в $(\mathbb{Z}, +)$ все подгруппы имеют вид $n\mathbb{Z}$, $n \in \mathbb{Z}_+$. Значит, любой идеал в $\mathbb{Z}$ имеет вид (n).

Пусть $I \subseteq F[x]$ — идеал, $f \in I$, $f \neq 0$, наименьшей степени. Тогда $(f) \subseteq I$. Обратно, $\forall\, g \in I$, по теореме о делении с остатком, $g = fq + r$, где $\deg r < \deg f$ $(\deg 0 \stackrel{\text{def}}{=} -\infty) \Rightarrow r = g - fq \in I \Rightarrow r = 0 \Rightarrow I = (f)$. ■

Пример 6. Пусть $R = F[x, y]$, $I = (x, y) = \{a_0 + a_1 x + a_2 y + \ldots \mid a_0 = 0\}$. Предположим, что I — главный идеал, то есть $\exists\, f \in I\colon I = (f)$. Тогда, по определению, $f \,\big|\, x$, $f \,\big|\, y \Rightarrow f = \text{const} \neq 0$. Любая ненулевая константа обратима $\Rightarrow$ по лемме 1, $I = F[x, y]$. Получившееся противоречие показывает, что I — неглавный идеал.

Конец лекции № 18 от 27 ноября 2013 г. (к началу)

Начало лекции № 19 от 2 декабря 2013 г.

Пусть теперь кольцо R не обязательно коммутативно.

Определение. Кольцо (алгебра) называется *простым (-ой)*, если в нём (ней) нет нетривиальных двусторонних идеалов, то есть нет двусторонних идеалов, кроме $\{0\}$ и R.

Определение. *Центром кольца (алгебры)* называется $Z(R) \stackrel{\text{def}}{=} \{a \in R \mid ab = ba\ \forall\, b \in R\}$.

Центр кольца — подкольцо, но, как правило, не идеал. Центр кольца — идеал $\Leftrightarrow$ кольцо коммутативно (центр — идеал $\Leftrightarrow$ идеал содержит единицу $\Leftrightarrow$ идеал — всё кольцо $\Leftrightarrow$ кольцо коммутативно).

Определение. F-алгебра A называется *центральной*, если $Z(A) = \{\lambda \cdot 1 \mid \lambda \in F\}$.

Теорема 1. *Пусть F — поле. Тогда $\mathrm{Mat}_n(F)$ — центральная простая алгебра над F $\forall\, n \in \mathbb{N}$.*

□ Из первого семестра известно, что если $\mathcal{AB} = \mathcal{BA}$ $\forall\, \mathcal{B} \in \mathrm{Mat}_n(F)$[15], то $\mathcal{A} = \lambda\mathcal{E}$, $\lambda \in F$, что доказывает центральность.

Пусть $I \subseteq \mathrm{Mat}_n(F)$ — двусторонний идеал, $0 \neq \mathcal{A} = \sum\limits_{i,j} a_{ij}\mathcal{E}_{ij} \in I$. Тогда $\exists\, k, l \in \{1, \ldots, n\}\colon a_{kl} \neq 0 \Rightarrow$ $\Rightarrow \mathcal{E}_{st} = a_{kl}^{-1}\mathcal{E}_{sk}\mathcal{A}\mathcal{E}_{lt} \in I$ $\forall\, s, t \in \{1, \ldots, n\}$. Но матричные единицы — базис $\mathrm{Mat}_n(F)$ как векторного пространства $\Rightarrow I = \mathrm{Mat}_n(F)$. ■

Определение. Пусть $I \subseteq R$ — двусторонний идеал в кольце R. На факторгруппе по сложению ${}^{R}\!/_{I}$ определим умножение: $(a + I)(b + I) \stackrel{\text{def}}{=} ab + I$. Проверим корректность такого задания умножения: если $i, j \in I$, то $(a + i + I)(b + j + I) = (a + i)(b + j) + I = ab + \underbrace{aj}_{\in I} + \underbrace{bi}_{\in I} + \underbrace{ij}_{\in I} + I = ab + I$. Ассоциативность и дистрибутивность очевидны, есть единица $1 + I$. Итак, задано *факторкольцо* по идеалу I.

Пример 7.

1. ${}^{\mathbb{Z}}\!/_{(n)} \cong \mathbb{Z}_n$.
2. ${}^{\mathbb{R}[x]}\!/_{(x^2+1)} \cong \mathbb{C}$.

Определение. *Гомоморфизмом колец* R и S называется отображение $\varphi\colon R \to S$, являющееся гомоморфизмом абелевых групп и такое, что $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall\, a, b \in R$ и $\varphi(1) = 1$.

Лемма 2.

1. $\mathrm{Ker}\,\varphi \subseteq R$ — *двусторонний идеал.*
2. $\mathrm{Im}\,\varphi \subseteq R$ — *подкольцо.*

[15] Все матрицы здесь обозначены буквами в особом начертании, чтобы не путать их обозначения с обозначением самой алгебры.

□

1. Мы знаем, что $\operatorname{Ker}\varphi$ — подгруппа и $\forall a \in \operatorname{Ker}\varphi, c \in R\ \varphi(ac) = \varphi(a)\varphi(c) = 0 \cdot \varphi(c)$. При этом $\forall b \in S$ $(0+0)b = 0 \cdot b + 0 \cdot b = 0 \cdot b \Rightarrow 0 \cdot b = 0$. Отсюда $0 \cdot \varphi(c) = 0$.
2. Аналогично.

■

Замечание. Если $\varphi\colon R \to S$ — гомоморфизм колец, R — поле, то φ инъективно.

