МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

АЛГЕБРА-3. СЕМИНАРЫ

ТРЕПАЛИН
АНДРЕЙ СЕРГЕЕВИЧ

МЕХМАТ МГУ

КОНСПЕКТ ПОДГОТОВЛЕН СТУДЕНТАМИ, НЕ ПРОХОДИЛ ПРОФ. РЕДАКТУРУ И МОЖЕТ СОДЕРЖАТЬ ОШИБКИ. СЛЕДИТЕ ЗА ОБНОВЛЕНИЯМИ НА VK.COM/TEACHINMSU.

ЕСЛИ ВЫ ОБНАРУЖИЛИ ОШИБКИ ИЛИ ОПЕЧАТКИ, ТО СООБЩИТЕ ОБ ЭТОМ, НАПИСАВ СООБЩЕСТВУ VK.COM/TEACHINMSU.

Оглавление

Семинар 1. Группы. Введение.

В этом семестре мы в основном будем заниматься изучением групп.

Определение. Группа - множество G с операцией " $\cdot$ ": $G \times G \to G$ со свойствами:

- 1) ассоциативность: $(ab)c = a(bc) \quad \forall a, b, c \in G$
- 2) существование нейтрального элемента: $\exists 1 \in G\colon\ \forall g \in G\colon\ \ g \cdot 1 = 1 \cdot g = g$
- 3) существование обратного элемента: $\forall g \in G\ \ \exists g^{-1} \in G\colon\ gg^{-1} = g^{-1}g = 1$

Если к тому же выполнено условие 4, то группа называется коммутативной (абелевой):

- 4) коммутативность: $ab = ba \quad \forall a, b \in G$

Замечание: в общем случае мы будем называть операцию в группе умножением (мультипликативная терминология), но нередко операцию в группе называют не умножением, а сложением (аддитивная терминология – используется только для абелевых групп).

Примеры групп:

1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$; операция – сложение.

2) $\mathbb{Q}\backslash\{0\}, \mathbb{R}\backslash\{0\}, \mathbb{C}\backslash\{0\}$; операция – умножение.

3) Матричные группы

- Полная матричная группа (т.е. группа, состоящая из всех невырожденных матриц над $\mathbb{R}$):

$$GL_n(\mathbb{R}) = \{A \in Mat_n(\mathbb{R}) \mid \det A \neq 0\}$$

Существует множество широко изучающихся подгрупп $GL_n(\mathbb{R})$, укажем некоторые из них.

- Специальная линейная группа (группа, состоящая из матриц с определителем 1):

$$SL_n(\mathbb{R}) = \{A \in Mat_n(\mathbb{R}) \mid \det A = 1\}$$

- Ортогональная группа (состоит из всех ортогональных матриц данного размера):

$$O_n(\mathbb{R}) = \{A \in Mat_n(\mathbb{R}) \mid A \cdot A^T = E\}$$

- Специальная ортогональная группа (состоит из ортогональных матриц с определителем 1):

$$SO_n(\mathbb{R}) = O_n(\mathbb{R}) \cap SL_n(\mathbb{R})$$

4) Конечные группы

- Группа вычетов:

$$\mathbb{Z}/n\mathbb{Z} \text{ - циклическая группа, } ord(\mathbb{Z}/n\mathbb{Z}) = n$$

- Группа подстановок:

$$S_n \text{ – симметрическая группа, } ord(S_n) = n!.$$

В S_n заслуживает внимания подгруппа четных постановок A_n (знакопеременная группа):

- Группа четных подстановок:

$$A_n = \{\sigma \in S_n, \sigma \ - \text{ четная}\}, ord(A_n) = n!/2$$

- Группа диэдра:

$$D_n \text{ - группа движений правильного } n\text{-угольника, } ord(D_n) = 2n$$

Подгруппа.

Определение. Подгруппа в группе G – это подмножество $H \subseteq G$, удовлетворяющее условиям:

- 1) замкнутость относительно умножения: $g, h \in H \Rightarrow g \cdot h \in H$
- 2) содержит нейтральный элемент: $1 \in H$
- 3) замкнутость относительно взятия обратного элемента: $g \in H \Rightarrow g^{-1} \in H$

Пример подгруппы:

$$\mathbb{Z}/n\mathbb{Z} \supset \mathbb{Z}/d\mathbb{Z}, \ \ d|n$$

Утверждение (теорема Лагранжа). Пусть $H \subseteq G$, тогда $ord(G) \vdots ord(H)$.

Доказательство.
Для доказательства этого утверждения введем понятие смежного класса. Смежный класс (левый) – это множество $gH = \{gh \,|h \in H\}$. Несложно заметить, что если g_1H и g_2H – смежные классы, то либо $g_1H = g_2H$, либо $g_1H \cap g_2H = \emptyset$. Таким образом, группа G разбивается на непересекающиеся смежные классы, в каждом из которых одинаковое количество элементов ($ord(H)$), поэтому $ord(G) \vdots ord(H)$. ■

Следствие. Порядок элемента делит порядок группы.

В качестве примера посмотрим, как устроены подгруппы в D_n. Поворот на угол $\frac{2\pi}{n}$ будем обозначать r, а симметрию будем обозначать s. D_n можно задать образующими r, s и

определяющими соотношениями: $D_n = < r, s \mid r^n = s^2 = 1,\ \ srs = r^{-1} >$. Легко видеть, что этим же определяющим соотношениям будут удовлетворять все группы вида $D_{n/k}$, где k - делитель n.

Упражнение. Бывают ли в S_n элементы порядка больше n ?

Решение.
Да, например, порядок элемента $(123)(45) \subset S_5$ равен 6. Вообще, порядок любого элемента S_n равен НОК длин всех циклов, в произведение которых разлагается этот элемент. ■

Отметим, что $S_2 \cong \mathbb{Z}/2\mathbb{Z}$, $S_3 \cong D_3$. Поищем подгруппы в S_4. Пусть T – правильный тетраэдр. Отметим, что его группа изометрий совпадает с S_4: $Sym\ (T) \cong S_4$ (см. рис. 1.1), но это полезное соображение не сильно приближает нас к нахождению всех подгрупп в S_4.

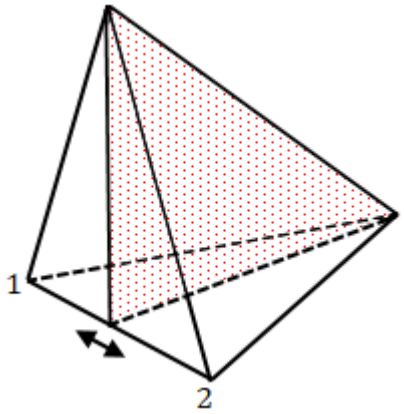

Рис. 1.1. $Sym\ (T) \cong S_4$

Порядок группы S_4 равен 24. Так как порядок подгруппы делит порядок группы, то порядок подгруппы в S_4 (отличной от самой S_4) может быть равен 1,2,3,4,6,8,12. Получаем следующие варианты:

- Подгруппа порядка 1 единственна (состоит из единичного элемента).
- Подгруппы порядка 2 и 3 – циклические (так как порядок элемента делит порядок группы, то каждый элемент в таких подгруппах либо единичный, либо имеет порядок 2 и 3 соответственно, т.е. порождает всю подгруппу).
- Подгруппы порядка 4 – это циклическая группа, содержащая перестановку (1234), а также не циклические группы (1,(12),(34),(1234)) и $(1, (12)(34), (13)(24), (14)(23))$.
- Подгруппы порядка 6 – это группы, изоморфные S_3, действующие на произвольных трех номерах набора 1234.

- Подгруппы порядка 8 – это группы симметрий квадрата (например, $< (1234), (12)(34) >$).
- Подгруппа порядка 12 – это подгруппа четных подстановок A_4.

Гомоморфизм групп.

Определение. Отображение $f: G \to H$ – гомоморфизм групп G и H, если $\forall g_1, g_2 \in G$ выполнено:

$$f(g_1 g_2) = f(g_1) f(g_2)$$

Определение. Пусть $f: G \to H$ – гомоморфизм групп. Тогда:

- $Im\, f = \{h = f(g) \mid g \in G\}$ – образ f
- $Ker\, f = \{g \in G \mid f(g) = 1\}$ – ядро f

Отметим, что $Im\, f$ – подгруппа в H, $Ker\, f$ – подгруппа в G. Например, рассмотрим гомоморфизм групп:

$$\mathbb{R}^+ \to \mathbb{C}^*$$
$$x \mapsto e^{2\pi i x}$$

Его образ – единичная окружность в $\mathbb{C}$ (т.е. все комплексные числа, по модулю равные единице), а ядро – $\mathbb{Z}$ (т.е. все целые числа). Этот гомоморфизм можно геометрически представить так: мы как бы наматываем положительный луч на единичную окружность в комплексной плоскости, причем каждый отрезок длины 1 полностью наматывается на окружность без перекрытий:

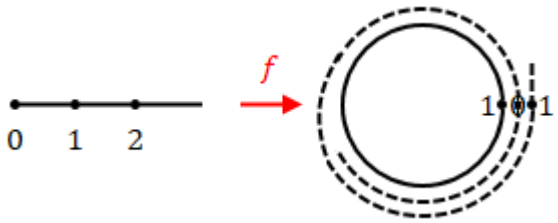

Рис. 1.2. Гомоморфизм $f(x) = e^{2\pi i x}$

Определение. Если $Ker\, f = 1$, то гомоморфизм называется мономорфизмом (вложением). Если $Im\, f = H$, то гомоморфизм называется эпиморфизмом. Если выполняются одновременно оба условия $Ker\, f = 1$ и $Im\, f = H$, то гомоморфизм называется изоморфизмом.

Пусть $f: G \to H$ – гомоморфизм групп, $Ker\, f = K$, $a, b \in G$. Отметим, что равенство $aK \cdot bK = abK$ не обязано выполняться (например, можно рассмотреть $G = S_3$ и $K = (12)$). Немного преобразуем: $aK \cdot bK = abK \Leftrightarrow K \cdot bK = bK \Leftrightarrow Kb = bK \Leftrightarrow K = bKb^{-1}$. Таким образом, ядро любого гомоморфизма является нормальной подгруппой.

Семинар 2. Классы сопряженности.

На прошлом семинаре мы выяснили, что ядро любого гомоморфизма является нормальной подгруппой.

Определение. Подгруппа $N \subseteq G$ называется нормальной, если $\forall g \in G$: $gNg^{-1} = N$. Обозначение: $N \lhd G$.

Более того, любая нормальная подгруппа является ядром некого гомоморфизма – по ней можно построить факторгруппу G/N (т.е. множество смежных классов с заданной на этом множестве групповой операцией).

Определение. Факторгруппа группы G по нормальной подгруппе N – это множество смежных классов G/N с операцией перемножения смежных классов как подмножеств в группе G:

$$XY = \{xy \mid x \in X, y \in Y\}$$

Проверим корректность данного определения, т.е. проверим, что в результате так определенного перемножения смежных классов получается смежный класс – пусть $A = aN, B = bN$, тогда $AB = aNbN = a(bNb^{-1})bN = abN$ – получили смежный класс элемента ab.

Остальные аксиомы группы (ассоциативность умножения смежных классов, наличие нейтрального и обратного элементов) вытекают из соответствующих аксиом в самой группе G.

Мы фактически доказали очень важную теорему о гомоморфизме (проверив, что ядро гомоморфизма – это нормальная подгруппа, и поняв, что смежные классы по ядру гомоморфизма перемножаются так же, как и соответствующие им элементы образа).

Теорема о гомоморфизме. Пусть $f: G \to H$ – гомоморфизм групп. Тогда

$$Im\, f \cong G/\, Ker\, f$$

Классы сопряженности.

Определение. Пусть $h \in G$. Его класс сопряженности – это множество всех элементов вида ghg^{-1}. Отметим, что:

- Нормальная подгруппа вместе с каждым своим элементом содержит и его класс сопряженности (следует из определения нормальной подгруппы).
- Класс сопряженности нейтрального элемента состоит только из него самого.
- В циклической группе класс сопряженности любого элемента состоит только из него самого: $ghg^{-1} = h$. Это верно и для любой абелевой группы.

Задача. Описать классы сопряженности в D_n.

Решение.
Поворот на угол $\frac{2\pi}{n}$ будем обозначать r, а симметрию будем обозначать s. Как уже упоминалось на семинаре 1, D_n можно задать образующими r, s и определяющими соотношениями:

$$D_n = < r, s \mid r^n = s^2 = 1,\ \ srs^{-1} = r^{-1} >$$

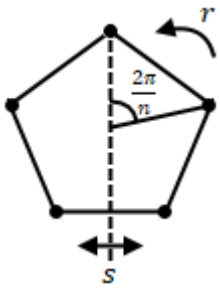

Рис. 2.1. D_n порождается r и s

Рассмотрим два случая – четного и нечетного n, но вначале выпишем соотношения, которые верны в общем случае (для любого n):

Класс сопряженности нейтрального элемента 1 состоит только из него самого: $C(1) = 1$.

Класс сопряженности поворота r^k состоит из элементов, полученных из r^k сопряжением всеми поворотами и отражениями:

$$C(r^k) = r^l r^k r^{-l} | l \in \mathbb{Z} \cup sr^l r^k (sr^l)^{-1} | l \in \mathbb{Z}$$

Но повороты коммутируют между собой: $r^l r^k r^{-l} = r^k$, а из равенства $sr^l r^k (sr^l)^{-1} = = sr^l r^k r^{-l} s^{-1} = sr^k s^{-1}$ видно, что поворот нужно сопрягать только с помощью одной симметрии s, а не всеми элементами группы D_n. Воспользуемся соотношением $rs = sr^{-1}$, получим $sr^k s^{-1} = r^{-k} s \cdot s^{-1} = r^{-k}$. Таким образом,

$$C(r^k) = r^k, sr^k s^{-1} = r^{\pm k}.$$

При $k = \frac{n}{2}$ и четном n класс сопряженности r^k состоит только из одного элемента:

$C(r^k) = r^{\frac{n}{2}}$. Таким образом, при четном n получаем еще один элемент, коммутирующий со всеми: это поворот на 180^0, он же – центральная симметрия.

Осталось сопрячь симметрии. Рассмотрим произвольное отражение sr^k. Класс сопряженности отражения sr^k состоит из элементов, полученных из sr^k сопряжением всеми поворотами и отражениями (причем удобнее произвольное отражение записать как $r^l s$):

$$C(sr^k) = \{r^l sr^k r^{-l} | l \in \mathbb{Z}\} \cup \{r^l ssr^k (r^l s)^{-1} | \, l \in \mathbb{Z}\} =$$

$$= \{sr^{-l} r^k r^{-l} | l \in \mathbb{Z}\} \cup \{r^l ssr^k r^l s \, | l \in \mathbb{Z}\} = \{sr^{-2l+k}, r^{2l+k} s \mid l \in \mathbb{Z}\} =$$

$$= \{sr^{-2l+k}, sr^{-2l-k} \mid l \in \mathbb{Z}\} = \begin{cases} \{sr^l \mid l \in \mathbb{Z}\}, & \text{если } n \text{ нечетно} \\ \{sr^{k+2l} \mid l \in \mathbb{Z}\}, & \text{если } n \text{ четно} \end{cases}$$

Таким образом, при нечетном n в $C(sr^k)$ содержатся все отражения, а при четном n все отражения делятся на два класса сопряженности. Геометрическая иллюстрация этого факта следующая: в нечетном случае все отражения сопряжены, так как они имеют один тип – это отражения относительно прямых, проходящих через вершину и середину противоположной стороны. А в четном случае есть два типа отражений – отражения относительно прямых, проходящих через середины противоположных сторон (они отличаются на четное число поворотов, так как композиция двух отражений относительно пересекающихся прямых – это поворот на удвоенный угол между прямыми) и отражения относительно прямых, проходящих через пары противоположных вершин многоугольника:

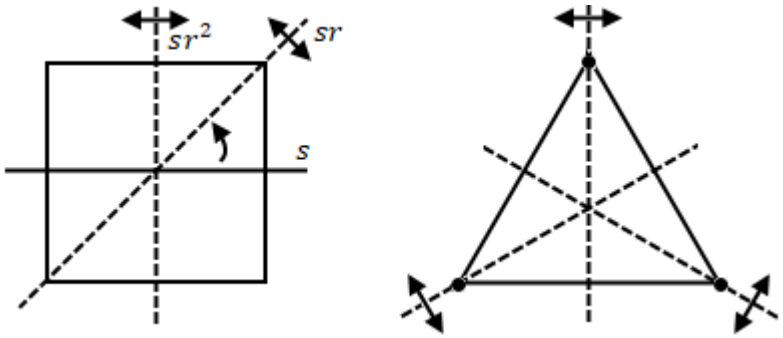

Рис. 2.2. Случаи четного и нечетного n

Эти два геометрически разных класса и являются разными классами сопряженности. Вывод: классы сопряженности в D_n устроены так:

$$n \text{ – нечетное: } \begin{cases} 1 \\ \{r^a, r^{-a}\} - \frac{n-1}{2} \text{ штук} \\ \{r^k s\}, \text{где } k - \text{любое} \end{cases}$$

$$n \text{ – четное: } \begin{cases} 1 \\ \{r^{n/2}\} \\ \{r^a, r^{-a}\} - \frac{n-2}{2} \text{ штук} \\ \{r^{2k}s\} - \frac{n}{2} \text{ штук} \\ \{r^{2k+1}s\} - \frac{n}{2} \text{ штук} \end{cases}$$

■

Классы сопряженности в S_n.

Оказывается, классы сопряженности в S_n параметризуются циклическими типами (т.е. перестановки в S_n сопряжены тогда и только тогда, когда они имеют одинаковое цикловое строение). Их количество можно посчитать с помощью диаграмм Юнга. Например, в S_4 есть пять классов сопряженности. Это $< id >$, (12), $(12)(34)$, (123), (1234).

Задача. Описать классы сопряженности в A_4.

Решение.
Заметим, что в S_4 существует три класса сопряженности, соответствующих четным перестановкам: $< id >$, $(12)(34)$, (123). Очевидно, что $< id >$ останется классом сопряженности в A_4, также и класс сопряженности, состоящий из перестановок $(12)(34)$, $(13)(24)$, $(14)(32)$ останется классом сопряженности в A_4. Остается разобраться с циклами длины 3 (их 8 штук), которые в S_4 входили в один класс сопряженности (123).

Предположим, существует перестановка g, переводящая элемент (123) в противоположный ему элемент (132): $g(123)g^{-1} = (132)$. Обратим внимание на порядки элементов в A_4: всякий неединичный элемент имеет порядок 2 или 3.

- Пусть g имеет порядок 2. Тогда $< (123), g > \cong S_3$, но S_3 не может содержаться в A_4, так как в S_3 произведение элементов порядка 2 дает элемент порядка 3, а в A_4 произведение элементов порядка 2 дает элемент порядка 2 – противоречие.
- Пусть g имеет порядок 3. Тогда с одной стороны, $g^3(123)g^{-3} = (123)$, а с другой стороны, $g^3(123)g^{-3} = (132)$ – противоречие.

Таким образом, классы сопряженности в A_4 – это $< id >$, класс сопряженности, состоящий из перестановок $(12)(34)$, $(13)(24)$, $(14)(32)$, и два класса, состоящих из циклов длины 3 (класс, содержащий (123) и класс, содержащий (132)). ■

Задача. Описать нормальные подгруппы в A_4.

Решение.
Воспользуемся следующими соображениями:

- Нормальная подгруппа вместе с каждым элементом содержит и его класс сопряженности
- Порядок подгруппы делит порядок группы

Очевидно, $< id >$ - нормальная подгруппа в A_4. Далее, как мы выяснили в предыдущей задаче, элементы (123) и (132) лежат в разных классах сопряженности. Поэтому нормальная подгруппа, содержащая (123), содержит и (132) (это взаимно обратные элементы), а значит, содержит и классы сопряженности этих элементов. Потому эта нормальная подгруппа содержит все элементы порядка 3 (их 8 штук). Но это невозможно, так как $|A_4| = 12$ (порядок подгруппы должен делить порядок группы).

Остается проверить класс сопряженности, состоящий из перестановок $(12)(34)$, $(13)(24)$, $(14)(32)$. Если мы добавим к этому классу сопряженности нейтральный элемент id, то как раз получим нормальную подгруппу. Напоследок заметим, что эта подгруппа будет нормальной также и в S_4. ■

Задача. Описать нормальные подгруппы в S_4.

Решение.
В предыдущей задаче мы нашли нормальную подгруппу в S_4, состоящую из перестановок id, $(12)(34)$, $(13)(24)$, $(14)(32)$. Для нахождения всех нормальных подгрупп в S_4 воспользуемся теми же соображениями, что и в предыдущей задаче.

Ранее мы отмечали, что в S_4 есть пять классов сопряженности. Это $< id >$, (12), $(12)(34)$, (123), (1234). Порядки этих классов равны соответственно $1, 6, 3, 8, 6$. Легко видеть (см. порядки классов сопряженности), что помимо нормальной подгруппы, найденной в предыдущей задаче, существует еще только одна нетривиальная нормальная подгруппа в S_4 – это A_4. ■

Прямое произведение.

Определение. Прямое произведение групп G_1 и G_2 – это множество пар $(g_1, g_2) \in G_1 \times G_2$ с операцией

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 h_1, g_2 h_2),$$

где $g_1, h_1 \in G_1$, $g_2, h_2 \in G_2$.

Напомним, что прямое произведение использовалось в теореме о структуре конечных абелевых групп:

Теорема. Любая конечная абелева группа изоморфна следующей:

$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z},$$

где $n_i \vdots n_{i+1}$.

Примеры групп малых порядков.

Приведем некоторые примеры групп малых порядков, которые нам пригодятся в дальнейшем.

Группы порядка 1:

- $< id >$

Группы порядка 2:

- $\mathbb{Z}/2\mathbb{Z}$

Группы порядка 3:

- $\mathbb{Z}/3\mathbb{Z}$

Группы порядка 4:

- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- $\mathbb{Z}/4\mathbb{Z}$

Группы порядка 5:

- $\mathbb{Z}/5\mathbb{Z}$

Группы порядка 6:

- $\mathbb{Z}/6\mathbb{Z}$
- $S_3 \cong D_3$ – неабелева

Группы порядка 7:

- $\mathbb{Z}/7\mathbb{Z}$

Группы порядка 8:

- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

- $\mathbb{Z}/8\mathbb{Z}$
- D_4 – неабелева
- Q_8 – группа кватернионов (неабелева).

Q_8 состоит из элементов $\pm 1,\ \pm i,\ \pm j,\ \pm k$. Операция умножения задана по правилам: $i^2 = j^2 = k^2 = -1,\ i \cdot j = k,\ j \cdot i = -k$.

Семинар 3. Автоморфизмы абелевых групп.

Разбор задач домашнего задания.

Задача 5. Описать все группы порядка 10.

Решение.
Пусть $|G| = 10$. Докажем, что либо $G \cong \mathbb{Z}/10\mathbb{Z}$, либо $G \cong D_5$. Если в G существует элемент a порядка 10, то $G \cong \mathbb{Z}/10\mathbb{Z}$ (так как в этом случае $G = < a >$, и G – циклическая группа порядка 10). Если в G не существует элемента порядка 10, то рассмотрим два случая:

1) $\forall a \neq 1$: $ord\ a = 2$. Докажем, что в этом случае G абелева. В самом деле, рассмотрим произвольные $a, b \in G$. Так как $ord\ (ab) = 2$, то $(ab)(ab) = 1$ – домножая это равенство справа на ba, получим $ababba = ba \Leftrightarrow abaa = ba \Leftrightarrow ab = ba$.

Далее воспользуемся теоремой о структуре конечных абелевых групп (см. семинар 2), из которой следует, что G имеет порядок 2^n – противоречие.

2) $\exists a \in G$: $ord\ a \neq 2$. Так как порядок элемента делит порядок группы, то $ord\ a = 5$, и $|< a >| = 5$. Рассмотрим элемент $b \in G$, не лежащий в $< a >$. Заметим, что $< a >$ - нормальная подгруппа в G (так как ее индекс равен 2), поэтому $bab^{-1} \in < a >$, т.е. $bab^{-1} = a^k$ для некоторого k.

Заметим, что $b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^kb^{-1} = (bab^{-1})^k = a^{k^2}$. Аналогично $b^4ab^{-4} = a^{k^4} = a$ (так как $k^4 \equiv 1\ (mod\ 5)$), т.е. элементы a и b^4 коммутируют.

Если $ord\ b = 5$, то и элементы a и b коммутируют (так как $1 = b^5 = b \cdot b^4$), и группа G абелева - противоречие. Значит, $ord\ b = 2$. В этом случае $k^2 \equiv 1\ (mod\ 5)$, откуда $k = \pm 1$. Если $k = 1$, то элементы a и b коммутируют, и группа G абелева - противоречие. Значит, $k = -1$, и тогда $bab^{-1} = a^{-1}$.

Итак, получаем $ord\ a = 5$, $ord\ b = 2$, $bab^{-1} = a^{-1}$ – определяющие соотношения для D_5. ■

Результат этой задачи можно обобщить: группа порядка $2p$, где p – простое, изоморфна либо $\mathbb{Z}/2p\mathbb{Z}$, или D_p.

Задача 1. Найти все нормальные подгруппы в D_n и факторы по ним.

Решение.
Снова воспользуемся тем, что:

- Нормальная подгруппа вместе с каждым элементом содержит и его класс сопряженности
- Порядок подгруппы делит порядок группы

Ранее мы уже описывали классы сопряженности в D_n (см. предыдущий семинар) – они устроены так:

- n – нечетное: $\begin{cases} 1 \\ \{r^a, r^{-a}\} - \frac{n-1}{2} \text{ штук} \\ \{r^k s\}, \text{где } k - \text{любое} \end{cases}$
- n – четное: $\begin{cases} 1 \\ \{r^{n/2}\} \\ \{r^a, r^{-a}\} - \frac{n-2}{2} \text{ штук} \\ \{r^{2k} s\} - \frac{n}{2} \text{ штук} \\ \{r^{2k+1} s\} - \frac{n}{2} \text{ штук} \end{cases}$

Случай 1 (n – нечетное).

Класс $\{r^k s\}$ (при любом k) не может содержаться в нормальной подгруппе (в нем “слишком много” элементов – порядок этой подгруппы не может делить порядок D_n, равный $2n$). Следовательно, в нормальной подгруппе в D_n могут быть только повороты. Нетрудно видеть, что любая подгруппа группы поворотов будет нормальной в D_n (а каждая подгруппа группы поворотов имеет вид $\{1, r^d, r^{2d}, \dots, r^{n-d}\}$, где $d \vdots n$).

Факторы по нормальным подгруппам в D_n:

$$D_n/\{1, r^d, r^{2d}, \dots, r^{n-d}\} \cong D_d$$

- факторгруппа по всякой нормальной подгруппе в D_n (при нечетном n) изоморфна D_d.

Случай 2 (n – четное).

Классы сопряженности $\{r^{2k} s\}$ и $\{r^{2k+1} s\}$ являются также и нормальными подгруппами в D_n, каждая из которых содержит $\frac{n}{2}$ элементов. Факторгруппы по этим нормальным подгруппам изоморфны $\mathbb{Z}/2\mathbb{Z}$:

$$D_n/\{r^{2k} s\} \cong \mathbb{Z}/2\mathbb{Z}$$
$$D_n/\{r^{2k+1} s\} \cong \mathbb{Z}/2\mathbb{Z}$$

Классы сопряженности $\{1\}$ и $\{r^{n/2}\}$ содержатся в нормальной подгруппе $\{1, r^{n/2}\}$, фактор по которой изоморфен $D_{n/2}$:

$$D_n/\{1, r^{n/2}\} \cong D_{n/2}$$

Осталось разобраться с $\frac{n-2}{2}$ классами сопряженности $\{r^a, r^{-a}\}$. Как и в случае нечетного n, каждый из этих классов сопряженности содержится в некоторой подгруппе группы поворотов, которая имеет вид $\{1, r^d, r^{2d}, \dots, r^{n-d}\}$, где $d \vdots n$. Каждая из таких подгрупп является нормальной, факторгруппа по этой нормальной подгруппе изоморфна D_d:

$$D_n/\{1, r^d, r^{2d}, \dots, r^{n-d}\} \cong D_d$$

■

Задача 4. Доказать, что группа D_4 не раскладывается в прямое произведение групп.

Решение.
Мы знаем, что $|D_4| = 8$. Теоретически может существовать два варианта разложения: $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ и $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, но обе эти группы абелевы, а D_4 – нет. Отсюда следует, что D_4 не является прямым произведением.

Докажем заодно, что D_8 не раскладывается в прямое произведение: $|D_8| = 16$, разложение $D_8 \cong D_4 \times \mathbb{Z}/2\mathbb{Z}$ невозможно, так как в D_8 есть элемент порядка 8, а в группе $D_4 \times \mathbb{Z}/2\mathbb{Z}$ такого элемента нет. Если бы D_8 и раскладывалась в прямое произведение, то только так: $D_8 \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (потому что в D_8 есть элемент порядка 8). Но группа $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ абелева, а D_8 – нет, поэтому D_8 не является прямым произведением.

Подобное рассуждение можно произвести для любой группы D_n, где n делится на 4. ■

Задача 3. Привести пример группы D_n, раскладывающейся в прямое произведение групп.

Решение.
При нечетном n выполнено:

$$D_{2n} \cong D_n \times \mathbb{Z}/2\mathbb{Z}$$

Действительно, D_{2n} обладает структурой внутреннего прямого произведения: D_{2n} содержит D_n в качестве нормальной подгруппы (при нечетном n), также D_{2n} содержит в качестве нормальной подгруппы группу $\{1, r^{n/2}\}$, которая изоморфна $\mathbb{Z}/2\mathbb{Z}$. Так как подгруппы D_n и $\{1, r^{n/2}\}$ пересекаются только по 1 и коммутируют друг с другом, их прямое произведение даст нам D_{2n}. ■

Абелевы группы.

Определение. Автоморфизм группы G – это изоморфизм группы на себя: $\varphi\colon\ G \twoheadrightarrow G$.

Множество всех автоморфизмов группы G (обозначение: $Aut\ G$) само является группой относительно операции композиции автоморфизмов.

Определение. Пусть $g \in G$. Внутренний автоморфизм $i_g\colon G \twoheadrightarrow G$ определяется следующим образом:

$$i_g(a) = gag^{-1}, \forall a \in G$$

Другими словами, внутренний автоморфизм, задаваемый элементом $g \in G$ – это операция сопряжения с этим элементом. Убедимся, что это действительно автоморфизм:

- биективность: $(i_g)^{-1} = i_{g^{-1}}$
- эндоморфизм: $i_g(ab) = gabg^{-1} = gag^{-1} \cdot gbg^{-1} = i_g(a) \cdot i_g(b)$

Если группа G абелева, то ее центр совпадает со всей группой и внутренних автоморфизмов нет (кроме тождественного). В общем случае группа внутренних изоморфизмов (обозначение: $Inn\ G$) изоморфна фактору группы по ее центру: $Inn\ G \cong G/Z(G)$.

Автоморфизмы абелевых групп.

Немного поговорим о том, как устроены внешние автоморфизмы абелевых групп. Начнем с циклических групп – найдем $Aut\ \mathbb{Z}$. Так как $\mathbb{Z}$ - это циклическая группа, у которой два порождающих элемента: 1 и -1, то в $Aut\ \mathbb{Z}$ всего два автоморфизма (это преобразования $x \mapsto \pm x$):

$$Aut\ \mathbb{Z} = Aut < 1 > \cong \mathbb{Z}/2\mathbb{Z}$$

Найдем $Aut\ (\mathbb{Z}/p\mathbb{Z})$. Так как $\mathbb{Z}/p\mathbb{Z}$ - это группа, у которой $\varphi(p) = p - 1$ порождающих элементов, то в $Aut\ (\mathbb{Z}/p\mathbb{Z})$ будет $p - 1$ элементов. При этом $Aut\ (\mathbb{Z}/p\mathbb{Z})$ изоморфна $\mathbb{Z}/(p-1)\mathbb{Z}$:

$$Aut\ (\mathbb{Z}/p\mathbb{Z}) \cong\ \mathbb{Z}/(p-1)\mathbb{Z}$$

Если мы рассмотрим произвольное n (не обязательно являющееся простым), то у $\mathbb{Z}/n\mathbb{Z}$ будет $\varphi(n)$ порождающих элементов, т.е. $\varphi(n)$ – порядок группы $Aut\ (\mathbb{Z}/n\mathbb{Z})$.

Пусть $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, тогда:

$$\varphi(n) = \prod_{i=1}^{k} \varphi\left(p_i^{a_i}\right) = \prod_{i=1}^{k} \varphi\left(p_i^{a_i}\right)(p_i - 1)$$

и

$$Aut\ (\mathbb{Z}/n\mathbb{Z}) \cong Aut\ (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times Aut\ (\mathbb{Z}/p_2^{a_2}\mathbb{Z}) \times \cdots \times Aut\ (\mathbb{Z}/p_k^{a_k}\mathbb{Z}),$$

где:

- если p_i нечетное, то $Aut\ (\mathbb{Z}/p_i^{a_i}\mathbb{Z}) \cong \mathbb{Z}/p_i^{a_i-1}(p_i-1)\mathbb{Z}$,
- если $p_i = 2$, то $Aut\ (\mathbb{Z}/2^{\alpha_0}\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha_0-2}\mathbb{Z})$

Задача. Выяснить, как устроена группа $Aut\ (\mathbb{Z}/8\mathbb{Z})$.

Решение.
Порядок группы $Aut\ (\mathbb{Z}/8\mathbb{Z})$ равен $\varphi(8) = 4$. Будем отождествлять группу $\mathbb{Z}/8\mathbb{Z}$ с остатками при делении на 8. Образующими этой группы будут остатки $1, 3, 5, 7$. При этом $ord\ (3) = 2$, $ord\ (5) = 2$, $ord\ (7) = 2$ – все неединичные образующие элементы имеют порядок 2. Поэтому $Aut\ (\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. ■

Задача. Выяснить, как устроена группа $Aut\ (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

Решение.
Группа $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ состоит из элементов $(0,0), (1,0), (0,1), (1,1)$. Образующими являются элементы $a = (1,0)$ и $b = (0,1)$ (оба этих элемента имеют порядок 2). При автоморфизме каждый из образующих элементов может переходить либо в a, либо в b, либо в $c = (1,1)$ – всего получаем 6 вариантов (все перестановки из трех элементов). Таким образом, $Aut\ (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$. ■

Семинар 4. Конечно порожденные абелевы группы.

Разбор задач домашнего задания.

Задача 3. Выяснить, как устроена группа $Aut\ (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

Решение.
Как и ранее, будем отождествлять группы $\mathbb{Z}/2\mathbb{Z}$ и $\mathbb{Z}/4\mathbb{Z}$ с остатками при делении на 2 и на 4 соответственно: $\mathbb{Z}/2\mathbb{Z} = \{0,1\}$ и $\mathbb{Z}/4\mathbb{Z} = \{0,1,2,3\}$. Несложно видеть, что в $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ образующими будут элементы $(1,0)$ и $(0,1)$. Они имеют порядок 4 и 2 соответственно, и могут перейти в элементы $(1,0)$, $(1,1)$, $(3,0)$, $(3,1)$ и $(0,1)$, $(2,1)$ соответственно. Отсюда следует, что $|Aut\ (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})| = 8$. Всего существует пять неизоморфных групп порядка 8:

- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- $\mathbb{Z}/8\mathbb{Z}$
- D_4
- Q_8

Обратим внимание на количество элементов порядка 2 в каждой из этих групп:

- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ - 3 элемента порядка 2
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ - 7 элементов порядка 2
- $\mathbb{Z}/8\mathbb{Z}$ - 1 элемент порядка 2
- D_4 - 5 элементов порядка 2
- Q_8 - 1 элемент порядка 2

Прямая проверка показывает, что в группе $Aut\ (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ всего 5 элементов порядка 2, откуда следует, что $Aut\ (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong D_4$. ■

Задача 4. Найти $|Aut\ (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})|$.

Решение.
В $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ образующими будут элементы $(1,0)$ и $(0,1)$. Мы можем рассматривать их как векторы над полем $\mathbb{Z}/3\mathbb{Z}$. Тогда группу $Aut\ (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$ можно отождествить с матричной группой, состоящей из матриц вида $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, где $\begin{pmatrix} a \\ c \end{pmatrix}$ – образ элемента $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} b \\ d \end{pmatrix}$ – образ элемента $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. При этом столбцы $\begin{pmatrix} a \\ c \end{pmatrix}$ и $\begin{pmatrix} b \\ d \end{pmatrix}$ должны быть ненулевыми и непропорциональными.

Столбец $\binom{a}{c}$ можно выбрать $9-1=8$ способами (подойдут все ненулевые элементы $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$), а столбец $\binom{b}{d}$ можно выбрать $9-3=6$ способами (подойдут все ненулевые элементы $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, которые непропорциональны $\binom{a}{c}$). Такая группа называется $GL_2(\mathbb{F}_3)$ и содержит $8\cdot 6=48$ элементов. ■

В общем случае

$$Aut\,((\mathbb{Z}/p\mathbb{Z})^n)\cong GL_n(\mathbb{F}_p)$$

Доказательство этого факта аналогично решению задачи 4. При этом

$$|Aut\,((\mathbb{Z}/p\mathbb{Z})^n)|=(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$$

Задача. Найти $Aut\,(\mathbb{Z}^2)$.

Решение.
Группу $\mathbb{Z}^2$ можно рассматривать как целочисленную решетку:

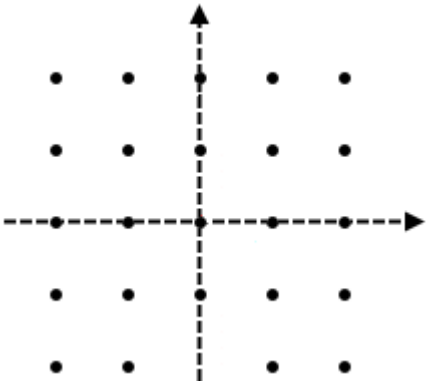

Рис. 4.1. Решетка $\mathbb{Z}^2$

Эта решетка порождена векторами $\binom{1}{0}$ и $\binom{0}{1}$, но это не единственная пара образующих. Попробуем понять, какие пары целочисленных векторов могут порождать $\mathbb{Z}^2$: пусть вектор $\binom{1}{0}$ переходит в $\binom{a}{b}$, а вектор $\binom{0}{1}$ переходит в $\binom{c}{d}$. Матрица $\begin{pmatrix}a & c\\ b & d\end{pmatrix}$ задает автоморфизм $\mathbb{Z}^2$ тогда и только тогда, когда $det\begin{pmatrix}a & c\\ b & d\end{pmatrix}=\pm 1$. Действительно, так как автоморфизмы образуют группу, у каждого автоморфизма должен существовать обратный, а это значит, что матрица, обратная к $\begin{pmatrix}a & c\\ b & d\end{pmatrix}$, также должна быть целочисленной, откуда $det\begin{pmatrix}a & c\\ b & d\end{pmatrix}=\pm 1$.

Найдем элементы конечного порядка в $Aut\,(\mathbb{Z}^2)$. Например, $\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$, $\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$ и $\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}$ – элементы порядка 2, а $\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$ – элемент порядка 4.

Попробуем найти элемент порядка 3 в $Aut\,(\mathbb{Z}^2)$. Если такая целочисленная матрица существует, то после приведения ее к жордановой форме (над полем комплексных чисел) на ее диагонали стояли бы комплексные корни третьей степени из 1, причем (так как определитель матрицы и ее след не изменились бы, т.е. остались целочисленными) произведение этих корней должно давать 1, а сумма -1. Попробуем найти целочисленную матрицу с определителем 1 и следом -1. Легко видеть, что матрица $\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}$ удовлетворяет этому условию, т.е. является элементом порядка 3 в $Aut\,(\mathbb{Z}^2)$.

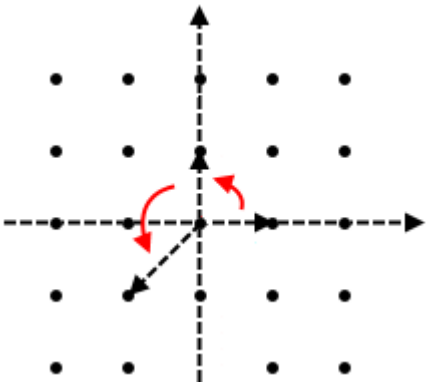

Рис. 4.2. Замена базиса в $\mathbb{Z}^2$, соответствующая автоморфизму порядка 3 в $Aut\,(\mathbb{Z}^2)$

Элемент порядка 6 найти легко – это $\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix} = \begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}$, а вот элементов конечного порядка, отличных от $1, 2, 3, 4, 6$ не существует (это следует из рассуждений, аналогичных рассуждениям, которые мы проводили для нахождения элемента порядка 3 – нельзя подобрать целочисленные матрицы с определителем ± 1, след которых также был бы целочисленным). ■

Конечно порожденные абелевы группы.

Определение. Конечно порожденная абелева группа G – это абелева группа с конечным числом порождающих, т.е. произвольный элемент группы G представляется в виде конечной целочисленной линейной комбинации порождающих элементов.

Определение. Система элементов $h_1, \dots, h_m \in G$ называется линейно зависимой, если существует целочисленная линейная комбинация элементов этой системы, равная нулю:

$$\exists l_1, \dots, l_m \in \mathbb{Z}, \exists l_i \neq 0: \quad l_1 h_1 + k_2 g_2 + \dots + l_m h_m = 0$$

Система $g_1, \dots, g_n \in G$ – базис группы G, если $G = < g_1, \dots, g_n >$ и $g_1, \dots, g_n$ линейно независима.

Определение. Абелева группа, имеющая базис, называется свободной.

Задача. Разложить в прямую сумму циклических групп факторгруппу A/B, где A – свободная абелева группа с базисом x_1, x_2, x_3, B – ее подгруппа, порожденная y_1, y_2, y_3:

$$\begin{cases} y_1 = 2x_1 \\ y_2 = 3x_2 \\ y_3 = x_3 \end{cases}$$

Решение.
Несложно видеть, что

$$A/B \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

A/B порождена образами элементов x_1, x_2, x_3. Элемент x_1 имеет порядок 2, элемент x_2 имеет порядок 3, элемент x_3 имеет порядок 1. ■

Задача. Разложить в прямую сумму циклических групп факторгруппу A/B, где A – свободная абелева группа с базисом x_1, x_2, x_3, B – ее подгруппа, порожденная y_1, y_2, y_3:

$$\begin{cases} y_1 = 3x_1 \\ y_2 = 7x_2 \\ y_3 = 0 \end{cases}$$

Решение.
Несложно видеть, что

$$A/B \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}$$

A/B порождена образами элементов x_1, x_2, x_3. Элемент x_1 имеет порядок 2, элемент x_2 имеет порядок 3, элемент x_3 имеет бесконечный порядок. ■

В разобранных выше задачах базисы x_1, x_2, x_3 и y_1, y_2, y_3 были согласованны. Разберем задачи 6 и 7 из домашнего задания, в которых базисы не согласованны.

Задача 6. Разложить в прямую сумму циклических групп факторгруппу A/B, где A – свободная абелева группа с базисом x_1, x_2, x_3, B – ее подгруппа, порожденная y_1, y_2, y_3:

$$\begin{cases} y_1 = 7x_1 + 2x_2 + 3x_3 \\ y_2 = 21x_1 + 8x_2 + 9x_3 \\ y_3 = 5x_1 - 4x_2 + 3x_3 \end{cases}$$

Решение.

Приведем матрицу преобразования целочисленными элементарными преобразованиями к диагональному виду:

$$\begin{pmatrix} 7 & 2 & 3 \\ 21 & 8 & 9 \\ 5 & -4 & 3 \end{pmatrix} \sim \begin{pmatrix} 7 & 2 & 3 \\ 0 & 2 & 0 \\ 5 & -4 & 3 \end{pmatrix} \sim \begin{pmatrix} 7 & 0 & 3 \\ 0 & 2 & 0 \\ 5 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 5 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 1 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & -6 \\ 0 & 2 & 0 \\ 1 & 0 & 3 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 0 & 0 & -6 \\ 0 & 2 & 0 \\ 1 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 3 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

Получаем

$$A/B \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$$

■

Задача 7. Разложить в прямую сумму циклических групп факторгруппу A/B, где A – свободная абелева группа с базисом x_1, x_2, x_3, B – ее подгруппа, порожденная y_1, y_2, y_3:

$$\begin{cases} y_1 = 5x_1 + 5x_2 + 2x_3 \\ y_2 = 11x_1 + 8x_2 + 5x_3 \\ y_3 = 17x_1 + 5x_2 + 8x_3 \end{cases}$$

Решение.
Приведем матрицу преобразования целочисленными элементарными преобразованиями к диагональному виду:

$$\begin{pmatrix} 5 & 5 & 2 \\ 11 & 8 & 5 \\ 17 & 5 & 8 \end{pmatrix} \sim \begin{pmatrix} 5 & 5 & 2 \\ 1 & -2 & 1 \\ 12 & 0 & 6 \end{pmatrix} \sim \begin{pmatrix} 0 & 15 & -3 \\ 1 & -2 & 1 \\ 12 & 0 & 6 \end{pmatrix} \sim \begin{pmatrix} 0 & 15 & -3 \\ 1 & 0 & 0 \\ 12 & 24 & -6 \end{pmatrix} \sim \begin{pmatrix} 0 & 3 & -3 \\ 1 & 0 & 0 \\ 0 & 0 & -6 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 0 & 3 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -6 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

Получаем

$$A/B \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$$

■

Семинар 5. Классификация конечных абелевых групп.

Разбор задач домашнего задания.

Задача. Найти элемент порядка 5 в $GL_4(\mathbb{Z})$.

Решение.
Будем действовать как на прошлом семинаре, когда мы искали элемент порядка 3 в $Aut(\mathbb{Z}^2)$. После приведения матрицы порядка 5 в $GL_4(\mathbb{Z})$ к жордановой форме (над полем комплексных чисел) мы должны получить матрицу

$$\begin{pmatrix} \omega_1 & 0 & 0 & 0 \\ 0 & \omega_2 & 0 & 0 \\ 0 & 0 & \omega_3 & 0 \\ 0 & 0 & 0 & \omega_4 \end{pmatrix}$$

где ω_i – какие-то корни степени 5 из единицы. Заметим, что у матрицы

$$\begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega^2 & 0 & 0 \\ 0 & 0 & \omega^3 & 0 \\ 0 & 0 & 0 & \omega^4 \end{pmatrix}$$

где $\omega = e^{\frac{2\pi i}{5}}$, будут подходящие целочисленные инварианты – это следует из вида ее характеристического многочлена:

$$\chi(\lambda) = \lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1$$

Итак, мы поняли, что элемент порядка 5 в $GL_4(\mathbb{Z})$ существует. Далее не составляет никакого труда догадаться, что это

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ -1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & -1 & -1 \end{pmatrix}$$

■

Отметим, что элемент порядка 5 в $GL_4(\mathbb{Z})$ можно найти не угадывая, а исходя из более строгих соображений. Во-первых, заметим, что элемент порядка 5 в $GL_5(\mathbb{Z})$ угадывается легко (просто переставляем базисные векторы по циклу), чему соответствует матрица

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Теперь рассмотрим подрешетку $x_1 + x_2 + x_3 + x_4 + x_5 = 0$ в $\mathbb{Z}^5$, которая будет изоморфна $\mathbb{Z}^4$ (так как x_5 однозначно определяется выбором x_1, x_2, x_3, x_4), также эта подрешетка будет инварианта относительно действия группы. Перестановке базисных векторов по циклу соответствует следующая цепочка: $x_1 \to x_2 \to x_3 \to x_4 \to -x_1 - x_2 - x_3 - x_4$. Теперь понятно, какой существует элемент порядка 5 в $GL_4(\mathbb{Z})$:

$$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

Аналогично выглядит элемент порядка n в $GL_{n-1}(\mathbb{Z})$.

Задача 2. Разложить в прямую сумму циклических групп факторгруппу A/B, где A – свободная абелева группа с базисом x_1, x_2, x_3, B – ее подгруппа, порожденная y_1, y_2, y_3:

$$\begin{cases} y_1 = 4x_1 + 5x_2 + x_3 \\ y_2 = 8x_1 + 9x_2 + x_3 \\ y_3 = 4x_1 + 6x_2 + 2x_3 \end{cases}$$

Решение.
Приведем матрицу преобразования целочисленными элементарными преобразованиями к диагональному виду:

$$\begin{pmatrix} 4 & 5 & 1 \\ 8 & 9 & 1 \\ 4 & 6 & 2 \end{pmatrix} \sim \begin{pmatrix} 4 & 5 & 1 \\ 0 & -1 & -1 \\ 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 4 & 4 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 4 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Получаем

$$A/B \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}$$

■

Задача. Разложить в прямую сумму циклических групп факторгруппу A/B, где A – свободная абелева группа с базисом x_1, x_2, x_3, B – ее подгруппа, порожденная y_1, y_2, y_3:

$$\begin{cases} y_1 = 6x_1 + 5x_2 + 4x_3 \\ y_2 = 7x_1 + 6x_2 + 9x_3 \\ y_3 = 5x_1 + 4x_2 - 4x_3 \end{cases}$$

Решение.
Приведем матрицу преобразования целочисленными элементарными преобразованиями к диагональному виду:

$$\begin{pmatrix} 6 & 5 & 4 \\ 7 & 6 & 9 \\ 5 & 4 & -4 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 8 \\ 2 & 2 & -13 \\ 5 & 4 & -4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 8 \\ 2 & 0 & -13 \\ 5 & -1 & -4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 8 \\ 0 & 0 & 3 \\ 5 & -1 & -4 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 8 \\ 0 & 0 & 3 \\ 5 & -1 & -4 \end{pmatrix} \sim$$
$$\sim \begin{pmatrix} 1 & 0 & 8 \\ 0 & 0 & 3 \\ 0 & -1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 3 \\ 0 & -1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

Получаем

$$A/B \cong \mathbb{Z}/3\mathbb{Z}$$

■

Покажем, почему алгоритм, примененный в задачах, приведенных выше, будет работать.

Утверждение. С помощью целочисленных элементарных преобразований строк и столбцов любую целочисленную матрицу $K \in Mat_{n\times l} \in \mathbb{Z}$ можно привести к виду

$$K^* = \begin{pmatrix} m_1 & & 0 & 0 & \dots & 0 \\ & \ddots & & \dots & \dots & \dots \\ 0 & & m_r & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \ddots & \dots \\ 0 & \dots & 0 & \dots & \dots & 0 \end{pmatrix}, m_i \in \mathbb{N}$$

Доказательство.
Будем доказывать лемму индукцией по $max\ \{n, l\}$.
База индукции: $n = l = 1$ – доказывать нечего.

Шаг индукции: $K = 0$ – доказывать нечего. Иначе (если матрица ненулевая):

- Выберем ненулевой элемент $k_{ij} \neq 0$ с самым маленьким модулем: $|k_{ij}| = min = m \in \mathbb{N}$. Далее переставим m в левый верхний угол (целочисленное преобразование 2-го типа), получим матрицу K'.
- Разделим элементы матрицы K', лежащие в первой строке или в первом столбце с остатком на m:

$$k_{i1} = p_{i1}m + k_{i1}''$$
$$k_{1j} = q_{1j}m + k_{1j}''$$

  Затем заменяем эти элементы на их остатки (вычитаем из соответствующей строки (столбца) первую строку (столбец) с подходящим коэффициентом) –

получим матрицу K'' из матрицы K' элементарными целочисленными преобразованиями строк и столбцов 1-го типа. В первом столбце и первой строке K'' стоят числа, меньшие по модулю, чем m.

- Далее: либо все ${k_{i1}}''$ и ${k_{1j}}''$ равны нулю, либо среди них есть хотя бы один ненулевой элемент. В этом случае ($\exists {k_{i1}}'' \neq 0$ или $\exists {k_{1j}}'' \neq 0$) применяем предыдущий шаг еще раз – снова выбираем элемент с самым маленьким модулем, переставляем его на позицию (1,1) и т.д. Так мы будем уменьшать наименьший модуль ненулевого элемента и рано или поздно получим матрицу K''' вида:

$$K''' = \left(\begin{array}{c|ccc} \pm m_1 & 0 & \dots & 0 \\ \hline 0 & & & \\ \dots & & \bar{K} & \\ 0 & & & \end{array}\right)$$

- Матрица $\bar{K}$ тоже целочисленная, но меньших размеров – по предположению индукции мы можем привести ее к псевдодиагональному виду целочисленными элементарными преобразованиями строк и столбцов – получим матрицу $\widetilde{K}$, которая выглядит, как показано на рис. 5.1.
- При необходимости поменяем знак у первой строки (столбца), т.е. применим целочисленное элементарное преобразование 3-го типа и получим матрицу K^* нужного вида. ■

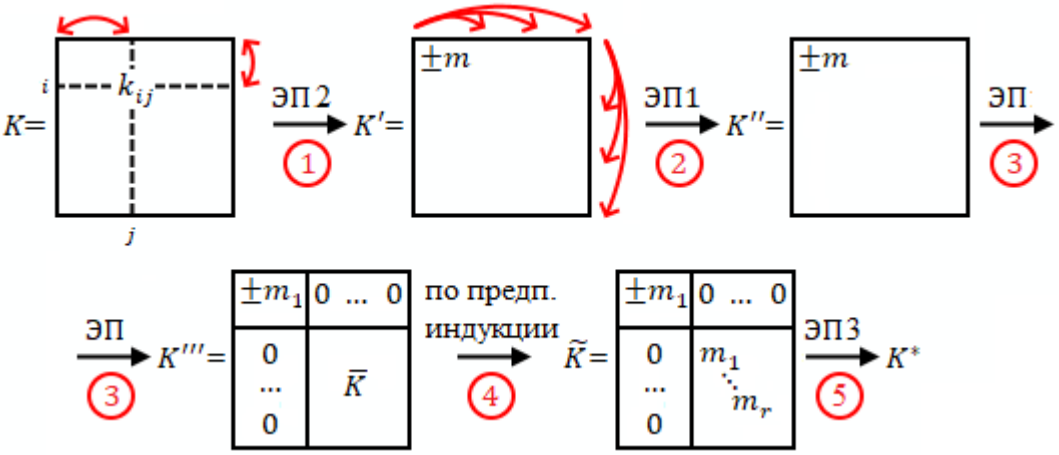

Рис. 5.1. Преобразования, приводящие K к K^*

Задача 5. Описать все конечные абелевы группы порядка 16, 24 и 36.