□ $\operatorname{Ker}\varphi$ — идеал $\Rightarrow \operatorname{Ker}\varphi = \{0\}$. ■

Теорема 2 (о гомоморфизме). *Пусть $\varphi\colon R \to S$ — гомоморфизм колец. Тогда отображение $\psi\colon \operatorname{Im}\varphi \to {}^{R}\!/_{\operatorname{Ker}\varphi}$, $b = \varphi(a) \mapsto a + \operatorname{Ker}\varphi$, является изоморфизмом колец, то есть $\operatorname{Im}\varphi \cong {}^{R}\!/_{\operatorname{Ker}\varphi}$.*

□ ψ корректно определено и является изоморфизмом абелевых групп.

Остаётся проверить сохранение умножения. Пусть $b = \varphi(a) \in \operatorname{Im}\varphi$, $d = \varphi(c) \in \operatorname{Im}\varphi$. Тогда $bd = \varphi(ac)$, $\psi(bd) = ac + \operatorname{Ker}\varphi = (a + \operatorname{Ker}\varphi)(c + \operatorname{Ker}\varphi) = \psi(b)\psi(d)$. ■

Пример 8.

1. $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, $a_0 + a_1x + \ldots + a_nx^n \mapsto \overline{a_0} + \overline{a_1}x + \ldots + \overline{a_n}x^n \Rightarrow \operatorname{Ker}\varphi = (p\mathbb{Z})[x]$, $\operatorname{Im}\varphi = \mathbb{Z}_p[x] \Rightarrow \mathbb{Z}_p[x] \cong$ $\cong {}^{\mathbb{Z}[x]}\!/_{(p\mathbb{Z})[x]}$.
2. Пусть $R = \mathcal{F}(M, F)$, где M — произвольное множество, F — поле. С каждой точкой $m \in M$ связан гомоморфизм $\varphi_m\colon R \to F$, $f \mapsto f(m)$. Тогда $\operatorname{Ker}\varphi_m = \{f \in R \mid f(m) = 0\} = I_m$, $\operatorname{Im}\varphi_m = F \Rightarrow F \cong {}^{R}\!/_{I_m}$.

Предложение 2. *Пусть F — поле, $f \in F[x]$. Тогда ${}^{F[x]}\!/_{(f)}$ — поле $\Leftrightarrow$ f неприводим.*

□

- $\boxed{\Rightarrow}$

  Пусть, от противного, f приводим, то есть $f(x) = p_1(x)p_2(x)$, где $p_i \in F[x]$, $\deg p_i \geqslant 1$. Тогда классы $p_1 + I$, $p_2 + I$, где $I = (f)$, отличны от нулевых, и $(p_1 + I)(p_2 + I) = p_1p_2 + I = f + I = 0 + I \Rightarrow$ в ${}^{F[x]}\!/_{(f)}$ есть делители нуля $\Rightarrow$ ${}^{F[x]}\!/_{(f)}$ — не поле, что противоречит условию.

- $\boxed{\Leftarrow}$

  Пусть f неприводим, $g + I$ — ненулевой класс. Тогда $f \nmid g \Rightarrow$ из неприводимости f, $(f, g) = 1 \Rightarrow$ по лемме о линейном представлении НОД, $\exists u, v \in F[x]$: $gu + fv = 1 \Rightarrow (g + I)(u + I) = gu + I = 1 - \underbrace{fv}_{\in I} + I = 1 + I \Rightarrow$

  $\Rightarrow g + I$ обратим $\Rightarrow$ ${}^{F[x]}\!/_{(f)}$ — поле.

■

Задача 2. *Доказать, что ${}^{F[x]}\!/_{(x-\alpha)} \cong F\ \forall \alpha \in F$.*

Задача 3. *Пусть $f_1, \ldots, f_k \in F[x]$: $(f_i, f_j) = 1\ \forall i \neq j$. Доказать, что тогда ${}^{F[x]}\!/_{(f_1 \ldots f_k)} \cong {}^{F[x]}\!/_{(f_1)} \oplus \ldots \oplus$ $\oplus$ ${}^{F[x]}\!/_{(f_k)}$.*

§ 3. Расширения полей

Пусть $F \subseteq K$ — расширение полей.

Определение. Расширение полей $F \subseteq K$ называется *конечным*, если $\dim_F K < +\infty$, то есть размерность K как векторного пространства над F конечна. В этом случае $[K : F] \stackrel{\text{def}}{=} \dim_F K$ называется *степенью расширения*.

Пример 9.

1. $\mathbb{R} \subseteq \mathbb{C}$ — расширение степени 2.
2. $\mathbb{Q} \subseteq \mathbb{R}$ не является конечным расширением.

Предложение 3. *Пусть $F \subseteq K \subseteq L$ — расширение полей, $F \subseteq K$, $K \subseteq L$ конечны. Тогда $F \subseteq L$ конечно, и $\dim_F L = \dim_F K \cdot \dim_K L$.*

□ Пусть $\{e_1, \ldots, e_n\}$ — базис K над F, $\{f_1, \ldots, f_m\}$ — базис L над K. Достаточно доказать, что $\{e_if_j\}$ — базис L над F.

$\forall a \in L\ a = b_1 f_1 + \ldots + b_m f_m$, $b_i \in K$. Далее, $b_i = \alpha_{1i} e_1 + \ldots + \alpha_{ni} e_n$, $\alpha_{ji} \in F$. Отсюда $a = \left(\sum\limits_j \alpha_{j1} e_j\right) f_1 + \ldots + \left(\sum\limits_j \alpha_{jm} e_j\right) f_m = \sum\limits_{i,j} a_{ji} e_j f_i$. Таким образом, через $\{e_i f_j\}$ всё выражается, и остаётся проверить линейную независимость. Пусть $\sum\limits_{i,j} \gamma_{ij} e_i f_j = 0$, $\gamma_{ij} \in F$. Тогда $\left(\sum\limits_i \gamma_{i1} e_i\right) f_1 + \ldots + \left(\sum\limits_i \gamma_{im} e_i\right) f_m = 0 \Rightarrow \sum\limits_i \gamma_{ij} e_i = 0$ $\forall j \in \{1, \ldots, m\} \Rightarrow \gamma_{ij} = 0\ \forall i, j \Rightarrow \{e_i f_j\}$ линейно независимы $\Rightarrow \{e_i f_j\}$ — базис. ■