Решение.
Воспользуемся теоремой о структуре конечно порожденных абелевы групп.

а) $16 = 2^4$. Возможны 5 вариантов:

- $\mathbb{Z}/16\mathbb{Z}$
- $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
- $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$
- $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
- $(\mathbb{Z}/2\mathbb{Z})^4$

б) $24 = 2^3 \cdot 3$. Группы, отвечающие множителю 2^3 – это $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$. Группа, отвечающая множителю 3 – это $\mathbb{Z}/3\mathbb{Z}$. Значит, всего абелевых групп порядка 24 будет 3:

- $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$
- $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
- $\mathbb{Z}/3\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^3$

в) $36 = 2^2 \cdot 3^2$. Группы, отвечающие множителю 2^2 – это $\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$. Группа, отвечающая множителю 3^2 – это $\mathbb{Z}/9\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z})^2$. Значит, всего абелевых групп порядка 36 будет 4:

- $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$
- $\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^2$
- $(\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/9\mathbb{Z}$
- $(\mathbb{Z}/2\mathbb{Z})^2 \oplus (\mathbb{Z}/3\mathbb{Z})^2$

■

Итак, мы видим, что классификация конечных абелевых групп сводится к классификации примарных абелевых групп (т.е. групп, порядок которых – это степень некоторого простого числа). Обсудим, как найти количество групп порядка p^k, где p – простое. Всего групп порядка p^k, где p – простое, будет столько же, сколько существует способов разбить число k на натуральные слагаемые. Разбиения также можно изображать диаграммами Юнга:

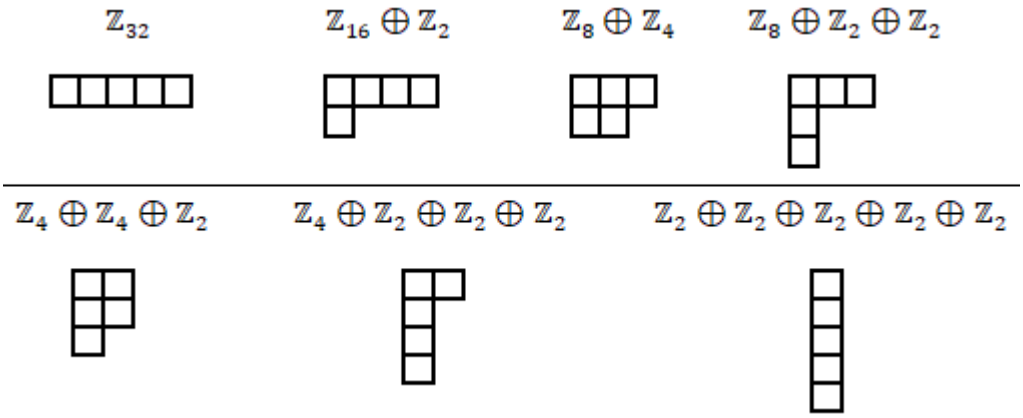

Рис. 5.2. Диаграммы Юнга, соответствующие разбиениям 5

Число разбиений $p(n)$ – это очень важный математический объект, такими диаграммами также кодируется, например, цикловое строение подстановок, и много других математических объектов.

Итак, если A – абелева группа, ее порядок равен $|A| = p_1^{k_1} \cdots p_n^{k_n}$, то групп такого порядка (с точностью до изоморфизма) $p(k_1) \cdots p(k_n)$ штук.

Задача 6. Пусть A и B – конечные абелевы группы Докажите, что все гомоморфизмы из A в B образуют группу (обозначение: $Hom(A, B)$).

Решение.

$$(\alpha + \beta)(x) = \alpha(x) + \beta(x)$$

- Ассоциативность: $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ – очевидно
- Нейтральный элемент: $e(x) = 0 \in B$
- Обратный элемент: $\alpha^{-1}(x) \equiv -\alpha(x)$

■

Задача 7. Опишите группу $Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$.

Решение.
Воспользуемся тем, что

$$\varphi(A_1 \oplus A_2, B) \cong \varphi(A_1, B) \oplus \varphi(A_2, B)$$

Тогда, если $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ и $m = p_1^{\beta_1} \cdots p_k^{\beta_k}$, то

$$Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \bigoplus_{p_i} Hom(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}, \mathbb{Z}/p_i^{\beta_i}\mathbb{Z})$$

Осталось разобраться, как устроены группы вида $Hom(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}, \mathbb{Z}/p_i^{\beta_i}\mathbb{Z})$. Разберем два случая:

- $\alpha_i < \beta_i$. Тогда $Hom\left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}, \mathbb{Z}/p_i^{\beta_i}\mathbb{Z}\right) \cong \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$
- $\alpha_i \geq \beta_i$. Тогда $Hom(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}, \mathbb{Z}/p_i^{\beta_i}\mathbb{Z}) \cong \mathbb{Z}/p_i^{\beta_i}\mathbb{Z}$

■

Семинар 6. Действие группы на множестве.

Разбор задач домашнего задания.

Задача 1. Привести пример группы, которая не является конечно порожденной, но каждый элемент которой имеет конечный порядок.

Решение.
В качестве примера можно привести множество всех бесконечных строк из 0 и 1 с операцией сложения по модулю 2 (т.е. многочленов над $\mathbb{Z}/2\mathbb{Z}$) – каждый элемент в этой группе имеет порядок 2.

Также можно рассмотреть группу $\mathbb{Q}/\mathbb{Z}$ (каждому рациональном числу сопоставим его дробную часть) – в ней, кроме того, что все элементы имеют конечный порядок, можно найти элементы сколь угодно большого порядка. Действительно, порядок несократимой дроби a/b будет равен b. Существует еще одна интерпретация этой группы. Рассмотрим отображение

$$\mathbb{Q} \to \mathbb{C}^*$$
$$x \mapsto e^{2\pi i x}$$

Это гомоморфизм групп, его ядро – это $\mathbb{Z}$, а образ (по теореме о гомоморфизме) изоморфен $\mathbb{Q}/\mathbb{Z}$. При этом гомоморфизме рациональные числа переходят в множество всех корней целой степени из единицы:

$$\sqrt[\infty]{1} = \bigcup_{n\in\mathbb{N}} \sqrt[n]{1}$$

■

Задача 3. Найти размерность пространства $\mathbb{R}[x_1, \dots, x_n]$ – симметричных многочленов степени не выше d (считаем, что $n > d$).

Решение.
Размерность пространства равна количеству элементов в базисе пространства, а базис состоит из симметрических многочленов вида $x_1^{a_{\sigma(1)}} x_2^{a_{\sigma(2)}} \cdots x_n^{a_{\sigma(n)}}$. Всего в базисе будет столько же элементов, сколько слагаемых в сумме

$$\sum_{\sigma\in S_n} x_1^{a_{\sigma(1)}} x_2^{a_{\sigma(2)}} \cdots x_n^{a_{\sigma(n)}}$$

т.е. столько же, сколько решений (в неотрицательных целых числах) у системы

$$\begin{cases} a_1 + a_2 + \cdots + a_n = d \\ a_1 \geq a_2 \geq \cdots \geq a_n \geq 0 \end{cases}$$

Таким образом, задача сводится к нахождению числа разбиений $p(d)$. ■

Действие группы на множестве.

Определение. Действие группы G на множестве X – это отображение

$$G \times X \to X$$
$$(g, x) \mapsto gx$$

со следующими свойствами: $\forall g_1, g_2 \in G, x \in X$:

- $ex = x$,
- $g_1(g_2 x) = (g_1 g_2)x$.

Действие группы на множестве – очень важный математический объект, который позволяет понять как свойства объекта, на котором действует группа, так и устройство самой группы.

Например, рассмотрим группу диэдра D_n. Мы определили ее как группу симметрий правильного n-угольника. В случае нечетного n любая ось симметрии проходит через центр n-угольника и одну из вершин, а в случае четного n любая ось симметрии проходит либо через противоположные вершины, либо через середины противоположных сторон n-угольника. При этом для нечетного n все симметрии лежат в одном классе сопряженности, а для четного n классов сопряженности для симметрий уже два. Понять этот факт нам помогло действие группы D_n на плоскости.

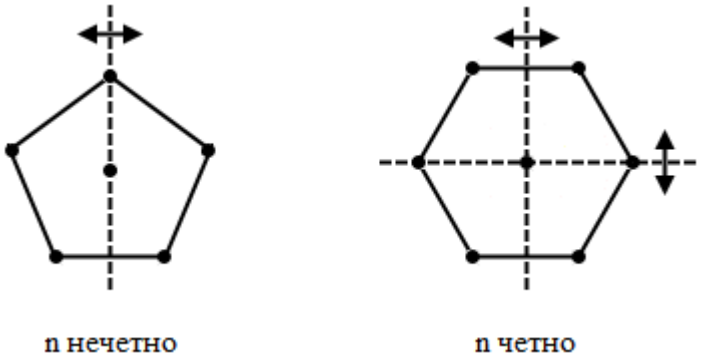

Рис. 6.1. Случай четного и нечетного n

Введем еще несколько важных понятий.

Определение. Отношение эквивалентности по действию группы G разбивает множество X на попарно непересекающиеся классы эквивалентности, которые называются орбитами для действия группы G на множестве X:

$$Gx = \{gx \mid g \in G\}$$

- орбита точки $x \in X$.

С понятием орбиты связано еще одно важное понятие в теории действий – понятие стабилизатора.

Определение. Пусть задано действие $G \curvearrowright X$. Стабилизатор точки $x \in X$ (обозначение: G_x) – это множество всех элементов группы G, действие которых оставляет точку x на месте:

$$G_x = \{g \in G:\ \ gx = x\}$$

Например, рассмотрим действие D_6 на плоскости и попробуем найти орбиту для произвольной точки плоскости. Орбита центра 6-угольника состоит из одной точки – нее самой. Орбита каждой вершины состоит из 6 точек – всех вершин 6-угольника. Также из 6 точек состоят орбиты точек, лежащих на осях симметрии 6-угольника. Орбиты точек общего положения на плоскости состоят из 12 точек – см. рис. 6.2:

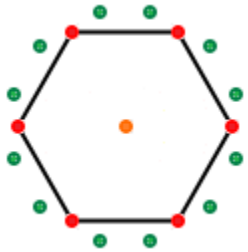

Рис. 6.2. Орбиты точек

Если мы в качестве множества X будем рассматривать не всю плоскость, а например, множество прямых, содержащих диагонали 6-угольника, то орбита каждой прямой будет состоять из трех элементов (трех прямых, содержащих диагонали). Этот пример показывает, что количество элементов в орбите зависит от множества, на котором действует группа.

Оказывается, имеет место следующее важное соотношение:

$$|G| = |Gx| \cdot |G_x|$$

- порядок группы равен произведению порядков орбиты и стабилизатора элемента. Это следует из теоремы Лагранжа и следующей теоремы:

Теорема. Существует взаимно-однозначное соответствие между точками орбиты точки x и множеством левых смежных классов группы G по стабилизатору точки x:

$$Gx \leftrightarrow G/G_x$$
$$y = gx \leftrightarrow gG_x$$

Доказательство.
Рассмотрим отображение

$$Gx \to G/G_x$$
$$y = gx \mapsto gG_x$$

Поймем, почему это отображение корректно определено (одна и та же точка y может получаться из x действием разных элементов группы G – нужно проверить, что все они соответствуют одному и тому же смежному классу справа).

Пусть $y = ax = bx$ - подействуем на обе части равенства элементом a^{-1}:

$$a^{-1}bx = x \Rightarrow a^{-1}b \in G_x \Rightarrow b = a \cdot a^{-1}b,\ \ a^{-1}b \in G_x$$

т.е. элементы a и b принадлежат одному и тому же смежному классу: $aG_x = bG_x$. Поэтому отображение определено корректно, кроме того, оно биективно. Следовательно, мы установили взаимно-однозначное соответствие

$$Gx \leftrightarrow G/G_x$$
$$y = gx \leftrightarrow gG_x$$

■

Определение. Действие группы тривиально, если $\forall g \in G$ и $x \in X$ выполнено $gx = x$.

Определение. Действие группы эффективно, если $\forall g \in G$, $g \neq 1$ и $x \in X$ выполнено $gx \neq x$.

Приведем еще пример действия. Рассмотрим действие циклической группы порядка n – например, рассмотрим подгруппу поворотов в D_6 – под действием этой группы каждая точка плоскости поворачивается вокруг центра правильного 6-угольника на угол, кратный $\pi/3$.

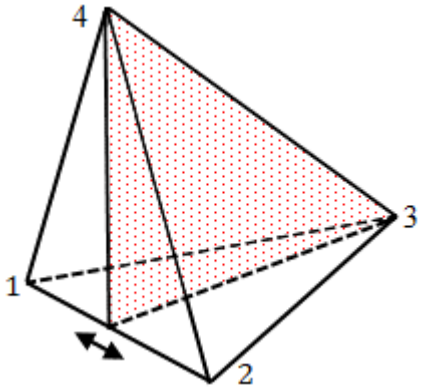

Рис. 6.3. $Sym\ (T) \cong S_4$

Теперь рассмотрим группу симметрий правильного тетраэдра. Как отмечалось ранее (см. семинар 1), его группа изометрий совпадает с S_4: $Sym\ (T) \cong S_4$ (см. рис. 6.3).

Действительно, $Sym(T)$ – это некоторая подгруппа в S_4. Но группа S_4 (как и все S_n) порождается транспозициями, поэтому нам достаточно показать, что транспозиция двух вершин реализуется некоторым движением пространства.

Это действительно так: транспозиция двух вершин – это отражение относительно плоскости, проходящей через середину стороны, содержащей эти вершины, и две другие вершины тетраэдра (см. рис. 6.3).

Посмотрим, какие могут быть длины орбит у разных элементов тетраэдра:

- Центр тетраэдра образует орбиту порядка 1.
- Вершины тетраэдра образуют орбиту порядка 4.
- Середины ребер образуют орбиту порядка 6.
- Точки, которые делят ребра в отношении $2:1$, образуют орбиту длины 12.
- Точки, лежащие на грани (но не на медианах этой грани) входят в орбиту длины 24.

Действие группы на себе самой.

Обсудим, как группа G действует на себе самой. Приведем три стандартных примера.

- $G \curvearrowright G$ левыми сдвигами: $(g_1g_2)g = g_1(g_2g)$
- $G \curvearrowright G$ правыми сдвигами: $g(g_1g_2)^{-1} = (gg_2)^{-1}{g_1}^{-1}$
- $G \curvearrowright G$ сопряжениями: $g \mapsto g_1g{g_1}^{-1}$

Из того, что сопряжение является действием группы на себя, и теоремы, приведенной выше, следует, что количество элементов в классе сопряженности делит порядок группы.

Рассмотрим поподробнее действие группы на себе левыми сдвигами. Количество элементов в орбите этого действия равно порядку группы – очевидно, так как по крайней мере произведение 1 на все элементы группы даст нам всю группу.

Пронумеруем элементы группы числами от 1 до n, тогда каждый элемент группы определяет какую-то перестановку в S_n. Следовательно, любая конечная группа G вкладывается в S_n, где $n = |G|$. Другими словами, группы подстановок – универсальные группы, в которые вкладывается любая другая группа.

Приведем еще одно наблюдение. Пусть v_i – базис векторного пространства V, $i \in G$, $\dim V = ord\ G$. Определим действие G на V следующим образом:

$$gv_i = v_{gi}$$

- определили действие G на базисе V, на остальные элементы V доопределяем по линейности. Таким образом, с помощью действия мы можем вложить группу G в группу линейных операторов на V.

Действия групп на векторных пространствах называются линейными действиями группы. Действие, приведенное выше, называется тавтологическим.

Пример. Рассмотрим вложение $D_n \hookrightarrow GL_2(\mathbb{R})$. Образующие D_n в матричном виде записываются следующим образом:

$$r = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}, \quad s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

Пример. Рассмотрим вложение $\mathbb{Z}/n\mathbb{Z} \hookrightarrow GL_1(\mathbb{C})$. Образующая: $\xi_n = e^{\frac{2\pi i}{n}}$.

Пример. Найдем $|G|$, где G – группа движений куба. При движении, оставляющем на месте куб, вершины куба каким-то образом переставляются, поэтому можно говорить о действии группы G на множестве вершин куба:

$$G \curvearrowright X = \{\text{вершины куба}\}$$

Это действие, очевидно, транзитивно (любую вершину некоторой последовательностью вращений можно перевести в любую другую).

Зафиксируем некоторую грань куба x – в орбиту Gx этой грани входит 6 элементов (все грани куба). Осталось найти $|G_x|$ – порядок стабилизатора грани. Но стабилизатор грани – это группа симметрий квадрата (т.е. D_4), а ее порядок, как мы знаем, равен 8. Поэтому

$$|G| = |Gx| \cdot |G_x| = 6 \cdot 8 = 48$$

Отметим, что группа вращений (собственных движений) куба имеет порядок 24.

Семинар 7. p-группы.

Разбор задач домашнего задания.

Задача 1. Существует ли действие группы.A_4 с орбитой длины 2 ?

Решение.
Нет, потому что в противном случае стабилизатор имел бы порядок 6 (так как $|A_4| = 12$), но в A_4 нет подгрупп порядка 6. ■

Задача 2. Описать группу вращений куба.

Решение.
В конце прошлого семинара мы нашли порядок группы движений куба, и порядок группы вращений (собственных движений) куба – он равен 24 (собственных движений столько же, сколько и несобственных). Группа вращений куба – это группа S_4. Изоморфизм строится так: каждому вращению ставится в соответствие перестановка главных диагоналей куба:

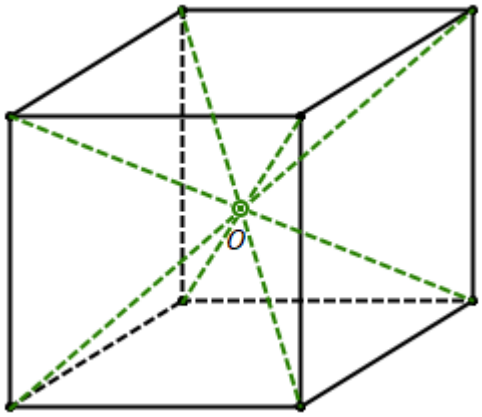

Рис. 7.1. $G \cong S_4$

■

Задача 3. Найти порядки группы движений и группы вращений икосаэдра.

Решение.
Рассмотрим действие группы симметрий икосаэдра на его гранях. Это действие, очевидно, транзитивно (любую грань некоторой последовательностью движений можно перевести в любую другую), поэтому оно имеет орбиту длины 20 (у икосаэдра 20 граней).

Осталось найти $|G_\Gamma|$ – порядок стабилизатора грани. Так как грань икосаэдра – правильный треугольник, группа симметрий которого – это S_3 (причем любая из этих симметрий входит также в группу симметрий икосаэдра), то $|G_\Gamma| = |S_3| = 6$. Поэтому

$$|G| = |G_\Gamma| \cdot |G_\Gamma| = 20 \cdot 6 = 120$$

Так как в группе движений икосаэдра собственных и несобственных движений поровну, то в группе вращений икосаэдра будет 60 элементов. Более того, оказывается, что группа вращений икосаэдра изоморфна A_5 (мы не будем это доказывать). ■

Задача 4. Найти все автоморфизмы графа, изображенного на рис. 7.2 (граф Петерсона).

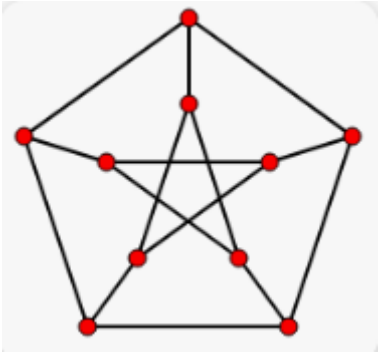

Рис. 7.2. Граф Петерсона

Решение.
Степени всех вершин этого графа одинаковы (равны 3), также любые две вершины соединяются либо одним, либо двумя ребрами, причем путь с таким количеством ребер единственный – поэтому в графе нет циклов длины 3 и 4.

Заметим, что порядок группы автоморфизмов этого графа равен 120. Действительно, любые два непересекающихся цикла длины 5 дополняют друг друга до полного графа, причем каждой вершине одного соответствует ровно одна вершина другого. В графе есть 12 циклов длины 5, причем каждый из них можно перевести в себя 10 способами.

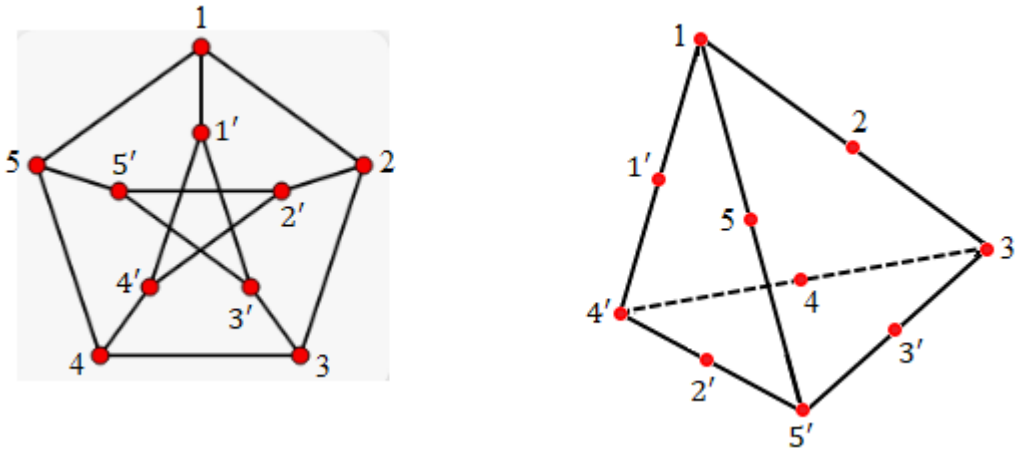

Рис. 7.3. К задаче 4

Также можно заметить, что граф Петерсона изоморфен графу, изображенному на рис. 7.3 (вершины графа – это вершины правильного тетраэдра и середины его ребер), поэтому порядок группы автоморфизмов графа Петерсона не менее 120 (так как в эту группу вложена S_4 и есть элемент порядка 5), также несложно показать, что он не может превосходить 120.

Теперь поймем структуру этой группы. Рассмотрим на проективной плоскости 5 точек общего положения и проведем все возможные прямые, соединяющие эти точки – получим $C_5^2 = 10$ прямых. Всего будет 15 точек пересечения этих прямых друг с другом, причем каждая прямая пересекается ровно с 3 другими. Прямые будем нумеровать в зависимости от того, какие точки они соединяют – например, прямую, соединяющую точки 1 и 3 обозначим l_{13}.

Несложно видеть, что мы получили интерпретацию графа Петерсона (вершины графа = прямые, ребра графа = точки пересечения прямых). Осталось заметить, что группа S_5 действует на этих прямых заменой индексов. Таким образом, группа автоморфизмов графа Петерсона изоморфна S_5. ■

Задача 6. Опишите группу $GL_2(\mathbb{F}_2)$

Решение.
Как было показано ранее (см. семинар 4), $Aut\ (\ (\mathbb{Z}/p\mathbb{Z})^n) \cong GL_n(\mathbb{F}_p)$, поэтому

$$GL_2(\mathbb{F}_2) \cong Aut\ (\ \mathbb{F}_2^2)$$

Также ранее было показано (см. семинар 3), что $Aut\ (\ \mathbb{F}_2^2) \cong S_3$. Таким образом,

$$GL_2(\mathbb{F}_2) \cong S_3$$

■

Задача 7. Опишите группу $PGL_2(\mathbb{F}_3)$

Решение.
Вначале, как и в предыдущей задаче, воспользуемся тем, что $GL_2(\mathbb{F}_3) \cong Aut\ (\ \mathbb{F}_3^2)$. Порядок этой группы равен 48. Далее воспользуемся тем, что $PGL_2(\mathbb{F}_3) = GL_2(\mathbb{F}_3)\backslash D^4$, откуда следует, что $|PGL_2(\mathbb{F}_3)| = 24$. Так как группа $PGL_2(\mathbb{F}_3)$ действует на проективных прямых, проходящих через точки $\mathbb{F}_3$, эффективно, то $PGL_2(\mathbb{F}_3) \cong S_4$. ■

p-группы

Определение. p-группы – это группы порядка p^k, где p – простое.

Как мы знаем, если порядок группы G равен простому числу p, то такая группа изоморфна $\mathbb{Z}/p\mathbb{Z}$. Если порядок группы G равен p^2, где p – простое, то G – абелева.

Утверждение. p-группа имеет нетривиальный центр.

Доказательство.
Пусть G - p-группа порядка p^k. Рассмотрим действие этой группы сопряжениями на себя. Так как порядок орбиты делит порядок группы, то порядок любой нетривиальной орбиты должен делиться на p. При этом орбита единичного элемента содержит только один элемент – его самого. Значит, одноточечных орбит должно быть хотя бы p штук (иначе сумма элементов во всех орбитах не будет делиться на p). Следовательно, в центре лежит не менее p элементов. ■

Утверждение. Если $|G| = p^2$, p-простое, то G – абелева.

Доказательство.
По предыдущему утверждению центр G нетривиален: $C(G) \neq \{e\}$. Рассмотрим $a \in C(G)$, и $b \in G$, такой что b не является степенью a (если такого b не существует, то группа G циклическая, а значит, абелева). Имеем: $ab = ba$ и $a^p = b^p = 1$, но это означает, что a и b порождают группу $(\mathbb{Z}/p\mathbb{Z})^2$, откуда следует, что G – абелева. ■

Задача. Привести пример неабелевой группы порядка p^3, где p – нечетное.

Решение.
Рассмотрим матрицы вида $\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$, где $a, b, c \in \mathbb{F}_p$. Очевидно, что матрицы такого вида образуют группу, ее порядок равен p^3 (на месте a, b, c может стоять любой элемент из $\mathbb{F}_p$ – всего получаем p^3 вариантов). Проверим, что группа неабелева:

$$\begin{pmatrix} 1 & a_1 & c_1 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a_2 & c_2 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_1 + a_2 & c_2 + a_1 b_2 + c_1 \\ 0 & 1 & b_1 + b_2 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & a_2 & c_2 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a_1 & c_1 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_1 + a_2 & c_2 + a_2 b_1 + c_1 \\ 0 & 1 & b_1 + b_2 \\ 0 & 0 & 1 \end{pmatrix}$$

Отсюда также следует, что в центре этой группы будут лежать матрицы, удовлетворяющие условию $a_1 b_2 = a_2 b_1$ для произвольной матрицы указанного вида, т.е. центр состоит из матриц вида

$$\begin{pmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$d \in \mathbb{F}_p$. Построенная группа называется группой Гейзенберга.

Еще один способ: рассмотрим группу, порожденную матрицами $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}$ ($\omega = e^{\frac{2\pi i}{3}}$ – корень степени 3 из единицы) и $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. Легко проверить, что эти матрицы не коммутируют, также несложно видеть, что порядок группы, порожденной этими матрицами, конечен – в самом деле, существует 3 варианта расположения ненулевых элементов:

$$\begin{pmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix} \quad \begin{pmatrix} 0 & * & 0 \\ 0 & 0 & * \\ * & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & * \\ * & 0 & 0 \\ 0 & * & 0 \end{pmatrix}$$

а каждый ненулевой элемент – это либо 1, либо ω, либо ω^2, при этом определитель каждой матрицы равен 1. Получаем, что всего в группе будет не более 27 элементов, в то же время, в ней не может быть менее 27 элементов (так как это неабелева 3-группа).

Центр этой группы состоит из скалярных матриц. Построенная группа называется обобщенной группой Гейзенберга. ■

Семинар 8. Централизатор элемента и нормализатор подгруппы.

Разбор задач домашнего задания.

Задача 1. В группе G порядка p^k построить нормальную группу порядка p^l для любого $l \leq k$.

Решение.
Всякая p-группа имеет нетривиальный центр, который тоже является p-группой (абелевой), а во всякой абелевой p-группа содержится подгруппа, изоморфная $\mathbb{Z}/p\mathbb{Z}$. Факторизуя группу G по этой подгруппе мы получим некоторую группу G_1 порядка p^{k-1}:

$$G_1 \cong G/(\mathbb{Z}/p\mathbb{Z})$$

- снова получили p-группу, но уже порядка p^{k-1}. И так далее: $G_2 \cong G_1/(\mathbb{Z}/p\mathbb{Z}), \cdots$, $G_l \cong G_{l-1}/(\mathbb{Z}/p\mathbb{Z})$, $|G_l| = p^{k-l}$. Получаем последовательность сюръективных гомоморфизмов

$$G \to G_1 \to \cdots \to G_l$$

Значит, существует и гомоморфизм $G \to G_l$. Тогда (по теореме о гомоморфизме), $G_l \cong G/H$, где H – некоторая нормальная подгруппа, порядок которой равен

$$|H| = \frac{|G|}{|G_l|} = \frac{p^k}{p^{k-l}} = p^l,$$

где $l \leq k$ – любое. ■

Задача 2. Пусть G- p-группа, $N \lhd G$. Доказать, что $N \cap C \neq \{1\}$ (C – центр G).

Решение.
Рассмотрим действие группы G сопряжениями на группе N. Орбиты всех элементов будут состоять либо из одного элемента, либо количество элементов в них будет делиться на p. При этом орбита единичного элемента содержит только один элемент – его самого. Значит, одноточечных орбит должно быть хотя бы p штук (иначе сумма элементов во всех орбитах не будет делиться на p). Следовательно, $N \cap C \neq \{1\}$:

$$gng^{-1} = n \Leftrightarrow gn = ng \Leftrightarrow n \in C$$

■

Задача 3. Построить неабелеву группу порядка 81, содержащую элемент порядка 9.

Решение.

На прошлом семинаре мы построили обобщенную группу Гейзенберга. Это неабелева группа порядка 27, порожденная матрицами $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}$ ($\omega = e^{\frac{2\pi i}{3}}$ – корень степени 3 из единицы) и $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. Все матрицы в этой группе имеют вид:

$$\begin{pmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix} \quad \begin{pmatrix} 0 & * & 0 \\ 0 & 0 & * \\ * & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & * \\ * & 0 & 0 \\ 0 & * & 0 \end{pmatrix}$$

здесь каждый ненулевой элемент – либо 1, либо ω, либо ω^2, при этом определитель каждой матрицы равен 1.

Теперь откажемся от условия равенства определителя единице. Получим неабелеву группу порядка 81 (она неабелева, так как группа Гейзенберга в ней содержится). Осталось найти в ней элемент порядка 9. Почти очевидно, что таким элементом является матрица

$$\begin{pmatrix} 0 & \omega & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

■

Задача 4. Найти коммутанты следующих групп: а) S_3, б) A_4, в) S_4, г) Q_8, д) D_n.

Решение.
а) Из того, что $A_3 \lhd S_3$ и S_3/A_3 – абелева, следует, что $S_3' \subseteq A_3$. Но в A_3 нет нетривиальных подгрупп, следовательно, $S_3' = A_3$ (S_3' не может быть равен 1, так как S_3 неабелева).

б) Как было выяснено ранее, $V_4 \lhd A_4$ – единственная нормальная подгруппа в A_4. Также $A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$ - абелева. Значит, $A_4' = V_4$ (четверная группа Клейна).

в) Докажем, что $S_n' = A_n$. Как мы знаем, группа S_n порождается транспозициями. Если транспозиции независимы, то они коммутируют между собой и их коммутатор тривиален, а если транспозиции зависимы, то:

$$[(i,j),(j,k)] = (i,j)\cdot(j,k)\cdot(i,j)^{-1}\cdot(j,k)^{-1} = (i,j,k)\cdot(i,j,k) = (i,k,j)$$

Так как тройные циклы порождают группу A_n при $n \geq 3$, то $S_n' \supseteq A_n$. Это включение верно и при $n = 1,2$, так как в этих случаях $A_n = \{\varepsilon\}$.

С другой стороны, $A_n \lhd S_n$, и $S_n/A_n \cong \{\pm 1\}$ абелева. Следовательно, $S_n' \subseteq A_n$. Таким образом, $S_n' = A_n$. В частности, $S_4' = A_4$.

г) Q_8 состоит из элементов $\pm 1, \pm i, \pm j, \pm k$. Операция умножения задана по правилам:

$$\begin{gathered} i^2 = j^2 = k^2 = -1, \\ i \cdot j = k, \quad j \cdot i = -k \\ j \cdot k = i, \quad k \cdot j = -i \\ k \cdot i = j, \quad i \cdot k = -j \end{gathered}$$

Вычисление коммутанта по определению показывает, что $Q_8' = \{\pm 1\}$.

д) $D_n = < r, s \mid r^n = s^2 = 1, srs^1 = r^{-1} >$. На семинаре 3 мы уже находили все нормальные подгруппы в D_n и факторы по ним. Рассмотрим два случая:

1) n – нечетное. Все нормальные подгруппы в D_n имеют вид $< 1, r^d, \dots, r^{n-d} >$ - подгруппы поворотов, порожденные элементом r^d, где $d \vdots n$. Имеем:

$$D_n / < 1, r^d, \dots, r^{n-d} > \cong D_d$$

- так как D_d будет абелевой лишь при $d = 1$, получаем, что $D_n' = < 1, r, \dots, r^{n-1} >$.

2) n – четное. Классы сопряженности $\{r^{2k}s\}$ и $\{r^{2k+1}s\}$ являются также и нормальными подгруппами в D_n, каждая из которых содержит $\frac{n}{2}$ элементов. Факторгруппы по этим нормальным подгруппам изоморфны $\mathbb{Z}/2\mathbb{Z}$:

$$\begin{gathered} D_n/\{r^{2k}s\} \cong \mathbb{Z}/2\mathbb{Z} \\ D_n/\{r^{2k+1}s\} \cong \mathbb{Z}/2\mathbb{Z} \end{gathered}$$

Так как $\mathbb{Z}/2\mathbb{Z}$ - абелева, то D_n' лежит в пересечении этих двух групп, т.е. в группе, порожденной r^2: $< 1, r^2, r^4, \dots, r^{n-2} >$. Факторизуем:

$$D_n / < 1, r^2, r^4, \dots, r^{n-2} > \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Так как группа $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ абелева, а факторгруппы по подгруппам вида $< 1, r^d, \dots, r^{n-d} >$, где $d > 2$ уже не будут абелевыми, то $D_n' = < 1, r^2, r^4, \dots, r^{n-2} >$. ■

Как мы обсуждали ранее, произвольную группу G можно вложить в группу $GL_n(K)$, также ее можно вложить в группу S_n. Зададимся вопросом – существуют ли еще такие

"универсальные" группы, в которые можно вложить произвольную группу? Может быть, такой группой является A_n?

Рассмотрим вложения $G \hookrightarrow S_n \hookrightarrow S_{n+2}$. Как мы знаем, $A_{n+2} \lhd S_{n+2}$, при этом половина перестановок (все четные) в S_n уже лежат в A_{n+2}. Рассмотрим нечетные перестановки в S_n: пусть $\sigma \in S_n$, но $\sigma \notin A_n$, тогда $\sigma(n+1, n+2) \in A_{n+2}$. Таким образом, мы получили вложение $S_n \hookrightarrow A_{n+2}$.

Теперь поймем, можно ли вложить произвольную группу в произведение диэдральных групп. Как мы знаем, всякая диэдральная группа является разрешимой. Заметим, что произведение разрешимых групп разрешимо. В самом деле, если G_1 и G_2 – разрешимые группы, то $(G_1 \times G_2)' = G_1' \times G_2'$. Также всякая подгруппа разрешимой группы является разрешимой. Поэтому группу, не являющуюся разрешимой, нельзя вложить в произведение диэдральных групп.

Задача. Разрешимы ли группы: а) $SL_2(\mathbb{F}_2)$, б) $SL_2(\mathbb{F}_3)$.

Решение.
а) Воспользуемся тем, что $SL_2(\mathbb{F}_2) \subset GL_2(\mathbb{F}_2)$. Как мы знаем (см. прошлый семинар), $GL_2(\mathbb{F}_2) \cong S_3$, а группа S_3 разрешима. Значит, и $SL_2(\mathbb{F}_2)$ разрешима.

б) Воспользуемся тем, что $SL_2(\mathbb{F}_3) \subset GL_2(\mathbb{F}_3)$. В $GL_2(\mathbb{F}_3)$ есть нормальная подгруппа, состоящая из скалярных матриц $\{E, 2E\}$. Профакторизовав по этой подгруппе группу $GL_2(\mathbb{F}_3)$, мы получим $PGL_2(\mathbb{F}_3)$, но (см. прошлый семинар) $PGL_2(\mathbb{F}_3) \cong S_4$, а группа S_4 разрешима. Значит, и $SL_2(\mathbb{F}_3)$ разрешима. ■

Централизатор. Нормализатор

Определение. Пусть $g \in G$. Централизатор g – это группа H, такая что $\forall h \in H$ выполнено $hgh^{-1} = g$. Другими словами, централизатор элемента g – это множество всех элементов группы, которые коммутируют с элементом g.

Определение. Пусть P – подгруппа в G. Нормализатор P – это группа H, такая что $\forall h \in H$ выполнено $hPh^{-1} = P$. Другими словами, нормализатор группы P – это наибольшая подгруппа в G, в которой P нормальна.

Задача. $(123) \in S_6$. Найти порядки централизатора (123) и нормализатора $< (123) >$.

Решение.
При действии группы S_6 на себе сопряжениями орбита элемента (123) состоит из циклов вида $(i\ j\ k)$ – всего в S_6 есть 40 таких циклов, при этом вся группа S_6 состоит из

$6! = 720$ элементов. Значит, порядок централизатора равен $720/40 = 18$. Централизатор (123) можно описать явно – это $\mathbb{Z}/3\mathbb{Z} \times S_3 \cong < (123), (456), (45) >$.

При действии группы S_6 на себе сопряжениями орбита группы $< (123) >$ состоит из 20 циклических групп. Значит, порядок нормализатора равен $720/20 = 36$. Нормализатор $< (123) >$ можно описать явно – это $S_3 \times S_3 \cong < (123), (12); (456), (45) >$. ■

Задача. $(123)(456) \in S_6$. Найти порядки централизатора $(123)(456)$ и нормализатора $< (123)(456) >$.

Решение.
При действии группы S_6 на себе сопряжениями орбита элемента $(123)(456)$ состоит из циклов вида $(i\ j\ k)(x\ y\ z)$ – всего в S_6 есть 40 таких циклов, при этом вся группа S_6 состоит из $6! = 720$ элементов. Значит, порядок централизатора равен $720/40 = 18$. Централизатор (123) можно описать явно – это $< (123), (456), (14)(25)(36) >$.

При действии группы S_6 на себе сопряжениями орбита группы $< (123)(456) >$.состоит из 20 циклических групп. Значит, порядок нормализатора равен $720/20 = 36$. Нормализатор $< (123)(456) >$ можно описать явно – это $< (123), (456), (14)(25)(36), (12)(45) >$. ■

Семинар 9. Полупрямое произведение групп.

Разбор задач домашнего задания.

Задача 1. Найти все разрешимые группы, порядок которых меньше 60.

Решение.
Заведомо можно сказать, что разрешимыми будут группы, порядок которых равен p^k (так как их центр нетривиален) и группы, порядок которых равен pq, где p, q – простые. Вопрос о разрешимости групп других порядков оставим до знакомства с теоремами Силова. ■

Задача 2. Найти количество элементов порядка 2 в различных классах сопряженности группы S_n.

Решение.
Элементы порядка 2 в S_n – это в точности перестановки, раскладывающиеся в произведение независимых транспозиций. Рассмотрим произведение k независимых транспозиций в S_n: $(12)\cdots(2k-1\ 2k)$ и найдем количество элементов в таком классе сопряженности. Как мы знаем, в S_n классы сопряженности состоят из перестановок с одинаковой цикловой структурой, т.е. сопряженные перестановки имеют вид $(i_1 i_2)\cdots(i_{2k-1} i_{2k})$. Выбрать числа $i_1, i_2, \cdots, i_{2k-1} i_{2k}$ (упорядоченный набор) из набора $1, \cdots, n$ мы можем $n(n-1)\cdots(n-2k+1)$ способами, при этом различных перестановок с нужной цикловой структурой будет

$$\frac{n(n-1)\cdots(n-2k+1)}{k!\,2^k}$$

(мы можем переставлять транспозиции и менять числа внутри транспозиции местами).

При $k=1$ (т.е. в классе сопряженности, состоящем из всех транспозиций) будет $\frac{n(n-1)}{2}$ элементов. Вопрос: в каком случае это число будет совпадать с количеством элементов в каком-нибудь другом классе сопряженности элемента S_n порядка 2 ? Оказывается, это возможно только в S_6 – в классах сопряженности перестановок (12) и $(12)(34)(56)$ будет одинаковое число элементов – 15.

Таким образом, при всех $n \neq 2,6$ при автоморфизмах S_n (так как при автоморфизме классы сопряженности переходят в классы сопряженности) транспозиции переходят в транспозиции (с помощью некоторого сопряжения) и $Aut\, S_n \cong S_n$. Но S_6 является исключением (как мы показали выше), и существует автоморфизм, переводящий классы сопряженности перестановок (12) и $(12)(34)(56)$ друг в друга. ■

Задача 3. Описать централизатор $(123)(456)$ в S_6.

Решение.
Заметим, что в централизаторе $(123)(456)$ присутствует группа $<(123),(456)>$ порядка 9, изоморфная $(\mathbb{Z}/3\mathbb{Z})^2$. На предыдущем семинаре мы выяснили, что порядок централизатора $(123)(456)$ равен 18, т.е. осталось найти перестановку из централизатора, переводящую цикл (123) в (456) – например, подойдет перестановка $(14)(25)(36)$. Получаем, что централизатор (123) – это $<(123),(456),(14)(25)(36)>$.

Опишем устройство этой группы. В группе $<(123),(456)>$ есть элемент, который коммутирует с $(14)(25)(36)$ – это $(123)(456)$. Запишем централизатор (123) в виде $<(123)(456),(123)(465),(14)(25)(36)>$. Так как $(123)(456)$ коммутирует и с $(123)(465)$, и с $(14)(25)(36)$, а группа $<(123)(465),(14)(25)(36)>$ состоит из 6 элементов и неабелева (т.е. изоморфна S_3), получаем, что централизатор $(123)(456)$ в S_6 изоморфен $\mathbb{Z}/3\mathbb{Z} \times S_3$. ■

Задача 4. Описать нормализатор $<(123)(456)>$ в S_6.

Решение.
На предыдущем семинаре мы выяснили, что порядок нормализатора $<(123)(456)>$ равен 36. Рассмотрим группу $<(123)(456),(123)(465),(14)(25)(36),(15)(24)(36)>$ - это группа порядка 36, изоморфная $S_3 \times S_3$, при этом несложно проверить, что она и будет нормализатором для $<(123)(456)>$. ■

Задача 5. Найти порядок нормализатора $<(123),(456)>$ в S_6.

Решение.
При действии группы S_6 на себе сопряжениями орбита группы $<(123),(456)>$ состоит из 10 групп (в самом деле, группа с таким же циклическим строением, как и у группы $<(123),(456)>$, определяется способом разбиения множества $(1,2,3,4,5,6)$ на два множества по три элемента в каждом. Выбор одного множества из трех элементов однозначно задает второе множество, мы можем осуществить его $C_6^3 = 20$ способами, а учитывая, что множества можно переставлять местами, всего получаем $\frac{20}{2} = 10$ вариантов). Значит, порядок нормализатора равен $720/10 = 72$. ■

Задача 6. Описать нормализатор $<(12345)>$ в S_5.

Решение.
Класс сопряженности группы $<(12345)>$ в S_5 состоит из 6 элементов (в самом деле, всего в S_5 есть 24 элемента порядка 5, а в каждой циклической подгруппе порядка 5 есть

4 образующих элемента порядка 5 – полуаем всего $\frac{24}{4} = 6$ циклических подгрупп порядка 5). Значит, порядок нормализатора равен $120/6 = 20$.

Теперь поймем структуру нормализатора. Непосредственно проверяется, что в нормализаторе лежат элементы $g = (12345)$ порядка 5 и $h = (2354)$ порядка 4. Значит (так как порядок нормализатора равен $5 \cdot 4 = 20$), они будут образующими:

$$G = \{g; h:\ g^5 = 1, h^4 = 1, hgh^{-1} = g^2\}$$

Таким образом, $\mathbb{Z}/5\mathbb{Z} \lhd G$ и $G/(\mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$. ■

Задача 7. Найти группу порядка 21 в S_7.

При решении этой задачи мы будем использовать следующую лемму:

Лемма. Если G – группа, H – подгруппа наименьшего простого индекса (т.е. $\frac{|G|}{|H|}$ – простое число p и у $|G|$ нет простых делителей, меньших p), то $H \lhd G$.

Решение.
В этой группе должен быть элемент порядка 7 – пусть это будет (1234567). Осталось найти элемент порядка 3, который бы вместе с (1234567) порождал бы всю группу. Эти элементы порядка 3 и 7 не коммутируют друг с другом (т.к. иначе мы бы получили группу, изоморфную $\mathbb{Z}/21\mathbb{Z}$, но в S_7 нет элементов порядка 21). В качестве элемента порядка 3 можно выбрать $(235)(476)$. Тогда

$$G = \{g; h:\ g^7 = 1, h^3 = 1, hgh^{-1} = g^2\}$$

■

Полупрямое произведение групп.

Обратим внимание на то, что в последних двух задачах мы получили группы, которые похоже устроены: группа G содержит две подгруппы N и H, причем N нормальная, а H – нет, $|N||H| = |G|$ и $G/N \cong H$. Также любой элемент $g \in G$ единственным образом представляется в виде $g = hn$, где $h \in H$ и $n \in N$ и выполнено условие $\forall h \in H$: $hNh^{-1} = N$. Следовательно, существует отображение $H \to Aut\ (N)$.

Как мы видим, выполняются все условия того, что группа раскладывается в прямое произведение двух своих подгрупп, кроме нормальности одной из подгрупп. Такое разложение называется не прямым, а полупрямым произведением.

Определение. $N \leftthreetimes H$ – полупрямое произведение относительно отображения $\varphi\colon H \to Aut\,(N)$ – это множество пар (n, h) с операцией $(n_1, h_1)(n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1 h_2)$.

Семинар 10. Теоремы Силова.

На прошлом семинаре мы определили полупрямое произведение групп, используя конструкцию внешнего умножения. Можно сделать это, используя конструкцию внутреннего умножения.

Определение. Пусть G – группа, $N, H \subseteq G$ – подгруппы. G есть полупрямое произведение подгрупп N и H относительно отображения $\varphi\colon\ H \to Aut\ (N)$ (обозначение: $G = N \underset{\varphi}{\rtimes} H$), если:

- $G/N \cong H$,
- $N \cap H = 1$,
- $N \lhd G$.

Примеры.

1) Всякое прямое произведение групп является также полупрямым (относительно тривиального гомоморфизма $\varphi\colon\ H \to Aut\ (N)$).

2) Группа диэдра $G = D_n = < r, s >$ раскладывается в полупрямое произведение подгруппы поворотов и подгруппы, порожденной какой-то симметрией: так как $N = \mathbb{Z}/n\mathbb{Z} = < r >,\ G/N \cong \mathbb{Z}/2\mathbb{Z},\ H \cong \mathbb{Z}/2\mathbb{Z} = < h >$, то

$$D_n \cong (\mathbb{Z}/n\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z})$$

В данном случае автоморфизм N задается отображением $r \mapsto r^{-1}$.

3) Рассмотрим группу $G = S_n$ и в ней подгруппы A_n и $< (12) >$. Любая перестановка из S_n либо четная, (т.е. из A_n), либо нечетная (т.е. ее можно представить в виде произведения некоторой транспозиции, например $(1,2)$ и перестановки из A_n). При этом $A_n \lhd S_n$, также $A_n \cap < (12) > = 1$, но $< (1,2) >$ не является нормальной подгруппой в S_n при $n \geq 3$. Имеем: $N = A_n,\ G/N \cong \mathbb{Z}/2\mathbb{Z},\ H \cong \mathbb{Z}/2\mathbb{Z} = < (1,2) >$ и

$$S_n = A_n \rtimes (\mathbb{Z}/2\mathbb{Z})$$

В данном случае автоморфизм N задается сопряжением транспозицией $(1,2)$.

Разбор задач домашнего задания.

Задача 1. Разложить группу S_4 в полупрямое произведение.

Решение.
В S_4 есть нетривиальные нормальные подгруппы A_4 и V_4 (группа Клейна):

- 1) $N = V_4$. Имеем: $H \cong \mathbb{Z}/V_4 = S_3$ и $S_4 = V_4 \leftthreetimes S_3$. Гомоморфизм φ: $S_3 \to Aut\ (V_4)$ в данном случае является изоморфизмом.
- 2) $N = A_4$. Этот случай разобран выше (пример 3).

■

Задача 2. Разложить группу D_4 в полупрямое произведение.

Решение.
В D_4 есть нетривиальные нормальные подгруппы $< r >$ (подгруппа поворотов), $< r^2 >$, $< r^2, s >$.

- 1) $N = < r >$. Этот случай разобран выше (пример 2).
- 2) $N = < r^2 >$. Имеем: $D_4/N \cong (\mathbb{Z}/2\mathbb{Z})^2$, и $r^2 \in D_4/N$, т.е. пересечение групп D_4/N и N нетривиально, и конструкцию полупрямого произведения для $N = < r^2 >$ применить не удастся.
- 3) $N = < r^2, s >$. Имеем: $H = D_4/N = < rs >$ и $S_4 = < r^2, s > \leftthreetimes < rs >$.

■

Задача 3. Разложить группу Q_8 в полупрямое произведение.

Решение.
Q_8 состоит из элементов $\pm 1, \pm i, \pm j, \pm k$. Так $i^2 = j^2 = k^2 = -1$, то всякая нетривиальная подгруппа (в частности, всякая нормальная подгруппа) содержит -1 (квадрат всякого неединичного элемента). Таким образом, персечение любых нетривиальных подгрупп в Q_8 нетривиально, и Q_8 нельзя разложить в полупрямое произведение.

Например, пусть $N \cong \mathbb{Z}/4\mathbb{Z}$ (например, $N = < i >$), тогда $G/N \cong \mathbb{Z}/2\mathbb{Z}$ и $-1 \in G/N$, т.е. пересечение N и G/N нетривиально. Если $N = \mathbb{Z}/4\mathbb{Z}$, т.е. $N = \{\pm 1\}$, то $G/N \cong (\mathbb{Z}/2\mathbb{Z})^2$ и снова пересечение N и G/N нетривиально. ■

Задача 4. Описать полупрямые произведения групп $\mathbb{Z}/5\mathbb{Z}$ и $\mathbb{Z}/4\mathbb{Z}$.

Решение.
Так как $Aut\ (\mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$, нам достаточно описать все гомоморфизмы $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$. Всего существует 3 таких гомоморфизма: если a – образующий элемент группы $\mathbb{Z}/4\mathbb{Z}$, то он может переходить в элементы $1, b, b^2, b^3$, при этом случаи $a \to b$ и $a \to b^3$ идентичны.

- Гомоморфизму $a \to 1$ соответствует полупрямое произведение (которое является прямым) $\mathbb{Z}/20\mathbb{Z}$
- Гомоморфизмам $a \to b$ и $a \to b^3$соответствует полупрямое произведение $(\mathbb{Z}/5\mathbb{Z}) \underset{\varphi}{\rtimes} (\mathbb{Z}/4\mathbb{Z})$. Эта группа изоморфна нормализатору группы $< (12345) >$ в S_5, который порождается перестановками (12345) и (2354)
- Гомоморфизму $a \to b^2$ соответствует полупрямое произведение $(\mathbb{Z}/5\mathbb{Z}) \underset{\psi}{\rtimes} (\mathbb{Z}/4\mathbb{Z})$ – мы не будем описывать его явно, но отметим, что полученная группа не будет изоморфна $(\mathbb{Z}/5\mathbb{Z}) \underset{\varphi}{\rtimes} (\mathbb{Z}/4\mathbb{Z})$, так как в $(\mathbb{Z}/5\mathbb{Z}) \underset{\psi}{\rtimes} (\mathbb{Z}/4\mathbb{Z})$ присутствует элемент порядка 10.

Задача. Построить неабелеву группу G порядка 27, в которой есть элемент порядка 9.

Решение.
Так как в G есть элемент порядка 9, то есть и нормальная подгруппа $N \cong \mathbb{Z}/9\mathbb{Z}$ (она будет нормальной, так как это подгруппа наименьшего простого индекса). Также $G/N \cong \mathbb{Z}/3\mathbb{Z}$. Прямое произведение N и G/N даст абелеву группу, изоморфную $\mathbb{Z}/27\mathbb{Z}$, поэтому построим полупрямое произведение.

$Aut\,(\mathbb{Z}/9\mathbb{Z}) \cong \mathbb{Z}/6\mathbb{Z}$. Пусть φ – нетривиальный гомоморфизм φ: $\mathbb{Z}/3\mathbb{Z} \to Aut\,(\mathbb{Z}/9\mathbb{Z})$, тогда $(\mathbb{Z}/9\mathbb{Z}) \underset{\varphi}{\rtimes} (\mathbb{Z}/3\mathbb{Z})$ – искомая группа. ■

Задача 5. Классифицировать группы порядка 15.