Предложение 4. *Пусть $f \in F[x]$ неприводим. Тогда $F \subseteq K = {}^{F[x]}\!/_{(f)}$ конечно и имеет степень $n = \deg f$.*

□ Любой класс из ${}^{F[x]}\!/_{(f)}$ однозначно записывается в виде $a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + I$, где $I = (f)$, $a_i \in F$. Это означает, что $1 + I$, $x + I, \ldots, x^{n-1} + I$ образуют базис K над F. ■

Определение. Пусть $f \in F[x]$ неприводим, $\deg f > 1$. Тогда, по теореме Безу, у f нет корней над F. С другой стороны, рассмотрим класс $\alpha = x + I \in K = {}^{F[x]}\!/_{(f)}$, $I = (f)$. Тогда $f(\alpha) = f(x) + I = 0 + I \Rightarrow \alpha$ корень $f(x)$ над K. Такой переход от F к K называется *присоединением корня* α неприводимого многочлена f к полю F. Поле $K = {}^{F[x]}\!/_{(f)}$ обозначается $F(\alpha) = \left\{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in F\right\}$ с умножением по модулю f.

Определение. Пусть $F \subseteq K$ — расширение полей. Тогда элемент $\alpha \in K$ называется *алгебраическим над F*, если $\exists\, h \in F[x]$: $h \neq 0$, $h(\alpha) = 0$. В противном случае α называется *трансцендентным*.

Пример 10.

1. Рассмотрим расширение полей $\mathbb{R} \subseteq \mathbb{C}$. Все элементы из $\mathbb{C}$ являются корнями многочленов степени $\leqslant 2$ над $\mathbb{R}$, то есть алгебраическими над $\mathbb{R}$.
2. Рассмотрим расширение полей $F \subseteq F(x)$, где $F(x)$ — поле рациональных полей. $x \in F(x)$ трансцендентен над F.

Задача 4. *Доказать, что $\alpha \in F(x)$ — алгебраический элемент над $F \Leftrightarrow \alpha \in F$.*

Конец лекции № 19 от 2 декабря 2013 г. (к началу)

Начало лекции № 20 от 9 декабря 2013 г.

Определение. *Минимальным многочленом* алгебраического элемента $\alpha \in K$ над полем F, где $F \subseteq K$ — расширение полей, называется многочлен $\mu_\alpha \in F[x]$ наименьшей степени, такой что $\mu_\alpha(\alpha) = 0$.

Пример 11. Пусть $F = \mathbb{Q}$, $K = \mathbb{C}$, $\alpha = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$. Тогда α — корень многочлена $x^5 - 1$. Но минимальный ли это многочлен? Нет, так как, разложив его на множители: $x^5 - 1 = (x-1)\left(x^4 + x^3 + x^2 + x + 1\right)$, — можно увидеть, что α — корень многочлена $x^4 + x^3 + x^2 + x + 1$. Является ли этот многочлен минимальным?

Лемма 3.

1. *μ_α неприводим над F.*
2. *$\forall h \in F[x]\ h(\alpha) = 0 \Leftrightarrow \mu_\alpha \mid h$. В частности, μ_α определён однозначно с точностью до умножения на ненулевое число.*

□

1. Пусть $\mu_\alpha(x) = p_1(x)\, p_2(x)$, $p_1, p_2 \in F[x]$. Тогда $\mu_\alpha(\alpha) = p_1(\alpha)\, p_2(\alpha) = 0$. Поскольку работаем в поле, в котором не может быть делителей нуля, то либо $p_1(\alpha) = 0$, либо $p_2(\alpha) = 0$. Пусть $p_1(\alpha) = 0$ (второй случай аналогично). Так как μ_α имеет минимальную степень среди всех многочленов, имеющих корнем α, то $\deg p_1 = 0 \Rightarrow \deg p_2 = \deg \mu_\alpha \Rightarrow \mu_\alpha$ неприводим.
2. По теореме о делении с остатком, $h(x) = \mu_\alpha(x)\, q(x) + r(x)$, $\deg r < \deg \mu_\alpha$. Подставляем α: $h(\alpha) = 0 \Leftrightarrow$ $\Leftrightarrow r(\alpha) = 0 \Leftrightarrow r = 0 \Leftrightarrow \mu_\alpha \mid h$.

■

Задача 5. *Доказать, что $x^4 + x^3 + x^2 + x + 1$ неприводим над Q*[16].

Определение. Пусть $F \subseteq K$ — расширение полей. $\forall \alpha \in K$ обозначим через $F[\alpha]$ подалгебру в K элементов вида $a_0 + a_1\alpha + \ldots + a_m\alpha^m$, где $m \in \mathbb{Z}_+$, $a_i \in F$.

Предложение 5. *Элемент $\alpha \in K$ алгебраичен $\Leftrightarrow F[\alpha]$ конечномерна. В этом случае $F[\alpha]$ является подполем, $F[\alpha] \cong F(\alpha) = {}^{F[x]}\!/_{(\mu_\alpha)}$.*

□

[16] Отсюда будет следовать, что это минимальный многочлен для $\alpha = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$.

- $\boxed{\Leftarrow}$

  Пусть $F[\alpha]$ конечномерна. Тогда $1, \alpha, \alpha^2, \ldots$ линейно зависимы $\Rightarrow \exists m \in Z_+, b_0, b_1, \ldots, b_m \in F$, не все равные нулю: $b_0 + b_1\alpha + \ldots + b_m\alpha^m = 0 \Rightarrow \alpha$ алгебраичен.

- $\boxed{\Rightarrow}$

  Пусть α алгебраичен, μ_α — его минимальный многочлен, $\deg \mu_\alpha = n$. Тогда $\alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_0$, $a_i \in F$. Индукция по k показывает, что при $k \geqslant n$ α^k выражается как линейная комбинация $1, \alpha, \ldots, \alpha^{n-1}$. Значит, $\dim_F F[\alpha] \leqslant n$. Конечномерность этим уже доказана, но на самом деле понятно даже, что $\dim_F F[\alpha] = n$. Действительно, рассмотрим гомоморфизм $\varphi\colon F[x] \to K$, $f \mapsto f(\alpha)$. Его образ $\operatorname{Im}\varphi = F[\alpha]$, его ядро $\operatorname{Ker}\varphi = (\mu_\alpha)$. Тогда, по теореме 5 о гомоморфизме, $F[\alpha] \cong {}^{F[x]}\!/_{(\mu_\alpha)} = F(\alpha)$.

■

Предложение 6. *Пусть $F \subseteq K$ — расширение полей. Тогда все элементы в K, алгебраические над F, образуют подполе $\overline{F}$ — алгебраическое замыкание F в K, и $F \subseteq \overline{F} \subseteq K$.*

Пример 12. *Пусть $F = \mathbb{Q}$, $K = \mathbb{C}$. Тогда $\mathbb{Q} \subseteq \overline{F} = \overline{\mathbb{Q}} = \mathbb{A} \subseteq \mathbb{C}$, где $\overline{\mathbb{Q}} = \mathbb{A}$ — поле алгебраических чисел. Это счётное множетство, так что $\overline{\mathbb{Q}} \subsetneq \mathbb{C}$.*

□ Ясно, что $F \subseteq \overline{F}$, так как элементы F — корни линейных многочленов. Надо проверить, что если α, $\beta \in \overline{F}$, то $\alpha \pm \beta$, $\alpha\beta \in \overline{F}$ и, при $\alpha \neq 0$, $\alpha^{-1} \in \overline{F}$.

Рассмотрим расширение $F \subseteq F(\alpha) \subseteq F(\alpha)(\beta)$. Тогда $\alpha \pm \beta$, $\alpha\beta$, $\alpha^{-1} \in F(\alpha)(\beta)$, так как $F(\alpha)(\beta)$ — поле $\Rightarrow F[\alpha \pm \beta]$, $F[\alpha\beta]$, $F\left[\alpha^{-1}\right]$ — подпространства векторного пространства $F(\alpha)(\beta)$, которое конечномерно над F, по предложениям 3 и 4 $\Rightarrow$ эти подпространства конечномерны $\Rightarrow \alpha \pm \beta$, $\alpha\beta$, $\alpha^{-1} \in \overline{F}$, по предложению 5. ■

§ 4. Поле разложения многочлена

Определение. Пусть $F \subseteq K$ — расширение полей. Говорят, что K *порождается* над F элементами α_1, …, $\alpha_s \in K$, если для любого подполя L: $F \subseteq L \subseteq K$ условие $\alpha_1, \ldots, \alpha_s \in L$ влечёт $L = K$. Другими словами, $K = \left\{ \frac{f(\alpha_1,\ldots,\alpha_s)}{g(\alpha_1,\ldots,\alpha_s)} \mid f, g \in F[x_1, \ldots, x_s], g(\alpha_1, \ldots, \alpha_s) \neq 0 \right\}$.

Пример 13. Поле $F(\alpha)$ порождается элементом α над F.

Определение. Пусть $f \in F[x]$ — произвольный многочлен. Тогда *полем разложения* f над F называется расширение $F \subseteq K$, для которого выполнены два условия:

1. f разлагается над K на линейные множители;
2. K порождается над F корнями f.

Задача 6. *Доказать, что $\mathbb{C}$ — поле разложения $x^2 + 1$ над $\mathbb{R}$, и описать поле разложения $x^2 + 1$ над $\mathbb{Q}$*[17].

Определение. Пусть $F \subseteq K$, $F \subseteq L$ — расширения полей. Тогда K и L *изоморфны над* F, если существует изоморфизм абстрактных полей $\varphi\colon K \to L$: $\varphi(\alpha) = \alpha \ \forall \alpha \in F$.

Теорема 3. *Пусть F — поле, $f \in F[x]$, $\deg f \geqslant 1$. Тогда поле разложения f над F существует и единственно с точностью до изоморфизма над F.*

□

- $\boxed{\exists}$

  Идея состоит в следующем. Разложим f на неприводимые: $f(x) = p_1(x) \ldots p_k(x)$. Пусть α — «корень» некоторого p_i (если у p_i нет корней, то перейдём от F к $F(\alpha)$). Тогда над $F(\alpha)$ $f(x) = (x - \alpha) q_1(x) \ldots q_r(x)$, q_j неприводимы над $F(\alpha)$, и так далее.

  Теперь формализуем идею. Рассмотрим последовательность расширений $F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots$, где K_i получается из K_{i-1} присоединением корня некоторого неприводимого делителя p_j, $\deg p_j > 1$, многочлена f над K_{i-1}. Так как число неприводимых делителей f при переходе от K_{i-1} к K_i увеличивается, но при этом не превосходит $\deg f$, то в итоге мы получим поле $K_s = K$, над которым f разлагается на линейные множители. При этом $K = F(\alpha_1)(\alpha_2)\ldots(\alpha_s)$, то есть K порождается над F корнями $\alpha_1, \ldots, \alpha_s$ многочлена f. Значит, K — поле разложения f над F.

[17] Это будет $\{a + bi \mid a, b \in \mathbb{Q}\}$.

- !

Пусть $F \subseteq L$ — другое поле разложения f над F. Построим последовательность гомоморфизмов $\varphi_i\colon K_i \to L$, $i \in \{0, 1, \ldots, s\}$, такие что $\varphi_0 = \mathrm{id}$, $\varphi_i\big|_{K_{i-1}} = \varphi_{i-1}$.