Решение.
Из первой теоремы Силова следует, что в G есть силовская 3-подгруппа H_3 и 5-подгруппа H_5. Так как это группы простого порядка, то $H_3 \cong \mathbb{Z}/3\mathbb{Z}$ и $H_5 \cong \mathbb{Z}/5\mathbb{Z}$.

Из третьей теоремы Силова следует, что $\nu_3(\mathrm{H}) \equiv 1 (\mathrm{mod}\,3)$ и $\nu_5(\mathrm{H}) \equiv 1 (\mathrm{mod}\,5)$, где $\nu_3(\mathrm{H})$ и $\nu_5(\mathrm{H})$ – количество силовских 3-подгрупп и 5-подгрупп соответственно. Кроме того, из второй теоремы Силова следует, что $\nu_3(\mathrm{H})$ является делителем 5, откуда следует, что $\nu_3(\mathrm{H}) = 1$. Аналогично, из второй теоремы Силова следует, что $\nu_5(\mathrm{H})$ является делителем 3, откуда следует, что $\nu_5(\mathrm{H}) = 1$.

Из второй теоремы Силова следует, что силовская подгруппа нормальна тогда и только тогда, когда она единственна, поэтому H_3 и H_5 нормальны в G. Далее нетрудно показать, что G раскладывается в прямое произведение H_3 и H_5, т.е. G – абелева группа, изоморфная $\mathbb{Z}/15\mathbb{Z}$.

Альтернативное решение: пусть $|G| = 15$. Из первой теоремы Силова следует, что в G есть силовская 5-подгруппа N. Так как это группа простого порядка, то $N \cong \mathbb{Z}/5\mathbb{Z}$ и

$N \lhd G$ (так как N – подгруппа наименьшего простого индекса в G), следовательно, $G/N \cong \mathbb{Z}/3\mathbb{Z}$.

Также из первой теоремы Силова следует, что в G есть силовская 3-подгруппа H. Так как это группа простого порядка, то $H \cong \mathbb{Z}/3\mathbb{Z}$. Получаем $G \cong \mathbb{Z}/5\mathbb{Z} \leftthreetimes \mathbb{Z}/3\mathbb{Z}$. Как мы знаем, $Aut\ (\mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$, но существует только единственный (тривиальный) гомоморфизм из $\mathbb{Z}/3\mathbb{Z}$ в $\mathbb{Z}/4\mathbb{Z}$, поэтому $G \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/15\mathbb{Z}$. ■

Задача 6. Классифицировать группы порядка 21.

Решение.
Рассуждениями, аналогичными рассуждениям из предыдущей задачи, получаем, что $G = \mathbb{Z}/7\mathbb{Z} \leftthreetimes \mathbb{Z}/3\mathbb{Z}$. Далее, $Aut\ (\mathbb{Z}/7\mathbb{Z}) \cong \mathbb{Z}/6\mathbb{Z}$, и существует два гомоморфизма из $\mathbb{Z}/3\mathbb{Z}$ в $\mathbb{Z}/6\mathbb{Z}$: тривиальному гомоморфизму соответствует прямое произведение: $G \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/21\mathbb{Z}$, а нетривиальному соответствует полупрямое произведение $G \cong \mathbb{Z}/5\mathbb{Z} \leftthreetimes \mathbb{Z}/3\mathbb{Z}$. ■

Вывод: пусть $|G| = pq$, p и q – простые, $p < q$. Тогда $G \supset N \cong \mathbb{Z}/q\mathbb{Z}$, $N \lhd G$ и $G \supset H \cong \mathbb{Z}/p\mathbb{Z}$. Получаем $G \cong (\mathbb{Z}/q\mathbb{Z}) \leftthreetimes (\mathbb{Z}/p\mathbb{Z})$. Далее, $Aut\ (\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$. Получаем два варианта:

- Если $(q-1)$ не делится на p, то $G \cong \mathbb{Z}/pq\mathbb{Z}$
- Если $(q-1)$ делится на p, то групп две: $G \cong \mathbb{Z}/pq\mathbb{Z}$ и $G \cong (\mathbb{Z}/q\mathbb{Z}) \leftthreetimes (\mathbb{Z}/p\mathbb{Z})$

Задача 7. Классифицировать группы порядка 12.

Решение.
Из третьей теоремы Силова следует, что $N(G_3) \equiv 1 (\mathrm{mod}\ 3)$ и $N(G_2) \equiv 1 (\mathrm{mod}\ 2)$, где $N(G_3)$ и $N(G_2)$ – количество силовских 3-подгрупп и 2-подгрупп соответственно, также $N(G_3)$ – делитель 4, а $N(G_2)$ – делитель 3. Получаем, $N(G_3) = 1$ или 4 и $N(G_2) = 1$ или 3.

Заметим, что случай $N(G_3) = 4$ и $N(G_3) = 3$ невозможен – в самом деле, если $N(G_3) = 4$, то G содержит 4 группы, изоморфные $\mathbb{Z}/3\mathbb{Z}$, которые пересекаются только по 1, т.е. G содержит 8 элементов порядка 3, и вне силовских 3-подгрупп лежит только 3 неединичных элемента, которые могут входить только в одну силовскую 2-подгруппу порядка 4. Следовательно, как минимум одна из силовских подгрупп единственна, а следовательно, нормальна.

Если силовская 3-подгруппа нормальна, получаем четыре варианта:

- $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

- $G \cong \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$
- $G \cong \mathbb{Z}/3\mathbb{Z} \leftthreetimes \mathbb{Z}/4\mathbb{Z}$
- $G \cong \mathbb{Z}/3\mathbb{Z} \leftthreetimes (\mathbb{Z}/2\mathbb{Z})^2 \cong D_6$

Если силовская 2-подгруппа нормальна, получаем один вариант:

- $G \cong (\mathbb{Z}/2\mathbb{Z})^2 \leftthreetimes \mathbb{Z}/3\mathbb{Z} \cong A_4$

■

Задача 8. Разрешимы ли группы G: а) порядка $2p^k$, б) порядка $3p^k$, в) порядка $4p^k$.

Решение.
а) Из первой теоремы Силова следует, что в G есть подгруппа порядка p^k – она нормальна (как подгруппа наименьшего простого индекса). Имеем: N – разрешимая p-группа, $G/N \cong \mathbb{Z}/2\mathbb{Z}$ - разрешимая группа. Следовательно, и G разрешима.

б) Если $p > 3$, то рассуждения аналогичны случаю а) и G разрешима. Если $p = 2$, то найдем количество силовских 2-подгрупп: из третьей теоремы Силова следует, что их 1 или 3 штук. Если силовская 2-подгруппа единственна, то снова рассуждаем как в п. а) и получаем, что G разрешима. Если количество силовских 2-подгрупп равно трем, то рассмотрим действие G на этих группах: из второй теоремы Силова следует, что все силовские 2-подгруппы сопряжены, поэтому существует нетривиальный гомоморфизм $G \to S_3$, следовательно, его ядро – разрешимая подгруппа в G. Тогда и G разрешима (по индукции).

в) Из третьей теоремы Силова следует, что в G существует 1 или 4 силовских p-подгруппы. Если силовская p-подгруппа единственная, то она нормальна, и рассуждениями, аналогичными случаю а), получаем, что G разрешима. Если в G существует 4 силовских p-подгруппы, то рассмотрим действие G на этих группах: из второй теоремы Силова следует, что все силовские p-подгруппы сопряжены, поэтому существует нетривиальный гомоморфизм $G \to S_4$, следовательно, его ядро – разрешимая подгруппа в G. Тогда и G разрешима (по индукции). ■

Задача 9. Разрешима ли группа G порядка pq^2?

Решение.
Если $q > p$, то силовская q-подгруппа нормальна (как подгруппа наименьшего простого индекса) и G разрешима. Если $p > q$, то из третьей теоремы Силова следует, что в G может существовать 1, q, или q^2 силовских p-подгруппы. Если силовская p-подгруппа единственная, то она нормальна, и G разрешима. Если в G существует q силовских p-подгрупп, то $q - 1$ должно делиться на p – получаем противоречие с условием $p > q$.

Если в G существует q^2 силовских p-подгрупп, то в G существует $q^2(p-1)$ элементов порядка p, и q^2 элементов другого порядка, т.е. силовская q-подгруппа единственна, следовательно, нормальна, и G разрешима. ■

Семинар 11. Теоремы Силова. Разрешимость группы.

Разбор задач домашнего задания.

На семинаре 9 мы начали разбор задачи, в которой требовалось найти все разрешимые группы, порядок которых меньше 60. Мы выяснили, что разрешимыми будут группы, порядок которых равен p^k (так как их центр нетривиален) и группы, порядок которых равен pq где p, q – простые. Также на прошлом семинаре (см. задачи 8 и 9) мы выяснили, что разрешимыми будут группы, порядок которых равен pq^2 и $2p^k, 3p^k, 4p^k$. Закончим решение этой задачи.

Задача 1. Найти все разрешимые группы, порядок которых меньше 60.

Решение.
Осталось разобрать следующие случаи: $|G| = 30, 40, 42, 56$.

- $|G| = 40$. Пусть N_5 – количество силовских 5-подгрупп. Из третьей теоремы Силова следует, что $N_5 \equiv 1\ (mod\ 5)$ и $8 \vdots N_5$, т.е. $N_5 = 1$. Итак, силовская 5-подгруппа единственна, а значит, она нормальна, и G разрешима.
- $|G| = 56$. Пусть N_7 – количество силовских 7-подгрупп. Из третьей теоремы Силова следует, что $N_7 \equiv 1\ (mod\ 7)$ и $8 \vdots N_7$, т.е. либо $N_7 = 1$, либо $N_7 = 8$.
  Если силовская 7-подгруппа единственная, то она нормальна, и G разрешима.
  Если в G существует 8 силовских 7-подгрупп, то в G должно быть $8 \cdot 6 = 48$ элементов порядка 7 (так как в каждой 7-подгруппе 6 нетривиальных элементов, каждый из которых имеет порядок 7). Оставшиеся 8 элементов должны образовывать силовскую 2-подгруппу, которая будет единственной, а значит, нормальной, поэтому G разрешима.
- $|G| = 42$. Пусть N_7 – количество силовских 7-подгрупп. Из третьей теоремы Силова следует, что $N_7 \equiv 1\ (mod\ 7)$ и $6 \vdots N_7$, т.е. $N_7 = 1$. Итак, силовская 7-подгруппа единственна, а значит, она нормальна, и G разрешима.
- $|G| = 30$. Пусть N_5 – количество силовских 5-подгрупп. Из третьей теоремы Силова следует, что $N_5 \equiv 1\ (mod\ 5)$ и $6 \vdots N_5$, т.е. $N_5 = 1$, либо $N_5 = 6$.
  Пусть N_3 – количество силовских 3-подгрупп. Из третьей теоремы Силова следует, что $N_3 \equiv 1\ (mod\ 3)$ и $10 \vdots N_3$, т.е. $N_3 = 1$, либо $N_3 = 10$.
  Если $N_3 = 1$, либо $N_5 = 1$, то имеем единственную силовскую 3-подгруппу или единственную силовскую 5-подгруппу, которая нормальна, а следовательно, G разрешима. Осталось понять, что случай $N_3 = 10$, $N_5 = 6$ не может быть реализован, так как тогда в G должно быть $10 \cdot 2 = 20$ элементов порядка 3 и $6 \cdot 4 = 24$ элемента порядка 5, что невозможно, так как $20 + 24 > 30$. ■

Задача 2. Найти порядок силовской 2-подгруппы в S_n.

Решение.
Как известно, $|S_n| = n!$, поэтому порядок силовской 2-подгруппы в S_n – это наибольшая степень двойки, которая делит $n!$:

$$|G_2| = 2^{\left[\frac{n}{2}\right]+\left[\frac{n}{2^2}\right]+\cdots+\left[\frac{n}{2^k}\right]},$$

где $2^k \leq n \leq 2^{k+1}$.

Аналогично ищется порядок силовской p-подгруппы в S_n:

$$|G_p| = p^{\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^k}\right]},$$

где $p^k \leq n \leq p^{k+1}$. ■

Задача 3. Описать силовские 2-подгруппы в группах S_4, S_5, S_6, S_7, S_8.

Решение.

- S_4:

$|S_4| = 4! = 2^3 \cdot 3$. Пусть N_2 – количество силовских 2-подгрупп. Из третьей теоремы Силова следует, что $N_2 \equiv 1\ (mod\ 2)$ и $3 \vdots N_2$, т.е. $N_2 = 1$, либо $N_2 = 3$.

Докажем, что $N_2 = 3$: в самом деле, рассмотрим группу диэдра D_4. Как мы знаем, $|D_4| = 2^3 = 8$ и существует три естественных вложения $D_4 \hookrightarrow S_4$, каждое из которых соответствует нумерации вершин квадрата, указанной на рис. 11.1:

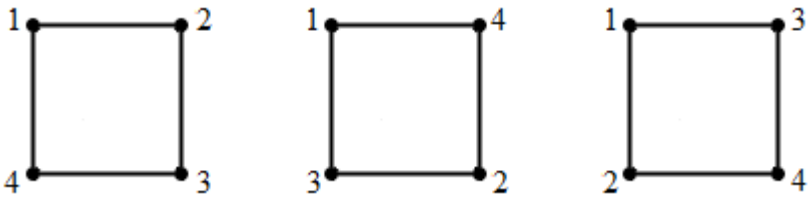

Рис. 11.1. Нумерации вершин квадрата, соответствующие различным вложениям $D_4 \hookrightarrow S_4$

Первая подгруппа порождается перестановками (1234) и (13), вторая подгруппа порождается перестановками (1423) и (12), третья подгруппа порождается перестановками (1342) и (14). Легко видеть, что эти три подгруппы попарно различны, так как каждая из них содержит разные элементы порядка 4.

Отметим, что необязательно было находить все силовские 2-подгруппы в S_4 явно (достаточно было найти одну, и вспомнить, что все силовские p-подгруппы сопряжены).

- S_5:

$|S_5| = 5! = 2^3 \cdot 3 \cdot 5$. Пусть N_2 – количество силовских 2-подгрупп. Из третьей теоремы Силова следует, что $N_2 \equiv 1\ (mod\ 2)$ и $15 \vdots N_2$, т.е. возможны варианты $N_2 = 1, 3, 5, 15$.

Докажем, что $N_2 = 15$: существует 5 способов вложить S_4 в S_5 (мы можем $C_5^4 = 5$ способами выбрать 4 элемента из 5, а пятый оставить неподвижным), при этом при каждом вложении мы получим 3 вложения $D_4 \hookrightarrow S_4$, каждое из которых соответствует силовской 2-подгруппе в S_5 (см. предыдущий пункт). Всего получаем $3 \cdot 5 = 15$ силовских 2-подгрупп в S_5.

- S_6:

$|S_6| = 6! = 2^4 \cdot 3^2 \cdot 5$. Так как любую 2-подгруппу можно вложить в силовскую 2-подгруппу (а в предыдущих пунктах мы выяснили, что в S_5 содержатся 2-подгруппы, изоморфные D_4), то каждая силовская 2-подгруппа в S_6 будет изоморфна группе $D_4 \times < e, (i\ j) >$, например, $< (1\ 2\ 3\ 4), (1\ 3), (5\ 6) >$.

Всего таких групп будет 45 – в самом деле, транспозицию $(i\ j)$ мы можем выбрать $C_6^2 = 15$ способами, а на оставшихся четырех номерах есть три 2-подгруппы, изоморфные D_4 (см. первый пункт задачи). Получаем $15 \cdot 3 = 45$ силовских 2-подгрупп в S_6.

- S_7:

$|S_7| = 7! = 2^4 \cdot 3^2 \cdot 5 \cdot 7$. Рассуждения аналогичны рассуждениям для S_5: существует 7 способов вложить S_6 в S_7, поэтому всего будет $7 \cdot 45 = 315$ силовских 2-подгрупп в S_7, все они будут устроены так же, как и в S_6.

- S_8:

$|S_8| = 8! = 2^7 \cdot 3^2 \cdot 5$. Попробуем рассмотреть группы вида $D_4 \times D_4$, которые действуют на непересекающихся четверках индексов: например, $< (1\ 2\ 3\ 4), (1\ 3) > \times < (5\ 6\ 7\ 8), (5\ 7) >$. Порядок такой группы равен 2^6, т.е. это не силовская 2-подгруппа в S_8, однако, группа

$$< (1\ 2\ 3\ 4), (1\ 3) > \times < (5\ 6\ 7\ 8), (5\ 7) > \rtimes < (15)(26)(37)(48) >$$

уже будет силовской 2-подгруппой в S_8.

Аналогичным образом можно описать, как устроена силовская 2-подгруппа в S_n. Далее, как мы знаем из теоремы Кэли, любую конечную группу порядка n можно вложить в S_n. Зададимся вопросом – для какого n существует вложение Q_8 в S_n (т.е. понятно, что по теореме Кэли Q_8 в S_8 вложить можно, но можно ли Q_8 вложить, например, в S_7)?

Оказывается, вложения не существует – ранее мы выяснили, как устроены силовские 2-подгруппы в S_7 – это $D_4 \times < e, (i\ j) >$, но в Q_8 шесть элементов порядка 4, а в $D_4 \times < e, (i\ j) >$ четыре элемента порядка 4, следовательно, вложения Q_8 в S_7 не существует. ■

Задача 4. Описать силовские p-подгруппы в группе S_{p^2} (p-простое).

Решение.
Из задачи 2 следует, что

$$|G_p| = p^{\left[\frac{p^2}{p}\right]+\left[\frac{p^2}{p^2}\right]+\cdots+\left[\frac{p^2}{p^k}\right]} = p^{p+1}$$

Вначале поймем, как построить группу порядка p^p: рассмотрим группу, состоящую из p циклов длины p:

$$< (1\ \cdots\ p), (p+1\ \cdots\ 2p), \cdots, (p^2-p+1\ \cdots\ p^2) >$$

- эта группа содержит p^p элементов (она изоморфна $(\mathbb{Z}/p\mathbb{Z})^p$). Теперь несложно понять, как получить группу порядка p^{p+1} (по аналогии с предыдущей задачей) – это

$$< (1\ \cdots\ p), (p+1\ \cdots\ 2p), \cdots, (p^2-p+1\ \cdots\ p^2) > \rtimes \sigma,$$

где $\sigma = (1\ p+1\ 2p+1\ \cdots\ p^2-p+1)(2\ p+2\ 2p+2\ \cdots\ p^2-p+2)\cdots(p\ 2p\ \cdots\ p^2)$, т.е. элемент, переставляющий элементы группы, состоящей из p циклов длины p, по кругу. Получаем группу, изоморфную $(\mathbb{Z}/p\mathbb{Z})^p \rtimes \mathbb{Z}/p\mathbb{Z}$. ■

Задача 9. а) Найти количество силовских 2-подгрупп в S_6.
б) Пусть G – подгруппа в S_6, $|G| = 48$. Доказать, что G содержит ровно три силовские 2-подгруппы.
в) Пусть G – подгруппа в S_6, $|G| = 48$. Доказать, что все такие подгруппы сопряжены.

Решение.
а) Мы уже получили решение этой задачи ранее (см. задачу 3): каждая силовская 2-подгруппа в S_6 будет изоморфна группе $D_4 \times < e, (i\ j) >$, например, $< (1\ 2\ 3\ 4), (1\ 3), (5\ 6) >$. Всего таких групп будет 45.

б) Пусть N_2 – количество силовских 2-подгрупп в G. Из третьей теоремы Силова следует, что $N_2 \equiv 1\ (mod\ 2)$ и $3 \vdots N_2$, т.е. $N_2 = 1$, либо $N_2 = 3$. Воспользуемся тем, что нормализатор силовской 2-подгруппы в S_6 совпадает с ней самой – значит, и нормализатор G совпадает с ней самой: $N_{S_6}(G) = G$. Следовательно, $N_2 = 3$.

В качестве примера подгруппы порядка 48 в S_6 можно привести, например, подгруппу $S_4 \times < (56) >$.

в) Из второй теоремы Силова следует, что все силовские 2-подгруппы в S_6 сопряжены. Как мы знаем из предыдущего пункта, если G – подгруппа в S_6, $|G| = 48$, то G содержит ровно три силовские 2-подгруппы – сопряжем G так, чтобы одна из входящих в нее силовских 2-подгрупп имела вид $G_2 = \mathbb{Z}_2 \times H$, где $H = < (12)(34), (13)(24), (14)(23), (56), (i\ j) >$.

Также в G есть подгруппа порядка 3 (следует из первой теоремы Силова), следовательно, в G есть элемент порядка 3 – обозначим его $(a\ b\ c)$. Осталось доказать, что $\{a, b, c\} \subset \{1,2,3,4\}$ – если мы это докажем, то докажем, что $G = \mathbb{Z}_2 \times S_4$ (так как добавление $(a\ b\ c)$ к порождающим элементам группы H даст S_4).

В самом деле, если $\{a, b, c\} \not\subset \{1,2,3,4\}$, то можно считать, что $(a\ b\ c) = (125)$ или $(a\ b\ c) = (156)$. В обоих случаях сопряжением при помощи этих перестановок перестановки (56) получаем перестановку (16). Далее, сопрягая (16) перестановками $(12)(34), (13)(24), (14)(23)$, получим перестановки $(26), (36), (46)$ соответственно. Но транспозиции $(16), (26), (36), (46), (56)$ порождают S_6, а $|S_6| \neq 48$ – противоречие. ■

Задача. Найти количество в A_5: а) силовских 2-подгрупп, б) силовских 3-подгрупп, в) силовских 5-подгрупп.

Решение.
$|A_5| = 5!/2 = 2^2 \cdot 3 \cdot 5$.

а) Пусть N_2 – количество силовских 2-подгрупп в A_5. Из третьей теоремы Силова следует, что $N_2 \equiv 1\ (mod\ 2)$ и $15 \vdots N_2$, т.е. возможны варианты $N_2 = 1, 3, 5, 15$.

б) Пусть N_3 – количество силовских 3-подгрупп в A_5. Из третьей теоремы Силова следует, что $N_3 \equiv 1\ (mod\ 3)$ и $20 \vdots N_3$, т.е. возможны варианты $N_3 = 1, 4, 10$.

в) Пусть N_5 – количество силовских 5-подгрупп в A_5. Из третьей теоремы Силова следует, что $N_5 \equiv 1\ (mod\ 5)$ и $12 \vdots N_5$, т.е. возможны варианты $N_5 = 1, 6$.

Варианты $N_2 = 1$, $N_3 = 1$, $N_5 = 1$ отпадают, так как в этом случае группы N_2, N_3, N_5 были бы нормальными, но A_5 – простая группа – противоречие. Таким образом, из третьей теоремы Силова сразу следует, что $N_5 = 6$.

Далее, в A_5 всего 20 циклов длины 3, а в каждой силовской 3-подгруппе в A_5 ровно два цикла длины 3, следовательно, $N_3 = 10$.

Так как $N_5 = 6$, а в каждой силовской 5-подгруппе в A_5 лежат 4 элемента порядка 5, то всего в A_5 будет $6 \cdot 4 = 24$ элемента порядка 5. Так как $N_3 = 10$, а в каждой силовской 3-подгруппе в A_5 лежат 2 элемента порядка 3, то всего в A_5 будет $10 \cdot 2 = 20$ элементов порядка 3. Остается $60 - (24 + 20) = 16$ элементов, которые будут лежать в 5 подгруппах порядка 4, т.е. $N_2 = 5$ (это несложно проверить, так как все силовские 2-подгруппы в A_5 сопряжены группе Клейна V_4). ■

Задача. Описать все подгруппы в S_5 (с точностью до сопряженности).

Решение.
Рассмотрим элементы порядка 5 в S_5. В каждой подгруппе в S_5 элементы порядка 5 либо отсутствуют, либо их ровно 4 (и они входят в силовскую 5-подгруппу), либо их 24 (см. предыдущую задачу – в A_5 24 элемента порядка 5).

Пусть N_5 – количество силовских 5-подгрупп в S_5. Из третьей теоремы Силова следует, что $N_5 \equiv 1 \ (mod\ 5)$ и $24 \vdots N_5$, т.е. возможны варианты $N_5 = 1, 6$. В предыдущей задаче мы выяснили, что в A_5 существует 6 силовских 5-подгрупп, значит, $N_5 = 6$.

Таким образом, любая подгруппа H в S_5 содержит либо все 6 силовских 5-подгрупп, либо ровно одну силовскую 5-подгруппу, либо вообще не содержит силовских 5-подгрупп, т.е. возможны следующие случаи:

- В H есть 6 силовских 5-подгрупп
- В H есть нормальная подгруппа $\mathbb{Z}/5\mathbb{Z}$
- Порядок H не делится на 5

1) Все элементы порядка 5 лежат в A_5 (см. предыдущую задачу), при этом они порождают A_5 (все элементы порядка 5 в S_5 сопряжены, поэтому если бы они входили в подгруппу, меньшую A_5, она была бы нормальной в A_5, но A_5 проста). Таким образом, получаем два варианта: $H = A_5$ и $H = S_5$.

2) Ранее (см. задача 6 семинар 9) мы описали нормализатор $< (12345) >$ в S_5. Его порядок равен 20, и $N_{S_5}(< (12345) >) \cong \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z} \cong < (12345), (2354) >$.

Все подгруппы H, содержащие нормальную подгруппу $\mathbb{Z}/5\mathbb{Z}$, будут подгруппами в $N_{S_5}(<(12345)>)$. Несложно видеть, что это $D_5 \cong <(12345),(25)(34)>$ и $\mathbb{Z}/5\mathbb{Z} \cong <(12345)>$.

3) Заметим, что если порядок H не делится на 5, то H не может действовать на номерах $1,2,3,4,5$ транзитивно (так как длина орбиты элемента должна делится на порядок H). Тогда либо $H \subset S_4$ (если найдется неподвижный элемент), либо $H \subset S_3 \times \mathbb{Z}/2\mathbb{Z}$ (если неподвижного элемента нет, то единственный вариант разбиения на орбиты – это орбиты длины 2 и 3).

Если $H \subset S_3 \times \mathbb{Z}/2\mathbb{Z}$, то либо $H = S_3 \times \mathbb{Z}/2\mathbb{Z}$, либо $H = S_3 \cong <(123),(23)(45)>$, либо $H = \mathbb{Z}/6\mathbb{Z} \cong <(123),(45)>$.

Если $H \subset S_4$, то нам осталось описать все группы в S_4. Пусть N_3 – количество силовских 3-подгрупп в S_4. Из третьей теоремы Силова следует, что $N_3 \equiv 1\ (mod\ 3)$ и $8 \vdots N_3$, т.е. $N_3 = 4$. Следовательно, в S_4 содержится 8 элементов порядка 3. Возможны следующие случаи:

- В H – 4 силовские 3-подгруппы,
- В H есть нормальная подгруппа $\mathbb{Z}/3\mathbb{Z}$,
- Порядок H не делится на 3.

1) Если H содержит все 4 силовские 3-подгруппы, то либо $H = A_4$, либо $H = S_4$.