Лемма 4. *Пусть $P \subseteq P(\alpha)$ — расширение поля P, полученно присоединением корня α неприводимого многочлена $h(x) = a_0 + a_1 x + \ldots + a_n x^n \in P[x]$, $\varphi\colon P \to P'$ — гомоморфизм, P' — поле. Тогда φ продолжается до гомоморфизма $\psi\colon P(\alpha) \to P'$ ровно столькими способами, сколько корней в P' у многочлена $h^\varphi(x) = \varphi(a_0) + \varphi(a_1)x + \ldots + \varphi(a_n)x^n$.*

□ Если ψ существует, то $\psi(a_0 + a_1\alpha x + \ldots + a_n\alpha^n) = \psi(a_0) + \psi(a_1)\psi(\alpha) + \ldots + \psi(a_n)\psi(\alpha)^n = \varphi(a_0) + \varphi(a_1)\psi(\alpha) + \ldots + \varphi(a_n)\psi(\alpha)^n = \psi(0) = 0$. Значит, $\psi(\alpha)$ — корень h^φ из P'.

Обратно, если β — корень h^φ в P', то формула $\psi\left(b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}\right) = \varphi(b_0) + \varphi(b_1)\beta + \ldots + \varphi(b_{n-1})\beta^{n-1}$ корректно определяет продолжение φ на поле $P(\alpha)$. ■

Итак, продолжение $\varphi_{i-1}\colon K_{i-1} \to L$ до $\varphi_i\colon K_i \to L$ возможно, так как $\widetilde{p_j} = p_j^{\varphi_{i-1}}$ делит f в $L[x]$ и f разлагается над L на линейные множители. Значит, $p_j^{\varphi_{i-1}}$ имеет корень в L. Тогда $\varphi_s\colon K = K_s \to L$ будет искомым изоморфизмом. В самом деле, φ_s инъективен (так как это гомоморфизм полей), $\varphi_s(K) \subseteq L$ содержит все корни L, а поскольку L порождается корнями, то $\varphi_s(K) = L$, то есть φ_s — биективный гомоморфизм, то есть изоморфизм.

■

Пример 14. Поле разложения $x^3 - 1$ над $\mathbb{Q}$ — это поле $\left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Q}\right\}$. Оно имеет над $\mathbb{Q}$ степень 2.

Конец лекции № 20 от 9 декабря 2013 г. (к началу)

Начало лекции № 21 от 11 декабря 2013 г.

§ 5. Конечные поля

Определение. Поле P называется *простым*, если в P нет подполей, отличных от P.

Пример 15.

1. $\mathbb{Q}$ — простое поле: если $P_1 \subseteq \mathbb{Q}$ — подполе, то $1 \in P_1 \Rightarrow \mathbb{Z} \subseteq P_1 \Rightarrow \mathbb{Q} \subseteq P_1 \subseteq \mathbb{Q} \Rightarrow P_1 = \mathbb{Q}$.
2. $\mathbb{Z}_p$, где p — простое, — простое поле: если $P_1 \subseteq \mathbb{Z}_p$, то $1 \in P_1 \Rightarrow \mathbb{Z}_p \subseteq P_1 \subseteq \mathbb{Z}_p \Rightarrow P_1 = \mathbb{Z}_p$.

Предложение 7. *Пусть F — поле. Тогда в F существует и единственно простое подполе P, и если $\mathrm{char}\, F = 0$, то $P \cong \mathbb{Q}$, а если $\mathrm{char}\, F = p$, то $P \cong \mathbb{Z}_p$.*

□ Пусть P — подполе в F. Тогда $1 \in P$.

Если $\mathrm{char}\, F = 0$, то $\langle 1\rangle \cong \mathbb{Z}_p \subseteq P$ — подкольцо $\Rightarrow$ поле частных $P\mathbb{Z} \cong \mathbb{Q} \subseteq P$ — подполе. Если P — простое, то $P \cong \mathbb{Q}$, и это подполе лежит в любом другом подполе $\Rightarrow P$ — единственное простое подполе.

Если $\mathrm{char}\, F = p$, то $\langle 1\rangle \cong \mathbb{Z}_p \subseteq P$ — подполе. Если P — простое, то $P \cong \mathbb{Z}_p$, и оно единственно. ■

Замечание. $\underbrace{(1 + \ldots + 1)}_{k}\underbrace{(1 + \ldots + 1)}_{l} = \underbrace{1 + \ldots + 1}_{kl}$; $\underbrace{1 + \ldots + 1}_{p} = 0$.

Предложение 8. *Пусть F — конечное поле, $P \subseteq F$ — подполе. Тогда $|F| = |P|^n$, где $n = [F : P]$.*

□ F конечно $\Rightarrow F$ — конечномерное векторное пространство над $P \Rightarrow \dim_P F = n$. Пусть $\{f_1, \ldots, f_n\}$ — базис F над P. Тогда $\forall a \in F\ \exists!\ \alpha_1, \ldots, \alpha_n \in P$: $a = \alpha_1 f_1 + \ldots + \alpha_n f_n \Rightarrow |F| = |P|^n$. ■

Предложение 9. *Конечное поле F имеет порядок p^n, где p — простое, $n \in \mathbb{N}$.*

□ F конечно $\Rightarrow \mathrm{char}\, F = p$, p — простое $\Rightarrow$ по предложению 7, $\mathbb{Z}_p \subseteq F \Rightarrow$ по предложению 8, $|F| = |\mathbb{Z}_p|^n = p^n$, где $n = [F : \mathbb{Z}_p]$. ■

Определение. Пусть F — произвольное поле, $\mathrm{char}\, F = p$. Тогда рассмотрим отображение $\varphi\colon F \to F$, $x \mapsto x^p$. Очевидно, что $\varphi(xy) = \varphi(x)\varphi(y)$. Как ни странно, также $\varphi(x + y) = \varphi(x) + \varphi(y)$. В самом деле, $(x + y)^p = \sum\limits_{k=0}^{p} C_p^k x^{p-k} y^k = x^p + y^p$, так как $p \,\big|\, C_p^k = \frac{p!}{k!(p-k)!}$ $\forall k \in \{1, \ldots, p-1\}$. Поэтому φ — эндоморфизм, то есть гомоморфизм поля F в себя. Он называется *эндоморфизмом Фробениуса*. Всегда $\mathrm{Ker}\,\varphi = \{0\}$, поэтому если F конечно, то φ инъективен, то есть биективен, что делает его *автоморфизмом Фробениуса*.