2) Если в H есть нормальная подгруппа $\mathbb{Z}/3\mathbb{Z}$, то либо $H = S_3$, либо $H = \mathbb{Z}/3\mathbb{Z}$.

3) Если порядок H не делится на 3, то H – подгруппа в силовской 2-подгруппе в S_4, т.е. H – подгруппа в D_4. Ранее мы разбирали, как устроены подгруппы в D_4: всего есть 7 вариантов: либо $H = D_4$, либо $H = \mathbb{Z}/4\mathbb{Z}$, либо $H = V_4$, либо $H = (\mathbb{Z}/2\mathbb{Z})^2 \cong <(12),(34)>$, либо $H = <(12)>$, либо $H = <(12)(34)>$, либо $H = id$.

Подытожим: мы получили полную классификацию (с точностью до сопряженности) подгрупп в S_5:

- S_5
- A_5
- $D_5 \cong <(12345),(25)(34)>$
- $\mathbb{Z}/5\mathbb{Z} \cong <(12345)>$
- $S_3 \times \mathbb{Z}/2\mathbb{Z}$
- $S_3 \cong <(123),(23)(45)>$
- $\mathbb{Z}/6\mathbb{Z} \cong <(123),(45)>$

- S_4
- A_4
- S_3
- $\mathbb{Z}/3\mathbb{Z}$
- D_4
- $\mathbb{Z}/4\mathbb{Z}$
- V_4
- $(\mathbb{Z}/2\mathbb{Z})^2 \cong < (12), (34) >$
- $< (12) >$
- $< (12)(34) >$
- id

■

Задача. Доказать, что если $|G| = pq^3$, p, q – простые, то группа G разрешима.

Решение.
На прошлом семинаре (см. задачу 9) мы доказали, что всякая группа порядка pq^2 разрешима. Повторим некоторые рассуждения из решения той задачи.
Если $q > p$, то силовская q-подгруппа нормальна (как подгруппа наименьшего простого индекса) и G разрешима. Если $p > q$, то из третьей теоремы Силова следует, что в G может существовать 1, q, q^2 или q^3 силовских p-подгруппы. Получаем четыре случая:

- Если силовская p-подгруппа единственная, то она нормальна, и G разрешима.
- Если в G существует q силовских p-подгрупп, то $q - 1$ должно делиться на p – получаем противоречие с условием $p > q$.
- Если в G существует q^3 силовских p-подгрупп, то в G существует $q^3(p-1)$ элементов порядка p, и q^3 элементов другого порядка, т.е. силовская q-подгруппа единственна, следовательно, нормальна, и G разрешима.
- Если в G существует q^2 силовских p-подгрупп, то $q^2 - 1 = (q-1)(q+1)$ должно делиться на p. Так как $p > q$, то $q + 1$ должно делиться на p, что возможно лишь для случая $q = 2,\ p = 3$, т.е. для $|G| = 24$, но группа порядка 24 разрешима (см. предыдущий семинар, задачу 8 п. б)).

■

Отметим также, что верны следующие утверждения:

- Если $|G| = pq^k,\ p, q$ – простые, то группа G разрешима.
- Если $|G| = pqr,\ p, q, r$ – простые, то группа G разрешима.

Семинар 12. Кольца. Введение.

Приступим ко второй части нашего курса, в которой мы будем рассматривать кольца, поля, и другие алгебраические структуры.

Определение. Кольцо – это множество R с двумя бинарными операциями (сложением и умножением), для которых выполнены следующие аксиомы:

1) R – абелева группа относительно сложения,
2) умножение дистрибутивно:

$$a(b+c) = ab + ac$$
$$(b+c)a = ba + ca$$

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

Мы будем рассматривать ассоциативные кольца, т.е. $\forall a, b, c \in R$ потребуем выполнения условия $a(bc) = (ab)c$. В зависимости от дополнительных свойств умножения, выделяют разные классы колец: коммутативные, с единицей, и т.д.

Примеры колец.

1) $\mathbb{Z}$ (целые числа) – коммутативное, ассоциативное кольцо с единицей. $\mathbb{Z}$ не является полем, так как в нем лишь два обратимых элемента ± 1.

2) $\mathbb{Z}/n\mathbb{Z}$ (вычеты по модулю n) - коммутативное, ассоциативное кольцо с единицей. Если n – простое число, то $\mathbb{Z}/n\mathbb{Z}$ является полем.

3) $R[x_1, \dots, x_n]$ (многочлены от n переменных над полем R) – коммутативное, ассоциативное кольцо с единицей.

4) $\mathcal{F}(X, R)$ (функции на множестве X со значениями в поле R) – коммутативное, ассоциативное кольцо с единицей.

5) $Mat_{n\times n}(R)$ (матрицы $n \times n$ над полем R) – некоммутативное, ассоциативное кольцо с единицей.

Задача 1. Привести пример кольца без единицы.

Решение.

- $2\mathbb{Z}$ - четные числа,
- 0 – кольцо, которое содержит один элемент – 0.

Задача 2. Показать, что множества чисел вида $a + bi$, где $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ является кольцом.

Решение.
Следует непосредственно из определения. ■

Отметим, что при рассмотрении колец появляются новые понятия и объекты, не существовавшие в группах, например, делители нуля и нильпотенты.

Определение. Элемент a кольца R называется делителем нуля, если $\exists b \in R$, $b \neq 0$, такой что $ab = 0$ (в этом случае a называют левым делителем нуля), или $ba = 0$ (в этом случае a называют правым делителем нуля).

Определение. Элемент $a \neq 0$ кольца R называется нильпотентом, если $\exists n$: $a^n = 0$.

Например, матричная единица $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ является одновременно делителем нуля и нильпотентом в $Mat_{3\times 3}(\mathbb{R})$.

Также делители нуля и нильпотенты есть, например, в кольце $\mathbb{Z}/n\mathbb{Z}$ (если n не является простым числом). В самом деле, если у чисел a и n есть общий множитель, то вычет a будет делителем нуля в $\mathbb{Z}/n\mathbb{Z}$. Если в разложение a входят все простые множители, входящие в разложение n, то вычет a будет нильпотентом в $\mathbb{Z}/n\mathbb{Z}$.

Если же у чисел a и n нет общих множителей, то вычет a будет обратимым (в самом деле, из алгоритма Евклида следует, что найдутся $u, v \in \mathbb{Z}$, такие что $au + nv = 1$ – рассматривая это равенство по модулю n, получаем, что $au = 1$, т.е. у элемента a есть обратный).

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

Несложно заметить, что обратимые элементы всякого кольца образуют группу по умножению. Например:

- в кольце $\mathbb{R}[x]$ многочленов от одной переменных над полем $\mathbb{R}$ обратимыми элементами являются ненулевые константы, которые образуют группу по умножению $\mathbb{R}\backslash\{0\}$
- в кольце $\mathcal{F}(\mathbb{R}, \mathbb{R})$ функций из $\mathbb{R}$ в $\mathbb{R}$ обратимыми элементами являются функции, не обращающиеся в ноль ни в одной точке $\mathbb{R}$. Такие функции образуют группу по умножению. Функции же, обращающиеся в ноль хотя бы в одной точке $\mathbb{R}$, являются делителями нуля в $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

Определение. Поле – это коммутативное ассоциативное кольцо с единицей, в котором каждый ненулевой элемент обратим.

Примеры полей.

1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ – поля рациональных, действительных, комплексных чисел.

2) $\mathbb{Z}/n\mathbb{Z}$, n-простое число – поле вычетов по модулю n.

3) $K(x)$ – поле рациональных дробей от одной переменной.

4) Множество чисел вида $a + b\sqrt{2}$, где $a \in \mathbb{Q}$, $b \in \mathbb{Q}$.

Можно рассматривать некоммутативные поля (такие поля называются телами).

Определение. Тело – это ассоциативное кольцо с единицей, в котором каждый ненулевой элемент обратим.

Пример тела. $\mathbb{H}$ - тело кватернионов. Кватернионом называется выражение $q = a + bi + cj + dk$, где $a, b, c, d \in \mathbb{R}$, а i, j, k – кватернионные единицы, связанные соотношениями:

$$\begin{aligned} i^2 = j^2 = k^2 = -1, \\ ij = k, \quad ji = -k \\ jk = i, \quad kj = -i \\ ki = j, \quad ik = -j \end{aligned}$$

Модель тела кватернионов:

$$\mathbb{H} \cong \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\} \subset Mat_{2\times 2}(\mathbb{C})$$

Изоморфизм задается следующим соответствием:

$$1 \leftrightarrow E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad i \leftrightarrow I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad j \leftrightarrow J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad k \leftrightarrow K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Определение. Алгебра над полем K – это множество A с тремя операциями: сложение, умножение, умножение на элементы поля K (скаляры), для которых выполнены следующие аксиомы:

1) относительно сложения и умножения на скаляры, A – векторное пространство над K,
2) умножение билинейно, т.е. выполнены свойства:

- дистрибутивность:

$$a(b+c) = ab + ac$$
$$(b+c)a = ba + ca$$

- однородность: $\forall a, b \in A,\ \forall \lambda \in K$

$$(\lambda a)b = a(\lambda b) = \lambda(ab)$$

В частности, $\mathbb{H}$ – это алгебра над $\mathbb{R}$. Отметим также, что в $\mathbb{H}$ в качестве подполей содержатся поля $\mathbb{R}$ и $\mathbb{C}$ (причем $\mathbb{C}$ можно вложить в $\mathbb{H}$ не единственным образом).

Кватернионы являются примером т.н. гиперкомплексных чисел (т.е. конечномерных алгебр над $\mathbb{R}$ с единицей) – обобщением понятия комплексных чисел. Но если $\mathbb{C}$ - расширение $\mathbb{R}$, которое является полем (т.е. обладает свойствами и коммутативности, и ассоциативности), то $\mathbb{H}$ уже не обладает свойством коммутативности, а дальнейшее обобщение – октонионы $\mathbb{O}$ (алгебра Кэли) не обладает ни свойством коммутативности, ни свойством ассоциативности. Это алгебра над $\mathbb{R}$, состоящая из элементов вида $x = a + bi + cj + dk + el + fm + gn + ho$, где $a, b, c, d, e, f, g, h \in \mathbb{R}$, а i, j, k, l, m, n, o связаны соотношениями, запомнить которые (после соответствующей нумерации) помогает плоскость Фано (проективная плоскость над полем из двух элементов):

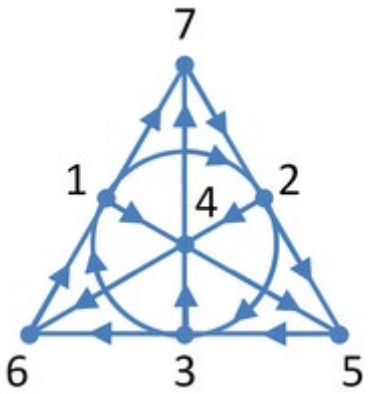

Рис. 12.1. Плоскость Фано для мнемонического запоминания таблицы умножения в $\mathbb{O}$

Определение. Пусть R – кольцо. Подкольцо – это подмножество R, замкнутое относительно операций сложения и умножения из R.

Примеры подколец.

1) $n\mathbb{Z}$ - подкольцо в $\mathbb{Z}$.

2) $\{k\bar{a}\}$ – подкольцо в $\mathbb{Z}/n\mathbb{Z}$, где $(a, n) > 1$, $k \in \mathbb{Z}$.

3) Многочлены $\{f \in \mathbb{R}[x] \mid f(x) = 0\}$ – подкольцо в $\mathbb{R}[x]$.

4) Многочлены с целыми (или рациональными) коэффициентами – подкольцо в $\mathbb{R}[x]$.

5) Дроби вида $\frac{a}{p^n}$ – подкольцо в $\mathbb{Q}$. Обратимыми элементами будут только $\pm p^k,\ k \in \mathbb{Z}$.

6) Дроби вида $\frac{a}{b}$, где $(b, p) = 1$ – подкольцо в $\mathbb{Q}$. Обратимыми элементами будут дроби $\frac{a}{b}$, где a не делится на p.

7) $\mathbb{Z}[i]$ – подкольцо в $\mathbb{C}$. Обратимые элементы: $\pm 1, \pm i$.

8) $\mathbb{Z}[\sqrt{2}]$ – подкольцо в $\mathbb{R}$. Обратимые элементы $a + b\sqrt{2}$ удовлетворяют равенству $a^2 - 2b^2 = \pm 1$.

Как и в теории групп, для сравнения разных алгебраических объектов, принадлежащих к одному классу, используется понятие гомоморфизма.

Определение. Гомоморфизм колец A и B – это отображение $f\colon A \to B$, для которого: $\forall x, y \in A$:

- $f(x + y) = f(x) + f(y)$
- $f(x \cdot y) = f(x) \cdot f(y)$

Для колец с единицей требуется выполнения еще одного условия (единица в A переходит в единицу в B):

$$f(1_A) = 1_B$$

Образ гомоморфизма:

$$Im\ f = \{b = f(a) \mid a \in A\}$$

Ядро гомоморфизма:

$$Ker\ f = \{a \in A \mid f(a) = 0\}$$

Для любого гомоморфизма колец $f\colon A \to B$ выполнено:

- $Im\ f \subseteq B$ – подкольцо
- $Ker\ f \lhd A$ – двусторонний идеал

Определение. Пусть A – кольцо. Идеалом в A называется подмножество $I \subseteq A$, для которого выполнено:

- I – подгруппа относительно сложения
- $A \cdot I \subseteq I$ – левый идеал,
  $I \cdot A \subseteq I$ – правый идеал.

Если идеал одновременно является левым и правым, то говорят, что он двусторонний. Обозначение для двустороннего идеала: $I \lhd A$.

Именно двусторонние идеалы являются полным аналогом нормальных подгрупп в теории групп. В коммутативном кольце все идеалы – двусторонние. Также идеал является подкольцом (при этом если $1 \in I$, то $I = A$).

Пример идеала. Рассмотрим $A = Mat_{n\times n}(K)$. Тогда

$$I = \{\text{матрицы, у которых все столбцы, кроме первого, нулевые}\}$$

– левый идеал (очевидно, что I – подгруппа в $Mat_n(K)$, и при умножении матрицы из I слева на произвольную матрицу из $Mat_{n\times n}(K)$ мы снова получим матрицу из I). Аналогично

$$I = \{\text{матрицы, у которых все строки, кроме первой, нулевые}\}$$

- правый идеал. Отметим, что двусторонних идеалов в алгебре матриц нет.

Факторкольцо.

В теории групп нормальные подгруппы используются для построения новых групп – мы можем строить по ним факторгруппы. Аналогичная конструкция есть и в теории колец.

Определение. Пусть A – кольцо, $I \lhd A$. Факторкольцо:

$$A/I = \{a + I \mid a \in A\}$$

- факторгруппа по сложению. Умножение смежных классов и умножение на скаляры определяется естественно: $\forall a, b \in A$:

- $(a + I) + (b + I) = (a + b) + I$
- $(a + I)(b + I) = ab + I$

Проверим корректность так заданного умножения смежных классов, т.е. что результат умножения не зависит от выбора представителей смежных классов: пусть

$$a + I = a' + I \Rightarrow a' = a + u,\ \ u \in I,$$
$$b + I = b' + I \Rightarrow b' = b + v,\ \ v \in I,$$

тогда

$$a'b' = (a + u)(b + v) = ab + av + ub + uv.$$

Здесь $av \in I,\ ub \in I, uv \in I$, значит и $av + ub + uv \in I$, то есть, $ab + I = a'b' + I$.

Примеры факторколец.

1) $n\mathbb{Z}$ - идеал в $\mathbb{Z}$. Получаем $\mathbb{Z}/n\mathbb{Z}$ - факторкольцо.

2) Рассмотрим (x) – идеал в $\mathbb{R}[x]$, порожденный элементом x. Этот идеал состоит из всех многочленов в $\mathbb{R}[x]$, которые делятся на x. Тогда $\mathbb{R}[x]/(x) \cong \mathbb{R}$ – факторкольцо (фактически мы каждому многочлену ставим в соответствие его значение в нуле, т.е. ставим в соответствие многочлену его остаток при делении на x). Аналогично $\mathbb{R}[x]/(x-2) \cong \mathbb{R}$ (каждому многочлену ставим в соответствие его остаток при делении на $x-2$).

Вообще, любой идеал в кольце многочленов от одной переменной можно породить одним элементом (такие идеалы называются главными). В самом деле, если количество порождающих больше одного, то применим к этим многочленам алгоритм Евклида. Несложно видеть, что получившийся многочлен будет лежать в идеале, также он будет порождать исходные многочлены. Кольцо, каждый идеал которого является главным, называется кольцом главных идеалов.

Рассмотрим $I = (x^n + \cdots)$ – идеал, порожденный многочленом степени n. Тогда $\mathbb{R}[x]/I$ будет состоять из элементов вида $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. Их сложение в $\mathbb{R}[x]/I$ определяется естественно, а умножение определяется в зависимости от вида многочлена $x^n + \cdots$. Например:

- В $\mathbb{R}[x]/(x^2)$ умножение определяется так:

$$(a + bx)(c + dx) = ac + (bc + ad)x$$

В $\mathbb{R}[x]/(x^2)$ есть нильпотенты: например, $x \cdot x = 0$

- В $\mathbb{R}[x]/(x^2 - 1)$ умножение определяется так:

$$(a + bx)(c + dx) = ac + bd + (ad + bc)x$$

В $\mathbb{R}[x]/(x^2 - 1)$ нильпотентов нет, но есть делители нуля: например, $(x-1)(x+1) = 0$

- В $\mathbb{R}[x]/(x^2 + 1)$ умножение определяется так:

$$(a + bx)(c + dx) = ac - bd + (ad + bc)x$$

В $\mathbb{R}[x]/(x^2 + 1)$ нет нильпотентов и делителей нуля. Отметим, что $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Вообще, факторизация $\mathbb{R}[x]$ по идеалу, порожденному неприводимым многочленом над $\mathbb{R}$, по сути означает добавление в $\mathbb{R}$ корней этого многочлена. Аналогично, например, $\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}(\sqrt{2})$.

Замечание. Ранее мы отметили, что любой идеал в кольце многочленов от одной переменной можно породить одним многочленов. Для кольца многочленов от многих переменных это утверждение неверно – например, в $\mathbb{R}[x,y]$ идеал (x,y) нельзя породить одним многочленом (т.о. $\mathbb{R}[x,y]$ не является кольцом главных идеалов).

Семинар 13. Идеалы в кольцах.

Сегодня мы будем говорить в основном о коммутативных кольцах.

Прямая сумма колец.

Определение. Пусть R_1, R_2 – кольца. Прямая сумма колец $R = R_1 \oplus R_2$ определяется как прямая сумма аддитивных групп R_1 и R_2: если $a, c \in R_1$ и $b, d \in R_2$, то

$$(a, b) + (c, d) = (a + c, b + d)$$

с умножением по правилу:

$$(a, b)(c, d) = (ac, bd)$$

Разбор задач домашнего задания.

Задача 1. Является ли кольцо $\mathbb{Z}[x]$ кольцом главных идеалов?

Решение.
Нет. Всякий идеал в этом кольце, порожденный одним многочленом, имеет вид $m\mathbb{Z}[x]$, $m \in \mathbb{Z}$. В качестве примера идеала, не имеющего такой вид, можно рассмотреть идеал, состоящий из многочленов с четным свободным членом:

$$(x, 2) = \{a_n x^n + \cdots a_1 x + 2a_0\} \neq \mathbb{Z}[x]$$

■

Задача 2. Описать, как устроены делители нуля в прямой сумме $\mathbb{C} \oplus \mathbb{C}$.

Решение.
Докажем, что все делители нуля в $\mathbb{C} \oplus \mathbb{C}$ имеют вид либо $(0, y)$, либо $(x, 0)$. В самом деле, пусть $(a, b)(c, d) = (ab, cd) = (0,0)$. Отсюда следует, что или $a = 0, d = 0$, или $b = 0, c = 0$. ■

Задачу 2 можно обобщить на случай произвольных колец. Для произвольных колец R_1 и R_2 делители нуля в $R_1 \oplus R_2$ имеют вид (a, b), где хотя бы один элемент из a и b – делитель нуля, или ноль (кроме элемента $(0,0)$ – это ноль в $R_1 \oplus R_2$, и он не является делителем нуля).

Отсюда, в частности, следует, что при гомоморфизме колец единица не всегда переходит в единицу – при вложении $R_1 \hookrightarrow R_1 \oplus R_2$ единица в R_1 переходит в делитель нуля в $R_1 \oplus R_2$ (который заведомо не может быть единицей в $R_1 \oplus R_2$). Чтобы 1 переходил в 1, нужно потребовать, чтобы гомоморфизм был сюръективен.

Кроме делителей нуля, для прямой суммы колец можно описать и другие важные типы элементов. Например, обратимые элементы в $R_1 \oplus R_2$ имеют вид (a, b), где a и b обратимы в R_1 и R_2 соответственно. Нильпотенты в в $R_1 \oplus R_2$ имеют вид (a, b), где a и b нильпотенты в R_1 и R_2 соответственно.

Посмотрим на примерах, как можно применять конструкцию прямой суммы для описания колец.

Задача 3. Доказать, что $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$, где n и m взаимно просты.

Решение.
Мы знаем, что $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ как абелевы группы, осталось разобраться с умножением. Так как n и m взаимно просты, то существуют u и v, такие что $1 = vn + um$. Домножая это равенство на произвольное $a \in \mathbb{Z}/nm\mathbb{Z}$, получим $a = avn + aum$, где $av \in \mathbb{Z}/m\mathbb{Z}$, а $au \in \mathbb{Z}/n\mathbb{Z}$. Выберем $a = n$, получим

$$n = vn^2 + unm = vn^2 \ (mod\ mn) \Longrightarrow vn = v^2n^2 \ (mod\ mn)$$

Аналогично, выбирая $a = m$, получаем $vm = v^2m^2 \ (mod\ mn)$. Учитывая полученные соотношения, получаем для произвольных $a = avn + aum$ и $b = bvn + bum$ из $\mathbb{Z}/nm\mathbb{Z}$:

$$(avn, aum)(bvn, bum) = (abvn, abum)$$

■

Задача 4. Рассмотрим $K[x]/(x^2 - 1)$, где K – произвольное поле. Доказать, что $K[x]/(x^2 - 1) \cong K \oplus K$.

Решение.
Вначале попробуем решить задачу “в лоб”. Напомним (см. прошлый семинар, случай $K = \mathbb{R}$), что умножение в $K[x]/(x^2 - 1)$определяется так:

$$(ax + b)(cx + d) = ac + bd + (ad + bc)x$$

Произвольные элементы $ax + b$ и $cx + d$ кольца $K[x]/(x^2 - 1)$ можно единственным образом представить в виде $ax + b = u(x - 1) + v(x + 1)$ и $cx + d = w(x - 1) + t(x + 1)$. Тогда

$$ax + b + cx + d = (u + w)(x - 1) + (v + t)(x + 1)$$

и

$$(ax + b)(cx + d) = \big(u(x - 1) + v(x + 1)\big)\big(w(x - 1) + t(x + 1)\big) =$$

$$= uw(x-1)^2 + vt(x+1)^2$$

Так как:

- $(x-1)^2 = x^2 - 2x + 1 = -2(x-1)\ mod\ (x^2-1)$,
- $(x+1)^2 = x^2 + 2x + 1 = 2(x+1)\ mod\ (x^2-1)$,

получаем

$$(ax+b)(cx+d) = 2uv(x-1) + 2vt(x+1)$$

- решение “в лоб” успеха не принесло. Будем действовать по аналогии с предыдущей задачей (считаем, что $char\ K \neq 2$): представим 1 в виде $1 = \frac{1}{2}(x+1) + (-\frac{1}{2})(x-1)$. Тогда, если мы произвольные элементы кольца $K[x]/(x^2-1)$ запишем в виде $a\frac{1}{2}(x+1) + b\left(-\frac{1}{2}\right)(x-1)$ и $c\frac{1}{2}(x+1) + d\left(-\frac{1}{2}\right)(x-1)$, то

$$\left(a\frac{1}{2}(x+1) + b\left(-\frac{1}{2}\right)(x-1)\right)\left(c\frac{1}{2}(x+1) + d\left(-\frac{1}{2}\right)(x-1)\right) =$$

$$= ac\frac{1}{4}(x+1)^2 + bd\frac{1}{4}(x-1)^2\ mod\ (x^2-1) =$$

$$= ac\frac{1}{2}(x+1) + bd\left(-\frac{1}{2}\right)(x-1)\ mod\ (x^2-1)$$

откуда следует, что $K[x]/(x^2-1) \cong K \oplus K$. ■

Задача 5. Рассмотрим $K[x]/(fg)$, где K – произвольное поле, многочлены f и g взаимно просты. Доказать, что $K[x]/(fg) \cong K[x]/(f) \oplus K[x]/(g)$.

Решение.
Так как $(f,g) = 1$, то существуют многочлены u и v, такие что $1 = u(x)f + v(x)g$. Далее, действуя как в задаче 3, получим, что $u(x)f = u(x)^2f^2\ mod\ (fg)$ и $v(x)g = v(x)^2g^2\ mod\ (fg)$, тогда

$$(au(x)f + bv(x)g)(cu(x)f + dv(x)g) = acu(x)^2f^2 + bdv(x)^2g^2\ mod\ (fg) =$$

$$= acu(x)f + bdv(x)g\ mod\ (fg)$$

Следовательно, $K[x]/(fg) \cong K[x]/(f) \oplus K[x]/(g)$. ■

В задачах 3-5 легко узнать различные модификации китайской теоремы об остатках. Продолжим решать подобные задачи.

Задача 6. Рассмотрим $\mathbb{F}_2[x]$ – кольцо многочленов над полем $\mathbb{F}_2$. Разложить в прямую сумму $\mathbb{F}_2[x]\,/\big(q(x)\big)$, где $\deg q(x) = 2$.

Решение.
Всего $\mathbb{F}_2[x]$ есть четыре многочлена второй степени: $x^2,\ x^2+x,\ x^2+1,\ x^2+x+1$.

- $q(x) = x^2 + x$. Так как $x^2 + x = x(x+1)$, мы можем воспользоваться результатом предыдущей задачи: $\mathbb{F}_2[x]/(x^2+x) \cong \mathbb{F}_2 \oplus \mathbb{F}_2$.
- $q(x) = x^2$. В $\mathbb{F}_2[x]/(x^2)$ четыре элемента: $0,\ 1,\ x,\ x+1$. Таблица умножения устроена следующим образом:

	0	**1**	$\boldsymbol{x}$	$\boldsymbol{x+1}$
0	0	0	0	0
1	0	1	x	$x+1$
$\boldsymbol{x}$	0	x	0	x
$\boldsymbol{x+1}$	0	$x+1$	x	1

- в прямую сумму разложить нельзя.

- $q(x) = x^2 + 1$. Так как в $\mathbb{F}_2[x]$ верно равенство $x^2 + 1 = (x+1)^2$, то этот случай заменой $x + 1 = t$ можно свести к предыдущему: $\mathbb{F}_2[x]/(x^2+1) \cong \mathbb{F}_2[x]/(x^2)$.
- $q(x) = x^2 + x + 1$. Так как многочлен $x^2 + x + 1$ неприводим над $\mathbb{F}_2$, то $\mathbb{F}_2[x]/(x^2+x+1)$ будет полем. В самом деле, построим таблицу умножения:

	0	**1**	$\boldsymbol{x}$	$\boldsymbol{x+1}$
0	0	0	0	0
1	0	1	x	$x+1$
$\boldsymbol{x}$	0	x	$x+1$	1
$\boldsymbol{x+1}$	0	$x+1$	1	x

- умножение коммутативно, ассоциативно, имеется единица и всякий элемент обратим. Поэтому $\mathbb{F}_2[x]/(x^2+x+1) \cong \mathbb{F}_4$. ■

Можно заметить некоторую закономерность (по аналогии с числами) – как кольцо вычетов по модулю простого числа было полем, так и факторкольцо по модулю неприводимого многочлена будет полем. Это не случайно.

Идеалы колец.

Определение. Идеал простой, если из условия $ab \in I$ следует, что $a \in I$ или $b \in I$.

Простой идеал в теории колец является обобщением простого числа. Теперь введем еще одно важное понятие теории колец – понятие максимального идеала.

Определение. В кольце с 1 идеал I называется максимальным, если не существует идеала I', такого что $I \subset I', I' \neq R$.

В приведенном определении условие наличия единицы в кольце важно, так как иначе не все максимальные идеалы будут простыми (что по многим причинам неудобно): например, в кольце $2\mathbb{Z}$ идеал $4\mathbb{Z}$ будет максимальным (если не требовать наличие 1 в кольце), но не будет простым (действительно, $2 \cdot 2 = 4 \in 4\mathbb{Z}$, но $2 \notin 4\mathbb{Z}$).

Итак, всякий максимальный идеал является простым (действительно, если бы он не был простым, то нашлись бы элементы $a, b \in I$, такие что $ab \in I$ но $a \notin I$ и $b \notin I$ – добавляя к I один из элементов a, b получили бы идеал, содержащий I, но не совпадающий с R). Но не всякий простой идеал является максимальным – например, в кольце $\mathbb{R}[x, y]$ идеал $I = (x)$ (множество многочленов от двух переменных, которые делятся на x) является простым, но $I \subset J(x, y), J \neq R$.

Характеристические свойства простых и максимальных идеалов.

- I – простой идеал $\Leftrightarrow R/I$ – без делителей нуля
- I – максимальный идеал $\Leftrightarrow R/I$ – поле

Доказательство.
1)
$\Rightarrow$: Пусть I – простой идеал, и $A, B \in R/I$ – делители нуля. Тогда для $a = f^{-1}(A)$, $b = f^{-1}(B)$ выполнено $a \notin I$ и $b \notin I$, но $ab \in I$ – противоречие. Значит, в R/I нет делителей нуля.

$\Leftarrow$: Пусть в R/I нет делителей нуля. Допустим, существуют $a, b \in I$, такие что $ab \in I$ но $a \notin I$ и $b \notin I$. Тогда для $A, B \in R/I$, где $A = f(a)$, $B = f(b)$, выполнено $AB = 0$ – противоречие, значит, I – простой идеал.

2)
$\Rightarrow$: Пусть I – максимальный идеал. Предположим, что R/I не является полем, т.е. существует необратимый $u \in R/I$. Рассмотрим $(u) \subset R/I$ – имеем: $f^{-1}(u)$ – идеал в R, и $I \subset f^{-1}(u)$ – противоречие. Значит, R/I – поле.

$\Leftarrow$: Пусть R/I – поле. Предположим, что $I \subset I', I' \neq R$. Тогда $f(I')$ – идеал в R/I (так как f – сюръективный гомоморфизм), но в поле не может существовать нетривиальный идеал – противоречие. ■

Например, рассмотренный выше идеал $J(x,y) \subset \mathbb{R}[x,y]$ является максимальным, так как $\mathbb{R}[x,y]/J(x,y) \cong \mathbb{R}$ - поле (это идеал, который соответствует вычислению значения многочлена из $\mathbb{R}[x,y]$ в точке $(0,0)$).

Вообще, если мы рассматриваем кольцо многочленов над алгебраически замкнутым полем, то любой максимальный идеал будет соответствовать вычислению значению многочлена из этого кольца в некоторой точке. Например, в $\mathbb{C}[x,y]$ максимальные идеалы имеют вид $(x-a, y-b)$. Простые идеалы в $\mathbb{C}[x,y]$ порождены неприводимыми многочленами – отметим, что во многих случаях они допускают “хорошую” геометрическую интерпретацию.

Семинар 14. Кольца главных идеалов.

Продолжим рассматривать коммутативные кольца (как правило, с единицей).

Разбор задач домашнего задания.

Задача 1. Объяснить, почему в определении максимального идеала важно условие наличия единицы в кольце. Привести пример кольца R без единицы, в котором идеал I будет максимальным (если не требовать наличие 1 в кольце), но не будет простым, и описать факторкольцо R/I.

Решение.
Как отмечалось на прошлом семинаре, в кольце $R = 2\mathbb{Z}$ идеал $I = 4\mathbb{Z}$ будет максимальным (если не требовать наличие 1 в кольце), но не будет простым (действительно, $2 \cdot 2 = 4 \in 4\mathbb{Z}$, но $2 \notin 4\mathbb{Z}$). При этом $R/I \ncong \mathbb{Z}/2\mathbb{Z}$ – в самом деле, R/I состоит из двух смежных классов: $4\mathbb{Z}$ и $4\mathbb{Z} + 2$, и умножение в этом факторкольце устроено не как в $\mathbb{Z}/2\mathbb{Z}$ (так как роль нуля играет $I = 4\mathbb{Z}$, но $(4\mathbb{Z} + 2)(4\mathbb{Z} + 2) = 4\mathbb{Z}$ – т.е. в этом кольце произведение любых двух элементов равно нулю). ■

Определение. Кольцо R, каждый идеал которого является главным, называется кольцом главных идеалов, т.е. $\forall I \subset R \ \exists a \in R\colon\ I = (a)$.

Кольца главных идеалов хороши тем, что в них простые идеалы – почти то же самое, что максимальные. Действительно, пусть $I = (p)$ – простой, но не максимальный идеал, тогда $I \subset (m)$ для некоторого $m \in R$, откуда следует, что $p = mu$. Так как $mu \in I$, и $m \notin I$, то $u \in I$, т.е. $u = kp$ для некоторого $k \in R$. Подставляя полученное равенство в равенство $p = mu$, получаем $p = mkp \Leftrightarrow (mk - 1)p = 0$. Возможны три варианта:

- $k = m^{-1}$ (т.е. m – обратимый элемент). Но тогда $R = (m)$ – получаем противоречие с определением максимального идеала
- $p = 0$, т.е. I – нулевой идеал
- $(mk - 1)$ или p являются делителями нуля

Мы будем рассматривать кольца главных идеалов, в которых нет делителей нуля. В таких кольцах всякий ненулевой простой идеал является максимальным.

Задача 2. Найти максимальные идеалы в кольце $\mathbb{R}[x]$ и описать факторкольца по ним.

Решение.
Как отмечалось на семинаре 12, кольцо $\mathbb{R}[x]$ является кольцом главных идеалов. Максимальные идеалы в $\mathbb{R}[x]$ имеют вид $I = (P(x))$, где $P(x)$ – неприводимый

многочлен. В самом деле: если $P(x) = A(x)B(x)$, то $P(x) \subset (A(x)) \neq \mathbb{R}[x]$, и обратно – если $P(x) \subset (A(x)) \neq \mathbb{R}[x]$, то $P(x) = A(x)B(x)$.

Теперь опишем, как устроено поле $\mathbb{R}[x]/(P(x))$. Факторизуя $\mathbb{R}[x]$ по многочлену степени d мы получаем векторное пространство размерности d (ставим в соответствие каждому элементу из $\mathbb{R}[x]$ его остаток при делении на данный многочлен степени d), т.е. абелева группа $\mathbb{R}[x]/(P(x))$ устроена как абелева группа соответствующего векторного пространства. Поймем, как там задается умножение.

Неприводимые многочлены над $\mathbb{R}$ имеют вид $x - a$ и $x^2 + px + q$, где $p^2 - 4q < 0$.

- $\mathbb{R}[x]/(x - a)$ задается отображением $P(x) \mapsto P(a)$, поэтому $\mathbb{R}[x]/(x - a) \cong \mathbb{R}$.
- Как уже отмечалось на семинаре 12, $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$. Любой многочлен вида $x^2 + px + q$, где $p^2 - 4q < 0$ можно соответствующей заменой привести к виду $t^2 + 1$ (на результат факторизации это не повлияет).

■

Описанная конструкция построения полей факторизацией кольца по идеалу, порожденному неприводимым многочленом, является универсальной. Например: рассмотрим в $\mathbb{Q}[x]$ идеал, порожденный неприводимым над $\mathbb{Q}$ многочленом $(x^2 - 2)$, тогда $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$. Если мы рассмотрим идеал, порожденный неприводимым над $\mathbb{Q}$ многочленом $(x^d - 2)$, то $\mathbb{Q}[x]/(x^d - 2) \cong \mathbb{Q}(\sqrt[d]{2})$.

Построение конечных полей.

В рассмотренных выше примерах идеалы использовались для построения бесконечных полей. Посмотрим, как с их помощью строить конечные поля.

Утверждение. Количество элементов в конечном поле равно степени некоторого простого числа.

Доказательство.
Пусть $\mathbb{F}$ – поле. Как известно, $char\ \mathbb{F} = 0$ или p, где p – простое (в самом деле, пусть $\underbrace{1 + \cdots + 1}_{mn \text{ слагаемых}} = 0$, тогда $0 = (\underbrace{1 + \cdots + 1}_{m \text{ слагаемых}})(\underbrace{1 + \cdots + 1}_{n \text{ слагаемых}})$, откуда следует, что $m = 1$, или $n = 1$, так как в поле нет делителей нуля).

Далее, если $char\ \mathbb{F} = p$, то $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \subset \mathbb{F}$ (так как 1 порождает $\mathbb{F}_p$). Заметим, что $\mathbb{F}$ является конечномерным векторным пространством над $\mathbb{F}_p$. Обозначим размерность этого векторного пространства d, тогда $|\mathbb{F}_p| = p^d$. ■

Пример. Построим поле $\mathbb{F}_4$.

Рассмотрим $\mathbb{F}_2[x]$ и найдем в нем неприводимые многочлены второй степени. В $\mathbb{F}_2[x]$ четыре многочлена второй степени: x^2, x^2+1, x^2+x, x^2+x+1, среди которых неприводим только x^2+x+1 (остальные имеют корни). Тогда

$$\mathbb{F}_2[x]\,/(x^2+x+1) \cong \mathbb{F}_4$$

■

Отметим, что для всякого d поле из p^d элементов существует, так как в $\mathbb{F}_p[x]$ найдутся неприводимые многочлены степени d. При этом все конечные поля одного порядка изоморфны друг другу. Конечные поля еще называются полями Галуа.

Определение. Кольцо R – евклидово, если существует отображение $N\colon\ R\backslash\{0\} \to \mathbb{N}$, такое что:

- 1) $N(a,b) \geq N(a)$, причем $N(a,b) = N(a) \Leftrightarrow b$ обратим,
- 2) Для любых $a, b \in R$, $b \neq 0$ найдутся q, r, такие что $a = bq + r$ и $N(b) > N(r)$ или $r = 0$.

Иными словами, кольцо R – евклидово, если в нем существует аналог алгоритма Евклида.

Задача 3. Найти все максимальные идеалы в кольце целых гауссовых чисел $\mathbb{Z}[i]$.

Решение.
Докажем, что кольцо $\mathbb{Z}[i]$ – евклидово. В качестве отображения N рассмотрим квадрат модуля: сопоставим каждому элементу $p+qi \in \mathbb{Z}[i]$ его норму $|p+qi|^2 = p^2+q^2 \in \mathbb{N}$. Пусть $a, b \in \mathbb{Z}[i]$ - покажем, как осуществляется деление a на b с остатком. Числа, кратные b (т.е. идеал, порожденный b) образуют подрешетку в $\mathbb{Z}[i]$:

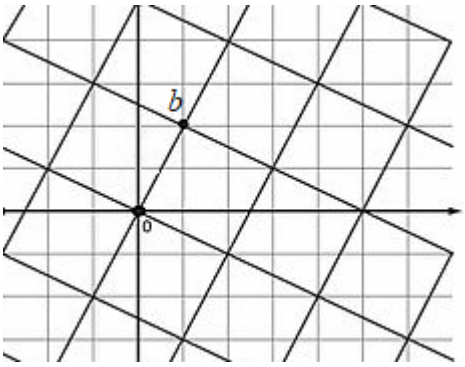

Рис. 14.1. Числа, кратные b, образуют подрешетку в $\mathbb{Z}[i]$

Число $a \in \mathbb{Z}[i]$ содержится в некотором квадрате этой подрешетки, и расстояние от a до некоторой вершины этого квадрата будет меньше стороны квадрата: $a - bq = r$, $|r| < |b|$. Таким образом, мы нашли q, r, такие что $a = bq + r$ и $N(b) > N(r)$ или $r = 0$.

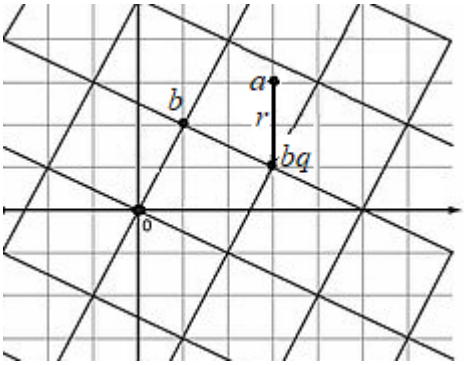

Рис. 14.2. Деление a на b с остатком в $\mathbb{Z}[i]$

Отметим важное свойство евклидовых колец: всякое евклидово кольцо является кольцом главных идеалов. В частности, $\mathbb{Z}[i]$ – кольцо главных идеалов, поэтому в $\mathbb{Z}[i]$ всякий ненулевой простой идеал является максимальным. Как устроены простые идеалы в $\mathbb{Z}[i]$ покажет следующее утверждение. ■

Утверждение. Пусть p простое. Доказать, что:

- Если $p = 2$, то идеал (p) не будет простым в $\mathbb{Z}[i]$
- Если $p = 4k + 1$, то идеал (p) не будет простым в $\mathbb{Z}[i]$
- Если $p = 4k + 3$, то идеал (p) будет простым в $\mathbb{Z}[i]$

Доказательство.
1) Если $p = 2$, то идеалу (p) будет соответствовать подрешетка (см. рис. 14.3, выделенная красным), содержащая другую подрешетку (см. рис. 14.3, выделена зеленым):

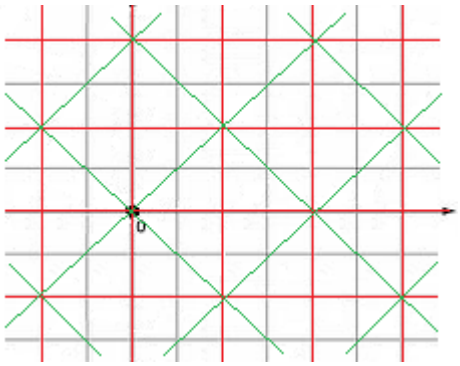

Рис. 14.3. Если $p = 2$, то идеал (p) не будет простым в $\mathbb{Z}[i]$

Т.е. 2 в кольце $\mathbb{Z}[i]$ не является простым числом, так как существует разложение $2 = (1 - i)(1 + i)$.

Пусть $p = 4k + 3$. $N(p) = |p|^2 = p^2$. Если $p = xy$, и x, y необратимы (т.е. $|x| \neq 1$, $|y| \neq 1$), то $|x||y| = |p|$ и $|x| = \sqrt{p} = |y|$. Но $\forall z = a + bi \in \mathbb{Z}[i]$ выполнено $|z| = \sqrt{a^2 + b^2}$. Прямым перебором получаем, что $\forall a, b \in \mathbb{Z}$ выполнено $a^2 + b^2 \equiv 0{,}1$ или $2\ (mod\ 4)$. Значит, если $p = 4k + 3$, то p нельзя представить в виде произведения элементов меньшей нормы, поэтому идеал (p) будет простым в $\mathbb{Z}[i]$. ■

Следствие. Если $p = 4k + 3$, то $\mathbb{Z}[i]/(p) \cong \mathbb{F}_{p^2}$.

Случай $p = 4k + 1$ мы разберем на следующем семинаре (см. задачу 3).

Семинар 15. Евклидовы кольца.

Разбор задач домашнего задания.

Задача 1. Построить поле из $3^3 = 27$ элементов.

Решение.
На прошлом семинаре мы обсуждали построение конечных полей – для построения поля из p^d элементов можно факторизовать кольцо многочленов над полем из p элементов по идеалу, порожденному неприводимым над этим полем многочленом степени d. В нашем случае в качестве такого многочлена можно выбрать $x^3 + x^2 + x - 1$ – он неприводим над $\mathbb{F}_3$, так как не имеет корней в $\mathbb{F}_3$. Получаем поле $\mathbb{F}_3[x]\,/(x^3 + x^2 + x - 1)$. ■

Задача 2. Доказать, что число 5 в $\mathbb{Z}[i]$ не является простым.

Решение.
Существует разложение 5 в $\mathbb{Z}[i]$ на два необратимых множителя: $5 = (2 + i)(2 - i)$. Множители $2 + i$ и $2 - i$ необратимы, так как модуль каждого из них больше 1. ■

Задача 3. Пусть p простое. Доказать, что если $p = 4k + 1$, то идеал (p) не будет простым в $\mathbb{Z}[i]$.

Решение.
Так как $\mathbb{Z}[i]$ – кольцо главных идеалов, и в нем всякий ненулевой простой идеал является максимальным, то достаточно показать, что (p) не будет максимальным в $\mathbb{Z}[i]$, т.е. что $\mathbb{Z}[i]/(p)$ не является полем.

Для этого докажем, что уравнение $x^2 + 1 = 0$ имеет в $\mathbb{Z}[i]/(p)$ более двух корней. Два корня очевидны – это $\pm i$. Далее, как известно, если p простое, то $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Так как по условию $p = 4k + 1$, то $p - 1$ делится на 4, т.е. $\exists a \in (\mathbb{Z}/p\mathbb{Z})^*$: $a^4 = 1\ (mod\ p)$ т.е. $\exists a \in (\mathbb{Z}/p\mathbb{Z})^*$: $a^2 = -1$. Так как $\mathbb{Z}/(p) \subset \mathbb{Z}[i]/(p)$, то уравнение $x^2 + 1 = 0$ будет иметь корни $\pm a$ в $\mathbb{Z}[i]/(p)$, т.е. должно выполняться равенство $a^2 + 1 = (a + i)(a - i) = 0$, т.е. в $\mathbb{Z}[i]/(p)$ есть делители нуля, и $\mathbb{Z}[i]/(p)$ не является полем.

Отметим, что если $p = 4k + 1$ и в $\mathbb{Z}[i]$ p раскладывается как $p = q_1 q_2$, то $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(q_1) \oplus \mathbb{Z}[i]/(q_2) \cong \mathbb{F}_p \oplus \mathbb{F}_p$. ■

Представление числа в виде суммы дух квадратов.

Итак, теперь мы полностью доказали утверждение, сформулированное в конце прошлого семинара: пусть p простое, тогда:

- Если $p = 2$, то идеал (p) не будет простым в $\mathbb{Z}[i]$
- Если $p = 4k + 1$, то идеал (p) не будет простым в $\mathbb{Z}[i]$
- Если $p = 4k + 3$, то идеал (p) будет простым в $\mathbb{Z}[i]$

Из этого утверждения можно получить красивые следствия. Пусть $p = 4k + 1$, тогда идеал (p) – не простой в $\mathbb{Z}[i]$, а значит, и не максимальный в $\mathbb{Z}[i]$. Пусть $(p) \subset (m)$, где (m) – максимальный идеал в $\mathbb{Z}[i]$, тогда $mm' = p$. Если $m = a + bi$, $m' = c + di$, то

$$mm' = (a + bi)(c + di) = (ac - bd) + (ad + bc)i \Longrightarrow \begin{cases} ac - bd = p \\ (ad + bc)i = 0 \end{cases}$$

Так как произведение двух комплексных чисел $m = a + bi$ и $m' = c + di$ дает действительное число p, то их аргументы противоположны, т.е. $m' = k(a - bi)$ для некоторого $k \in \mathbb{R}$, откуда следует, что $c = ak, d = -bk$. Учитывая это, получаем, что

$$mm' = ac - bd = k(a^2 + b^2) = p$$

Отсюда следует, что $k = 1$, тогда $a^2 + b^2 = p$. Таким образом, мы получили, что любое простое число, сравнимое с 1 по модулю 4, представляется в виде суммы двух квадратов. Подытожим:

- Если $p = 2$, то p можно представить в виде суммы двух квадратов: $2^2 = 1^2 + 1^2$
- Если $p = 4k + 1$, то p можно представить в виде суммы двух квадратов
- Если $p = 4k + 3$, то p нельзя представить в виде суммы двух квадратов (так как сумма двух квадратов не может дать остаток 3 при делении на 4)

Теперь поймем, когда произвольное натуральное число можно представить в виде суммы двух квадратов. Заметим, что произведение двух чисел, представимых в виде суммы двух квадратов, тоже можно представить в виде суммы двух квадратов (см. тождество Брахмагупты):

$$(a^2 + b^2)(c^2 + d^2) = (ax + by)^2 + (bx - ay)^2$$

Отсюда следует, что всякое число $N \in \mathbb{N}$, в разложение которого на простые множители входят только 2 и простые числа вида $p = 4k + 1$, можно представить в виде суммы двух квадратов.

Пусть теперь $n = uq$, где q – простое, $q = 4k + 3$. Докажем, что n нельзя представить в виде суммы двух квадратов, если q входит в разложение n нечетное число раз. Для этого рассмотрим равенство $n = a^2 + b^2$ по модулю q: получим $0 = a^2 + b^2$.

Как мы знаем, если q простое, то $(\mathbb{Z}/q\mathbb{Z})^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$, т.е. порядок группы $(\mathbb{Z}/q\mathbb{Z})^*$ равен $4k+2$ и в нем нет элементов порядка 4 (так как порядок элемента делит порядок группы): $\forall a \in (\mathbb{Z}/q\mathbb{Z})^*\colon\ a^4 \neq 1\ (mod\ q) \Longrightarrow \forall a \in (\mathbb{Z}/q\mathbb{Z})^*\colon\ a^2 \neq -1\ (mod\ q)$.

Следовательно, уравнение $0 = a^2 + b^2 \Leftrightarrow 0 = 1 + (ba^{-1})^2$ имеет решение только если $a = 0\ (mod\ q)$ и $b = 0\ (mod\ q)$, т.е. a^2 делится на q^2 и b^2 делится на q^2, откуда следует, что $n = a^2 + b^2$ делится на q^2. Разделим равенство $n = a^2 + b^2$ на q^2 и снова применим наше рассуждение, и так далее – в итоге мы либо найдем представление n в виде суммы двух квадратов, либо придем к противоречию (когда множитель вида $q = 4k+3$ будет входить в разложение в первой степени).

Подытожим: пусть $N \in \mathbb{N}$, тогда $N = a^2 + b^2$ для некоторых целых a и b тогда и только тогда, когда:

$$N = 2^{\alpha} \prod_{\substack{p=4k+1,\\ p-\text{простое}}} p^{\beta_p} \prod_{\substack{q=4k+3,\\ q-\text{простое}}} q^{2\gamma_q}$$

Задача 4. Доказать, что кольцо $\mathbb{Z}[\omega]$, где $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ является факториальным (элементы этого кольца еще называют числами Эйзенштейна).

Решение.
Докажем, что $\mathbb{Z}[\omega]$ евклидово (из чего следует, что $\mathbb{Z}[\omega]$ факториально). Как и в случае гауссовых чисел (см. предыдущий семинар) в качестве нормы N рассмотрим квадрат модуля: пусть $z = a + b\omega = a + b\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$, тогда

$$|a + b\omega|^2 = \left(a - \frac{b}{2}\right)^2 + \left(b\frac{\sqrt{3}}{2}\right)^2 = a^2 - ab + b^2 \in \mathbb{N}$$

$\mathbb{Z}[\omega]$ образует треугольную решетку в $\mathbb{C}$:

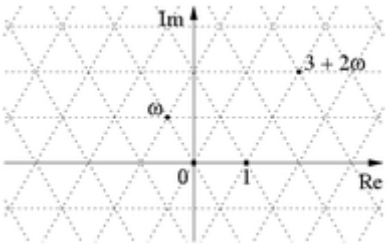

Рис. 15.1. $\mathbb{Z}[\omega]$ образует треугольную решетку в $\mathbb{C}$

Деление чисел Эйзенштейна с остатком проводится аналогично делению с остатком гауссовых чисел (см. предыдущий семинар, задачу 3) с той лишь разницей, что теперь элементами решетки будут не квадраты, а треугольники.

Итак, $\mathbb{Z}[\omega]$ евклидово, следовательно, $\mathbb{Z}[\omega]$ факториально. ■

Задача 5. Доказать, что кольцо $\mathbb{Z}[i\sqrt{3}]$ не является факториальным.

Решение.
Существует два разложения 4 в $\mathbb{Z}[i\sqrt{3}]$ на множители: $4 = 2 \cdot 2$ и $4 = (1 - i\sqrt{3})(1 + i\sqrt{3})$. Докажем, что множители $2,\ 1 - i\sqrt{3}$ и $1 + i\sqrt{3}$ необратимы в $\mathbb{Z}[i\sqrt{3}]$.

Норма в $\mathbb{Z}[i\sqrt{3}]$: $N\left(a + ib\sqrt{3}\right) = a^2 + 3b^2$. Допустим, существует разложение $2 = \omega_1\omega_2$, тогда $4 = N(2) = N(\omega_1)N(\omega_2)$. Отсюда следует, что либо $N(\omega_1) = 1$, либо $N(\omega_2) = 1$, т.е. какой-то из элементов ω_1 и ω_2 обратим (вариант $N(\omega_1) = 2$ или $N(\omega_2) = 2$ невозможен, так как $a^2 + 3b^2 \neq 2$ для целых a, b).

Для $1 - i\sqrt{3}$ и $1 + i\sqrt{3}$ рассуждения аналогичны (так как норма этих чисел тоже равна 4). Таким образом, числа $2,\ 1 - i\sqrt{3}$ и $1 + i\sqrt{3}$ необратимы в $\mathbb{Z}[i\sqrt{3}]$, поэтому кольцо $\mathbb{Z}[i\sqrt{3}]$ не является факториальным. ■

Мы доказали, что $\mathbb{Z}[i\sqrt{3}]$ не факториально, в частности, не евклидово – в нем нельзя делить с остатком, так как $\mathbb{Z}[i\sqrt{3}]$ образует прямоугольную решетку в $\mathbb{C}$, и расстояние от центра прямоугольника решетки до его вершин будет таким же, как и его меньшая сторона (т.е. равно 1) – остаток будет не меньше делителя.