Если $\varphi\colon F \to F$, то его неподвижные точки $F^{\varphi} = \{a \in F \mid \varphi(a) = a\}$ образуют подполе в F.

Теорема 4. *Для любого простого p и натурального n поле из p^n элементов существует и единственно. Такие поля обозначают $\mathbb{F}_{p^n}$ или $\mathbb{F}_q$, где $q = p^n$, и называют полями Галуа. Например, $\mathbb{F}_p = \mathbb{Z}_p$.*

□

- $\boxed{!}$

  Пусть F — поле из $q = p^n$ элементов. Мультипликативная группа $F^{\times} = F \setminus \{0\}$ имеет порядок $q-1$. Тогда, по теореме 2 Лагранжа, $a^{q-1} = 1 \ \forall a \in F^{\times} \Rightarrow a^q = a \ \forall a \in F \Rightarrow$ все элементы F являются корнями многочлена $x^q - x \Rightarrow F$ — поле разложения $x^q - x$ над $\mathbb{Z}_p \Rightarrow$ по теореме 3, все такие поля изоморфны над $\mathbb{Z}_p$, а значит, и просто изоморфны.

- $\boxed{\exists}$

  Пусть F — поле разложения $x^q - x$ над $\mathbb{Z}_p$. Если $f(x) = x^q - x$, то $f'(x) = -1 \Rightarrow f$ не имеет кратных корней $\Rightarrow$ у f в поле F ровно q различных корней. Эти корни — неподвижные точки автоморфизма $\varphi^n\colon F \to F$, где φ — автоморфизм Фробениуса, $x \xmapsto{\varphi^n} x^{p^n} = x^q$. Значит, они образуют подполе, которое совпадает с F, по определению поля разложения $\Rightarrow |F| = q$.

■

Следствие. Для любого простого p и натурального n существует неприводимый многочлен степени n над $\mathbb{Z}_p$.

□ Мультипликативная группа $\mathbb{F}_{p^n}^{\times}$ — циклическая. Пусть α — её порождающий. Тогда $\mathbb{Z}_p \subseteq \mathbb{Z}_p(\alpha) \subseteq \mathbb{F}_{p^n}$. Но $\mathbb{F}_{p^n} = \{0\} \cup \{\alpha^k \mid k \in \{0, 1, \ldots, p^n - 2\}\} \Rightarrow \mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$. С другой стороны, $\mathbb{Z}_p(\alpha) \cong {}^{\mathbb{Z}_p[x]}\!/_{(\mu_\alpha)}$, и степень $\mathbb{Z}_p(\alpha)$ над $\mathbb{Z}_p$ равна $\deg \mu_\alpha$. Но степень $\mathbb{F}_{p^n}$ над $\mathbb{Z}_p$ равна $n \Rightarrow n = \deg \mu_\alpha \Rightarrow \mu_\alpha$ — неприводимый многочлен степени n над $\mathbb{Z}_p$. ■

Пример 16. Построим поле из четырёх элементов. Пользуясь вышеизложенной конструкцией, его можно построить как ${}^{\mathbb{Z}_2[x]}\!/_{(x^2+x+1)} = \{\overline{0}, \overline{1}, \overline{x}, \overline{x}+\overline{1}\}$, $\overline{x} = x + I = x + (x^2 + x + 1)$; например, $\overline{x}^2 = \overline{x} + \overline{1}$.

Теорема 5. *Каждое подполе в $\mathbb{F}_{p^n}$ изоморфно $\mathbb{F}_{p^d}$, где $d \mid n$, и $\forall d \mid n$ такое подполе существует и единственно.*

□ Если $F \subseteq \mathbb{F}_{p^n}$ — подполе, то $\mathbb{Z}_p \subseteq F \subseteq \mathbb{F}_{p^n} \Rightarrow |F| = p^d$, по предложению 9. Тогда $|\mathbb{F}_{p^n}| = p^n = |F|^s$, где $s = [\mathbb{F}_{p^n} : F]$, по предложению 8. Значит, $p^n = (p^d)^s = p^{ds} \Rightarrow d \mid n$.

Далее, если $d \mid n$, то $p^n - 1 = (p^d)^s - 1^s = (p^d - 1)k \Rightarrow x^{p^n-1} - 1 = \left(x^{p^d-1}\right)^k - 1^k = \left(x^{p^d-1} - 1\right) g(x) \Rightarrow$
$\Rightarrow x^{p^n} - x = \left(x^{p^d} - x\right) g(x) \Rightarrow$ поле разложения $x^{p^d} - x$ над $\mathbb{Z}_p$ лежит в поле разложения $x^{p^n} - x$ над $\mathbb{Z}_p \Rightarrow$
$\Rightarrow \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$. Поскольку все элементы поля из p^d элементов удовлетворяют уравнению $x^{p^d} - x = 0$, такое подполе единственно. ■

Задача 7. *Доказать, что $\mathrm{Aut}(\mathbb{F}_{p^n}) = \langle\varphi\rangle$, где φ — автоморфизм Фробениуса.*

Задача 8. *Доказать, что $\mathrm{Aut}(\mathbb{R}) = \{e\}$.*

§ 6. Алгебры с делением. Теорема Фробениуса

Определение. *Телом* называется кольцо[18], в котором все ненулевые элементы обратимы. Другими словами, коммутативное тело — это поле.

Определение. *Алгеброй с делением* называется алгебра над поле F, являющаяся телом.

Задача 9. *Доказать, что конечномерная алгебра является алгеброй с делением $\Leftrightarrow$ в ней нет делителей нуля.*

Пример 17. $\mathbb{H} = \{x + iy + jz + ku \mid x, y, z, u \in \mathbb{R}\}$, где $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$, — *алгебра кватернионов*[19]. Пусть $q = x + iy + jz + ku$ — кватернион. Тогда *сопряжённый к q* $\overline{q} = x - iy - jz - ku$. Проверяется, что:

1. $\overline{q_1 q_2} = \overline{q_1} \cdot \overline{q_2}$;
2. $q\overline{q} = \overline{q}q = x^2 + y^2 + z^2 + u^2 \overset{\text{def}}{=} N(q)$ — *норма кватерниона.*

[18] Рассматриваем только ассоциативные кольца с делением.

[19] Кватернионы были открыты сэром Уильямом Гамильтоном в 1843 году.

Отсюда $\forall q \neq 0 \, \exists q^{-1} = \frac{\overline{q}}{N(q)}$. Значит, алгебра кватернионов — алгебра с делением.

Задача 10. *Доказать, что уравнение $x^2 + 1 = 0$ имеет над $\mathbb{H}$ бесконечно много решений.*

Замечание. $\mathbb{C} \subseteq \mathbb{H}$, но $\mathbb{H}$ не является алгеброй над $\mathbb{C}$, так как i и j не коммутируют.

Замечание. Матричная реализация: легко проверить, что $\mathbb{H} \cong \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\} \subseteq \mathrm{Mat}_2(\mathbb{C})$, $x + iy + jz + ku \leftrightarrow \begin{pmatrix} x + iy & z + iu \\ -z + iu & x - iy \end{pmatrix}$. Эту реализацию можно записать через базисные элементы:

$$1 \leftrightarrow E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \leftrightarrow I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j \leftrightarrow J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k \leftrightarrow K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Ассоциативность умножения матриц нам уже известна, и для доказательства изоморфности остаётся решить следующую задачу.

Конец лекции № 21 от 11 декабря 2013 г. *(к началу)*

Начало лекции № 22 от 16 декабря 2013 г.

Задача 11. *Доказать, что соотношения между E, I, J и K такие же, как и между 1, i, j и k.*

Замечание. Пусть A — алгебра (ассоциативная с единицей) над полем F. Тогда $F \cong F \cdot 1 \subseteq A$, где $1 \in A$; $\lambda \leftrightarrow \lambda \cdot 1$. Значит, можно считать, что $F \subseteq A$ и даже $F \subseteq Z(A)$, где $Z(A) \stackrel{\text{def}}{=} \{a \in A \mid ax = xa \, \forall x \in A\}$ — *центр алгебры A*.

□ $(\lambda \cdot 1) \cdot a = \lambda \cdot (1 \cdot a) = \lambda \cdot (a \cdot 1) = a \cdot (\lambda \cdot 1)$. ■

Определение. Пусть A — F-алгебра. Тогда элемент $\alpha \in A$ называется *алгебраическим*, если $\exists f \in F[x]$: $f \neq 0$, $f(\alpha) = 0$. В противном случае α называется *трансцендентным*.

Предложение 10. *Пусть A — F-алгебра, $\dim_F A < +\infty$. Тогда все элементы алгебры — алгебраические.*

□ Пусть $\dim_F A = n$, $\alpha \in A$. Тогда $1, \alpha, \alpha^2, \ldots, \alpha^n$ — $n+1$ векторов в n-мерном линейном пространстве $\Rightarrow$ они линейно зависимы $\Rightarrow$ существует линейная комбинация $c_0 + c_1\alpha + \ldots + c_n\alpha^n = 0$, $c_i \in F$. Тогда многочлен $f(x) = c_0 + c_1 x + \ldots + c_n x^n$ и есть искомый аннулирующий многочлен. ■

Определение. *Минимальным многочленом* алгебраического элемента α F-алгебры A называется многочлен $\mu_\alpha \in F[x]$ наименьшей степени с единичным старшим членом, такой что $\mu_\alpha(\alpha) = 0$.

Лемма 5.

1. *Для данного алгебраического элемента минимальный многочлен существует и единственен.*
2. $\forall f \in F[x] \; f(\alpha) = 0 \Leftrightarrow \mu_\alpha \mid h$.

Доказательства обоих фактов повторяют доказательства аналогичных фактов для расширений полей.

Предложение 11. *В алгебре с делением минимальный многочлен любого алгебраического элемента неприводим.*

□ Опять же, доказательство такое же, как и для расширений полей, но мы его приведём. Пусть $\mu_\alpha = fg$, $\deg f, \deg g < \deg \mu_\alpha$. Тогда $\mu_\alpha(\alpha) = f(\alpha) g(\alpha) = 0$, при этом $f(\alpha) \neq 0$, $g(\alpha) \neq 0$. Но в алгебре с делением не может быть делителей нуля, что, в силу возникающего противоречия, означает неприводимость μ_α. ■

Предложение 12. *Любая конечномерная алгебра с делением A над алгебраически замкнутым полем F (например, над $\mathbb{C}$) изоморфна F.*

□ $\forall \alpha \in A$ μ_α неприводим, по предложению 11. Но над алгебраически замкнутым полем все неприводимые многочлены имеют первую степень $\Rightarrow \mu_\alpha(x) = x - \lambda \Rightarrow \alpha = \lambda \cdot 1 \Rightarrow A = F \cdot 1 \cong F$. ■

Теорема 6 (Фробениуса). *Любая конечномерная $\mathbb{R}$-алгебра с делением изоморфна либо $\mathbb{R}$, либо $\mathbb{C}$, либо $\mathbb{H}$.*

□

1. Пусть A — конечномерная $\mathbb{R}$-алгебра с делением. Если $A = \mathbb{R}$, то всё доказано. Иначе возьмём $a \in A \setminus \mathbb{R}$. Тогда $\mu_a(x) = x^2 + \alpha x + \beta$, причём, поскольку он, по предложению 11, неприводим, то у него нет действительных корней, то есть $\alpha^2 - 4\beta < 0$. Подставляем a: $a^2 + \alpha a + \beta = 0 \Rightarrow \left(a + \frac{\alpha}{2}\right)^2 + \left(\beta - \frac{\alpha^2}{4}\right) = 0$. Обозначив $b \stackrel{\text{def}}{=} a + \frac{\alpha}{2}$, $\delta \stackrel{\text{def}}{=} \beta - \frac{\alpha^2}{4}$, получаем $b^2 + \delta = 0$, где $\delta > 0$.

   Рассмотрим $i \stackrel{\text{def}}{=} \frac{b}{\sqrt{\delta}} \Rightarrow i^2 + 1 = 0 \Rightarrow i^2 = -1 \Rightarrow \langle 1, i \rangle_{\mathbb{R}} \subseteq A$ — подалгебра в A, изоморфная $\mathbb{C}$. Итак, можно считать, что $\mathbb{C} \subseteq A$.

   Однако A — не обязательно $\mathbb{C}$-алгебра, так как A и $\mathbb{C}$, вообще говоря, не коммутируют.

2. Если $A = \mathbb{C}$, то всё доказано. Иначе рассмотрим A как векторное пространство над $\mathbb{C}$, где комплексные скаляры умножаются на векторы слева (то есть умножение задаётся как $\mathbb{C} \times A \to A$, $(\lambda, a) \mapsto \lambda \cdot a$).

   Пусть $\mathcal{I}\colon A \to A$ — комплексный линейный оператор, $\mathcal{I}a = a \cdot i$. Тогда $\mathcal{I}^2 = -\mathcal{E}$, где $\mathcal{E}$ — тождественный оператор. Значит, $\mathcal{I}^4 = \mathcal{E} \Rightarrow \mathcal{I}$ как оператор конечного порядка диагонализируем, что известно из курса линейной алгебры, и его собственные значения $\pm i$. Значит, всё пространство A распадается в прямую сумму двух собственных подпространств: $A = A_+ \oplus A_-$, где $A_\pm$ — подпространство векторов с собственным значением $\pm i$, то есть $\forall\, a \in A_+\ \mathcal{I}a = a \cdot i = i \cdot a$, $\forall\, b \in A_-\ \mathcal{I}b = b \cdot i = -i \cdot b$.

   Лемма 6. *$A_+ \cdot A_+ \subseteq A_+$, $A_+ \cdot A_- \subseteq A_-$, $A_- \cdot A_+ \subseteq A_-$, $A_- \cdot A_- \subseteq A_+$. В этом случае говорят, что на A задана градуировка по модулю 2.*

   □ Пусть $a \in A_+$, $b \in A_-$. Тогда $(ab)\, i = a\,(bi) = a\,(-ib) = -a\,(ib) = -\,(ai)\, b = -\,(ia)\, b = -i\,(ab) \Rightarrow$ $\Rightarrow ab \in A_-$. Аналогично доказываются остальные включения. ■

   Лемма 7. *A_+ — тело.*

   □ То, что A_+ — подалгебра, доказывается в лемме 6.

   $\forall\, a \in A_+\colon a \neq 0\ \exists\, a^{-1} = b \in A \Rightarrow b = b_+ + b_-$, где $b_+ \in A_+$, $b_- \in A_-$ $\Rightarrow A_+ \ni 1 = ab = \underbrace{ab_+}_{\in A_+} + \underbrace{ab_-}_{A_-} \Rightarrow$

   $\Rightarrow \begin{cases} ab_+ = 1, \\ ab_- = 0 \end{cases}$ $\Rightarrow b_- = 0$, так как в алгебре нет делителей нуля $\Rightarrow b = b_+ \in A_+$. ■

   Следствие. $A_+ = \mathbb{C}$.

   □ A_+ — конечномерная алгебра с делением над $\mathbb{C}$. ■

3. Если $A_- = \{0\}$, то $A = A_+ = \mathbb{C}$. Иначе возьмём $a \in A \setminus \{0\} \Rightarrow \mu_a(x) = x^2 + \alpha x + \beta$, $\alpha^2 - 4\beta < 0 \Rightarrow$

   $\Rightarrow \underbrace{a^2}_{\in A_+} + \underbrace{\alpha a}_{A_-} + \underbrace{\beta}_{\in \mathbb{C} = A_+} = 0 \Rightarrow \begin{cases} a^2 + \beta = 0, \\ \alpha a = 0 \end{cases} \Rightarrow \begin{cases} \alpha = 0, \\ \beta > 0 \end{cases} \Rightarrow a^2 + \beta = 0.$

   Рассмотрим $j = \frac{b}{\sqrt{\beta}}$: $j^2 + 1 = 0 \Rightarrow j^2 = -1$.

   Лемма 8. *$A_- = \mathbb{C} \cdot j$.*

   □ Проиллюстрируем:

   $$A_+ \underset{\cdot j}{\overset{\cdot j}{\rightleftarrows}} A_-,$$

   то есть $A_- \cdot j \subseteq A_+ = \mathbb{C} \Rightarrow A_- \cdot j^2 = A_- \subseteq A_+ \cdot j = \mathbb{C} \cdot j \subseteq A_-$. ■

   $A = A_+ \oplus A_-$, $A_+ = \langle 1, i \rangle_{\mathbb{R}}$, $A_- = \left\langle j, ij \overset{\text{def}}{=} k \right\rangle_{\mathbb{R}}$. Значит, $A = \langle 1, i, j, k \rangle_{\mathbb{R}}$, $i^2 = j^2 = -1$, $ij = -ji = k$. Остальные соотношения между кватернионными единицами выводятся из этих; например, $k^2 = (ij)^2 = ijij = -iijj = -\,(-1) \cdot (-1) = -1$. Итак, $A \cong \mathbb{H}$.

   ■

Задача 12. *Вывести оставшиеся соотношения.*

Теорема 7 (Веддерберна). *Всякая конечномерная алгебра с делением над конечным полем (то есть конечное тело) является полем*[20].

Конец лекции № 22 от 16 декабря 2013 г. (к началу)

[20] Теорема приводится без доказательства.