До этого мы рассматривали деление с остатком в коммутативных кольцах, теперь посмотрим, что будет в некоммутативных – например, можно ли делить с остатком в кольце кватернионов. Рассмотрим в $\mathbb{H}$ целочисленную решетку кватернионов вида $q = a + bi + cj + dk$, где $a, b, c, d \in \mathbb{Z}$. Это решетка в четырехмерном пространстве, где фундаментальными областями являются четырехмерные кубы. Делить с остатком в этом кольце нельзя (так как расстояние от центра четырехмерного единичного куба до его вершин равно 1 – ситуация аналогична кольцу $\mathbb{Z}[i\sqrt{3}]$).

Однако, если мы добавим к кольцу $\mathbb{Z}[i\sqrt{3}]$ середины прямоугольников, то получим уже знакомое нам кольцо $\mathbb{Z}[\omega]$, образующую треугольную решетку в $\mathbb{C}$, в котором можно делить с остатком. Точно так же к решетке, состоящей из четырехмерных кубов, можно добавить середины этих кубов, т.е. числа вида $q = a + bi + cj + dk$, где a, b, c, d – полуцелые одновременно. Получившееся кольцо хотя и не будет коммутативным, но в

нем уже можно делить с остатком, а значит, можно провести рассуждения, аналогичные нашим рассуждениям о представлении натуральных чисел в виде двух квадратов, и разобраться с вопросом о представлении числа в виде суммы четырех квадратов.

Поля.

Перейдем к рассмотрению полей. Ранее (см. семинар 12) мы давали определение поля и приводили некоторые примеры полей:

Определение. Поле – это коммутативное ассоциативное кольцо с единицей, в котором каждый ненулевой элемент обратим.

Также можно сказать, что поле $\mathbb{K}$ – это абелева группа по сложению и умножению, для которых выполнено свойство дистрибутивности: $a(b+c) = ab + ac, \forall a, b, c \in \mathbb{K}$.

Примеры полей.

1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ – поля рациональных, действительных, комплексных чисел

2) $\mathbb{Z}/n\mathbb{Z}$, n-простое число – поле вычетов по модулю n

3) $\mathbb{K}(x)$ – поле рациональных дробей от одной переменной

4) $\mathbb{K}(\sqrt{a})$, где $\mathbb{K}$ – поле, a – не квадрат в $\mathbb{K}$

Семинар 16. Поля. Введение.

Первое знакомство с полями.

Приведем еще несколько примеров полей:

- $\overline{\mathbb{Q}}$ – поле алгебраических чисел (его элементы – числа, являющиеся корнями многочленов с рациональными коффициентами)
- $\mathbb{Q}(x)$ – поле рациональных функций (его элементы – рациональные дроби $\frac{P(x)}{Q(x)}$, где $P(x), Q(x) \in \mathbb{Q}[x]$, при этом $\frac{P_1(x)}{Q_1(x)} = \frac{P_2(x)}{Q_2(x)} \Leftrightarrow P_1(x)Q_2(x) = P_2(x)Q_1(x)$
- $\mathbb{F}_p$ – поле из p элементов. Если p простое, $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$

Определение. Наименьшее $n \in \mathbb{N}$: $\underbrace{(1 + \cdots + 1)}_{n \text{ слагаемых}} = 0$, называется характеристикой поля (обозначение: $char\ \mathbb{K}$). Если такого $n \in \mathbb{N}$ не существует, то полагаем $char\ \mathbb{K} = 0$.

- Всякое конечное поле имеет положительную характеристику (так как поле конечно, то найдутся различные k, m, такие что $\underbrace{(1 + \cdots + 1)}_{k \text{ слагаемых}} = \underbrace{(1 + \cdots + 1)}_{m \text{ слагаемых}}$, тогда $\underbrace{(1 + \cdots + 1)}_{k-m \text{ слагаемых}} = 0$).
- Если $char\ \mathbb{K} > 0$, то $char\ \mathbb{K}$ – простое число. В самом деле, пусть $\underbrace{1 + \cdots + 1}_{km \text{ слагаемых}} = 0$, тогда $0 = \underbrace{(1 + \cdots + 1)}_{k \text{ слагаемых}}\underbrace{(1 + \cdots + 1)}_{m \text{ слагаемых}}$, откуда следует, что $k = 1$, или $m = 1$, так как в поле нет делителей нуля.
- Всякое поле характеристики 0 содержит $\mathbb{Q}$ в качестве подполя, а всякое поле характеристики $p > 0$ содержит $\mathbb{F}_p$ в качестве подполя.

Построение конечных полей.

Ранее (см. семинар 14) мы уже обсуждали построение конечных полей с помощью факторизации кольца многочленов по идеалу, порожденному неприводимым многочленом, в частности, построили поле $\mathbb{F}_4$. Сделаем это снова, но уже не используя факторизацию.

Пример. Построим поле $\mathbb{F}_4$.

Так как поле – абелева группа по сложению, то порядок всякого элемента должен делить порядок поля. Но характеристика поля – простое число, поэтому порядок всякого элемента должен быть простым делителем порядка поля. В нашем случае получаем $char\ \mathbb{F}_4 = 2$. Таким образом, $\mathbb{F}_4 \supset \mathbb{F}_2$.

Построим таблицу сложения в $\mathbb{F}_4$. Теоретически возможны два варианта: либо $\mathbb{F}_4$ устроено как $\mathbb{Z}/4\mathbb{Z}$, либо как $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Нетрудно убедиться, что имеет место второй вариант. Обозначим a элемент в $\mathbb{F}_4$, который не равен 0 и 1, тогда:

+	**0**	**1**	***a***	***a* + 1**
0	0	1	a	$a+1$
1	1	0	$a+1$	a
a	a	$a+1$	0	1
***a* + 1**	$a+1$	a	1	0

Таблица умножения:

*	**0**	**1**	***a***	***a* + 1**
0	0	0	0	0
1	0	1	a	$a+1$
a	0	a	$a+1$	1
***a* + 1**	0	$a+1$	1	a

- из таблицы умножения следует, что $a^2 = a + 1$, что в поле характеристики 2 равносильно равенству $a^2 + a + 1 = 0$. Таким образом, мы еще раз убедились, что $\mathbb{F}_2[x]/(x^2 + x + 1) \cong \mathbb{F}_4$ – результат, который мы получили на семинаре 14.

Определение. Пусть L – поле, $L \supset K$ – поле, и операции в L и K устроены одинаково. Тогда говорят, что K – подполе в L, а L – расширение поля K.

Утверждение. Пусть L – поле, $L \supset K$ – подполе. Тогда L – векторное пространство над K.

Доказательство этого утверждения тривиально (все аксиомы векторного пространства следуют из того, что L – поле), но из него вытекает важное следствие.

Следствие. Пусть $\mathbb{F}$ – конечное поле. Тогда $|\mathbb{F}| = p^n$ для некоторого простого p и $n \in \mathbb{N}$.

Доказательство.
Так как $\mathbb{F}$ конечно, то $\mathbb{F} \supseteq \mathbb{F}_p$ – конечное расширение полей. Обозначим $(\mathbb{F}: \mathbb{F}_p) = n$. Тогда $\mathbb{F} \cong (\mathbb{F}_p)^n$ как векторное пространство над $\mathbb{F}_p$ – этот изоморфизм задается выбором базиса в $\mathbb{F}$ над полем $\mathbb{F}_p$. Следовательно, $|\mathbb{F}| = |(\mathbb{F}_p)^n| = p^n$. ■

Пример. Построим поле $\mathbb{F}_8$.

Чем больше порядок поля, тем сложнее задавать его с помощью таблиц (как мы это сделали в случае $\mathbb{F}_4$). Воспользуемся тем, что $\mathbb{F}_8$ – трехмерное векторное пространство над $\mathbb{F}_2$ – для построения базиса $\mathbb{F}_8$ нужно найти три линейно независимых вектора над $\mathbb{F}_2$.

Обозначим a элемент $\mathbb{F}_8$, который не равен 0 и 1. Четыре элемента $\mathbb{F}_8$ нам уже известны: это $0, 1, a, a+1$ – посмотрим, что будет, если возвести a в квадрат:

- $a^2 \neq 0$, так как в поле нет делителей нуля
- $a^2 \neq 1 \Leftrightarrow (a-1)(a+1) \neq 0$, так как в поле нет делителей нуля
- $a^2 \neq a \Leftrightarrow a(a-1) \neq 0$, так как в поле нет делителей нуля
- $a^2 \neq a+1 \Leftrightarrow a^2+a+1 \neq 0$, так как в противном случае $\mathbb{F}_8$ содержало бы $\mathbb{F}_4$ в качестве подполя (см. построение $\mathbb{F}_4$ выше), но это невозможно – тогда бы $\mathbb{F}_8$ было векторным пространством над $\mathbb{F}_4$, и порядок $\mathbb{F}_8$ должен был быть равен степени четверки

Таким образом, a^2 – еще один элемент поля $\mathbb{F}_8$, и мы нашли три линейно независимых вектора над $\mathbb{F}_2$ – это $1, a, a^2$. Получаем, что $\mathbb{F}_8$ состоит из следующих элементов:

$$\mathbb{F}_8 = \{0,\ \ 1,\ \ a,\ \ a+1,\ \ a^2,\ \ a^2+1,\ \ a^2+a+1\}$$

Для задания таблицы умножения осталось понять, чему равно a^3. Несложным перебором получаем, что возможны два варианта: $a^3 = a+1$ и $a^3 = a^2+1$. Итак:

$$\mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3+x+1) \cong \mathbb{F}_2[x]/(x^3+x^2+1)$$

Поля $\mathbb{F}_2[x]/(x^3+x+1)$ и $\mathbb{F}_2[x]/(x^3+x^2+1)$ изоморфны, так как в $\mathbb{F}_2[x]$ многочлены x^3+x+1 и x^3+x^2+1 получаются друг из друга заменой переменной. На самом деле, все поля одного порядка изоморфны друг другу – этот результат мы докажем чуть позже.

Пример. Построим бесконечное поле положительной характеристики.

До сих пор мы сталкивались с двумя случаями: бесконечными полями характеристики 0 и конечными полями положительной характеристики. Мы знаем, что нет конечных полей характеристики 0. А бывают ли бесконечные поля положительной характеристики?

Оказывается, бывают – например, поле $\mathbb{F}_2(x)$, состоящее из дробей $\frac{P(x)}{Q(x)}$, где $P(x), Q(x) \in \mathbb{F}_2[x]$ является примером бесконечного поля характеристики 2 (понятно, что это универсальный пример и $\mathbb{F}_p(x)$ – бесконечное поле характеристики p). Такая конструкция называется полем частных.

Расширение полей.

На предыдущих семинарах мы сталкивались с расширениями двух типов:

- добавление к полю корня многочлена, неприводимого над этим полем (например, $\mathbb{Q}(\sqrt{2})$ – расширение поля $\mathbb{Q}$)
- добавление к полю переменной (например, $\mathbb{F}_2(x)$ – расширение поля $\mathbb{F}_2$)

Определение. Пусть $L \supset K$ – расширение полей. Тогда элемент $a \in L$ – алгебраический (над K), если существует ненулевой аннулирующий многочлен $P(x) \in K[x]$, такой что $P(a) = 0$. В противном случае элемент a называют трансцендентным.

Определение. Расширение полей $L \supset K$ называется конечным, если L конечномерно над K (как векторное пространство): $dim_K L < \infty$. Степень расширения $(L: K) = dim_K L$.

Утверждение. Всякий элемент в конечном расширении – алгебраический.

Доказательство.
Пусть $L \supset K$ – конечное расширение полей и $a \in L$. Рассмотрим последовательность $1, a, a^2, a^3, \ldots$ Так как L – конечномерное векторное пространство над K, то $\exists k$: $1, a, \ldots, a^k$ – линейно зависимы над K, т.е. существует их нетривиальная линейная комбинация $c_0 + c_1 a + \cdots + c_k a^k = 0$ – нашли аннулирующий многочлен для a, значит, a – алгебраический над K. ■

Если расширение полей $L \supset K$ не является конечным, то не всякий элемент L является алгебраическим.

Примеры трансцендентных элементов.

- Пусть $\mathbb{K}$ – поле. Рассмотрим $\mathbb{K}(x)$ – поле рациональных функций над $\mathbb{K}$. Тогда x – неалгебраический (трансцендентный) элемент над $\mathbb{K}$
- Рассмотрим расширение $\mathbb{R} \supset \mathbb{Q}$. Число π – трансцендентный элемент над $\mathbb{Q}$

Алгебраические элементы образуют подполе. Например, докажем, что элемент $\sqrt{2} + \sqrt{3}$ будет алгебраическим над $\mathbb{Q}$: пусть $\sqrt{2} + \sqrt{3} = x$, тогда $x^2 = 5 + 2\sqrt{6} \Leftrightarrow x^2 - 5 = 2\sqrt{6}$, откуда $x^4 - 10x^2 + 1 = 0$. Таким образом, $x^4 - 10x^2 + 1$ – аннулирующий многочлен для $\sqrt{2} + \sqrt{3}$, т.е. элемент $\sqrt{2} + \sqrt{3}$ алгебраичен над $\mathbb{Q}$.

Гомоморфизмы полей.

Определение. Гомоморфизм полей K и L – это отображение $f: K \to L$, для которого: $\forall a, b \in K$:

- $f(a+b) = f(a) + f(b)$
- $f(a \cdot b) = f(a) \cdot f(b)$

Из основной теореме о гомоморфизме для колец следует, что $Im\, f \cong K/I$, где $I = Ker\, f$. Но поле содержит всего два идеала: $I = (0)$ и $I = K$. Случай $I = K$ бессодержателен, остается вариант $I = (0)$, который означает, что f является вложением, и K – подполе в L. Если $K = L$, то получаем отображение поля в себя.

Определение. Автоморфизм поля – это его изоморфизм на себя: $f\colon K \to K$ – гомоморфизм, $Im\, f = K$.

Автоморфизмы поля K образуют группу $Aut(K)$.

Примеры автоморфизмов полей.

1) В $\mathbb{C}$ определены операции сложения и умножения комплексных чисел:

- $(a+bi) + (c+di) = (a+c) + (b+d)i$
- $(a+bi)(c+di) = (ac-bd) + (ad+bc)i$

Из этих равенств следуют еще два:

- $(a-bi) + (c-di) = (a+c) - (b+d)i$
- $(a-bi)(c-di) = (ac-bd) - (ad+bc)i$

Отображение $a+bi \mapsto a-bi$, называемое сопряжением, сохраняет сумму и произведение, и является автоморфизмом поля $\mathbb{C}$.

2) Рассмотрим в поле $\mathbb{Q}(\sqrt{2})$ отображение $a+b\sqrt{2} \mapsto a-b\sqrt{2}$. Имеем:

- $\left(a-b\sqrt{2}\right) + \left(c-d\sqrt{2}\right) = (a+c) - (b+d)\sqrt{2}$
- $\left(a-b\sqrt{2}\right)\left(c-d\sqrt{2}\right) = (ac+2bd) - (ad+bc)\sqrt{2}$

Отображение $a+b\sqrt{2} \mapsto a-b\sqrt{2}$, также называемое сопряжением, сохраняет сумму и произведение, и является автоморфизмом поля $\mathbb{Q}(\sqrt{2})$.

3) Поймем, как устроена группа $Aut(\mathbb{Q})$. Пусть $f \in Aut(\mathbb{Q})$, тогда

$$f(a) = f(a \cdot 1) = f(a)f(1) \Rightarrow f(a) = f(1)$$

Поэтому

$$f(n) = f(\underbrace{1 + \cdots + 1}_{n \text{ слагаемых}}) = \underbrace{f(1) + \cdots + f(1)}_{n \text{ слагаемых}} = nf(1) = n,$$

и

$$f\left(\frac{p}{q}\right) = \frac{f(p)}{f(q)} = \frac{p}{q}$$

Следовательно, f – тождественный.

4) Поймем, как устроена группа $Aut(\mathbb{Q}(\sqrt[3]{2}))$. Пусть $f \in Aut(\mathbb{Q}(\sqrt[3]{2}))$, тогда $f\left(\frac{p}{q}\right) = \frac{p}{q}$ (рассуждения из пункта 3 справедливы для любого поля нулевой характеристики, так как всякое такое поле содержит $\mathbb{Q}$).
Пусть $f(\sqrt[3]{2}) = u$. Применим к равенству $(\sqrt[3]{2})^3 - 2 = 0$ отображение f, получим:

$$f\left((\sqrt[3]{2})^3 - 2\right) = \left(f(\sqrt[3]{2})\right)^3 - f(2) = u^3 - 2 = 0$$

Получившееся уравнение имеет лишь один корень $u = \sqrt[3]{2}$ в $\mathbb{Q}(\sqrt[3]{2})$ (остальные два будут комплексными). Получаем $f(\sqrt[3]{2}) = \sqrt[3]{2}$, т.е. группа $Aut(\mathbb{Q}(\sqrt[3]{2}))$ состоит из одного элемента – тождественного автоморфизма.

Зафиксируем полезные соображения, следующие из примеров 3 и 4:

- если $char\ K = 0$, то при автоморфизме $\mathbb{Q}$ тождественно переходит в $\mathbb{Q}$ (аналогично, если $char\ K = p$, то $\mathbb{F}_p$ тождественно переходит в $\mathbb{F}_p$)
- корень многочлена при автоморфизме переходит в корень этого же многочлена

5) Пусть $char\ K = 2$, тогда в нем выполнено $(a+b)^2 = a^2 + b^2$ и $(ab)^2 = a^2b^2$, т.е. возведение в квадрат является автоморфизмом. Например, для $K = \mathbb{F}_4$:
$0 \mapsto 0$
$1 \mapsto 1$
$a \mapsto a^2 = a + 1$
$a + 1 \mapsto (a+1)^2 = a$

Аналогично, если $char\ K = p$, тогда в нем выполнено $(a+b)^p = a^p + b^p$ и $(ab)^p = a^p b^p$, т.е. возведение в p-ую степень задает автоморфизм конечных полей, который называется автоморфизмом Фробениуса.

Семинар 17. Расширения полей.

Разбор задач домашнего задания.

Для решения задач нам понадобится следующая важная теорема:

Теорема о башне расширений. Пусть $K \subset L \subset M$ – расширения полей. Тогда расширение $M \supset K$ конечно тогда и только тогда, когда $L \supset K$ и $M \supset L$ конечны. При этом $(M:K) = (M:L) \cdot (L:K)$.

Определение. Пусть $L \supset K$ – расширение полей. Если элемент $a \in L$ – алгебраический (над K), то многочлен $\mu_a^K(x)$ (аннулирующий многочлен минимальной положительной степени со старшим коэффициентом 1) называется минимальным многочленом элемента a.

Задача 1. Найти минимальный многочлен над $\mathbb{Q}$ для $\sqrt[3]{2} + \sqrt{3}$.

Решение.
1) Пусть $\sqrt[3]{2} + \sqrt{3} = t$, тогда:

$$\sqrt[3]{2} = t - \sqrt{3} \Leftrightarrow 2 = t^3 - 3\sqrt{3}t^2 + 9t - 3\sqrt{3} \Leftrightarrow \sqrt{3}(3t^2 + 3) = t^3 + 9t - 2 \Longrightarrow$$

$$\Longrightarrow (t^3 + 9t - 2)^2 - 3(3t^2 + 3)^2 = 0$$

Т.е. многочлен $P(t) = (t^3 + 9t - 2)^2 - 3(3t^2 + 3)^2$ является аннулирующим для $\sqrt[3]{2} + \sqrt{3}$. Докажем, что он также является минимальным – для этого найдем степень расширения $(\mathbb{Q}[\sqrt[3]{2} + \sqrt{3}] : \mathbb{Q})$.

2) Докажем вначале, что $(\mathbb{Q}[\sqrt[3]{2}][\sqrt{3}] : \mathbb{Q}) = 6$ – для этого рассмотрим башню расширений:

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{Q}[\sqrt[3]{2}][\sqrt{3}]$$

Имеем:

- $(\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}) = 3$, так как минимальный многочлен $\sqrt[3]{2}$ над $\mathbb{Q}$ равен $x^3 - 2$, его степень равна 3
- $(\mathbb{Q}[\sqrt[3]{2}][\sqrt{3}] : \mathbb{Q}[\sqrt[3]{2}]) = 2$, так как минимальный многочлен $\sqrt{3}$ над $\mathbb{Q}[\sqrt[3]{2}]$ равен $x^2 - 3$, его степень равна 2 (степень минимального многочлена не может быть меньше, так как, очевидно, многочлен первой степени над $\mathbb{Q}[\sqrt[3]{2}]$ не зануляет $\sqrt{3}$)

Тогда по теореме о башне расширений:

$$\left(\mathbb{Q}\left[\sqrt[3]{2}\right][\sqrt{3}] : \mathbb{Q}\right) = \left(\mathbb{Q}\left[\sqrt[3]{2}\right] : \mathbb{Q}\right)\left(\mathbb{Q}\left[\sqrt[3]{2}\right][\sqrt{3}] : \mathbb{Q}\left[\sqrt[3]{2}\right]\right) = 3 \cdot 2 = 6$$

3) Теперь докажем, что $\mathbb{Q}\left[\sqrt[3]{2} + \sqrt{3}\right] = \mathbb{Q}\left[\sqrt[3]{2}\right][\sqrt{3}]$. Рассмотрим башню расширений:

$$\mathbb{Q} \subset \mathbb{Q}\left[\sqrt[3]{2} + \sqrt{3}\right] \subset \mathbb{Q}\left[\sqrt[3]{2} + \sqrt{3}\right][\sqrt{3}] \subset \mathbb{Q}\left[\sqrt[3]{2}\right][\sqrt{3}]$$

Имеем:

- $\mathbb{Q}\left[\sqrt[3]{2} + \sqrt{3}\right][\sqrt{3}] = \mathbb{Q}\left[\sqrt[3]{2}\right][\sqrt{3}]$ (легко видеть, что всякий элемент одного поля является также и элементом другого, так как присоединяемые элементы выражаются друг через друга), поэтому $\left(\mathbb{Q}\left[\sqrt[3]{2}\right][\sqrt{3}] : \mathbb{Q}\left[\sqrt[3]{2} + \sqrt{3}\right][\sqrt{3}]\right) = 1$
- $\left(\mathbb{Q}\left[\sqrt[3]{2} + \sqrt{3}\right][\sqrt{3}] : \mathbb{Q}\left[\sqrt[3]{2} + \sqrt{3}\right]\right) = 1$ или 2, так как степень минимального многочлена $\sqrt{3}$ над $\mathbb{Q}\left[\sqrt[3]{2} + \sqrt{3}\right]$ может быть равна 1 или 2

Пусть $\left(\mathbb{Q}\left[\sqrt[3]{2} + \sqrt{3}\right] : \mathbb{Q}\right) = x$, тогда по теореме о башне расширений, $x\left(\mathbb{Q}\left[\sqrt[3]{2} + \sqrt{3}\right][\sqrt{3}] : \mathbb{Q}\left[\sqrt[3]{2} + \sqrt{3}\right]\right) = 6$, откуда следует, что x равен либо 3, либо 6, т.е. x делится на 3.

Абсолютно аналогичными рассуждениями, рассматривая расширение $\mathbb{Q}\left[\sqrt[3]{2} + \sqrt{3}\right]\left[\sqrt[3]{2}\right]$ вместо $\mathbb{Q}\left[\sqrt[3]{2} + \sqrt{3}\right][\sqrt{3}]$, можно получить, что x делится на 2. Следовательно, $x = 6$.

Так как $\deg P(t) = 6$ и его старший коэффициент равен 1, то $P(t)$ является минимальным многочленом над $\mathbb{Q}$ для $\sqrt[3]{2} + \sqrt{3}$. ■

Задача 2. Найти степень расширения $\mathbb{Q}\left[\sqrt{2} + \sqrt{3} + \sqrt{6}\right]$.

Решение.
1) Пусть $\sqrt{2} + \sqrt{3} + \sqrt{6} = t$, тогда:

$$\sqrt{2} + \sqrt{3} = t - \sqrt{6} \Longrightarrow 5 + 2\sqrt{6} = t^2 - 2\sqrt{6}t + 6 \Leftrightarrow \sqrt{6}(2 + 2t) = t^2 + 1 \Leftrightarrow$$

$$\Leftrightarrow (t^2 + 1)^2 - 24(t + 1)^2 = 0$$

Т.е. многочлен $P(t) = (t^2 + 1)^2 - 24(t + 1)^2$ является аннулирующим для $\sqrt{2} + \sqrt{3} + \sqrt{6}$. Так как $\deg P(t) = 4$, то $\left(\mathbb{Q}\left[\sqrt{2} + \sqrt{3} + \sqrt{6}\right] : \mathbb{Q}\right) = 4$ или 2.

2) Докажем, что $\left(\mathbb{Q}\left[\sqrt{2} + \sqrt{3} + \sqrt{6}\right] : \mathbb{Q}\right) \neq 2$. Для этого докажем вспомогательное утверждение: если $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$, где $a, b, c, d \in \mathbb{Q}$, то $a = b = c = d = 0$.

В самом деле:

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0 \Leftrightarrow a + b\sqrt{2} = \sqrt{3}(-c - d\sqrt{2})$$

Так как $\mathbb{Q}[\sqrt{2}]$ – поле, то домножая получившееся равенство на элемент, обратный к $-c - d\sqrt{2}$, мы получили бы, что $\sqrt{3} = a' + b'\sqrt{2}$ для некоторых $a', b' \in \mathbb{Q}$. Возведем в квадрат:

$$3 = (a')^2 + 2(b')^2 + 2a'b'\sqrt{2} \Leftrightarrow 2a'b'\sqrt{2} = 3 - (a')^2 - 2(b')^2 \in \mathbb{Q}$$

- получили противоречие. Значит, у элемента $-c - d\sqrt{2}$ нет обратного в $\mathbb{Q}[\sqrt{2}]$, а это означает, что $c = d = 0$, следовательно, и $a = b = 0$.

3) Если бы выполнялось равенство $(\mathbb{Q}[\sqrt{2} + \sqrt{3} + \sqrt{6}] : \mathbb{Q}) = 2$, тогда степень минимального многочлена над $\mathbb{Q}$ для $\sqrt{2} + \sqrt{3} + \sqrt{6}$ была бы равна 2, т.е. для некоторых $n, k \in \mathbb{Q}$ было бы выполнено:

$$\left(\sqrt{2} + \sqrt{3} + \sqrt{6}\right)^2 + n\left(\sqrt{2} + \sqrt{3} + \sqrt{6}\right) + k = 0 \Leftrightarrow$$

$$\Leftrightarrow \left(2 + 3 + 6 + 6\sqrt{2} + 4\sqrt{3} + 2\sqrt{6}\right) + n\left(\sqrt{2} + \sqrt{3} + \sqrt{6}\right) + k = 0 \Leftrightarrow$$

$$\Leftrightarrow 11 + k + (n+6)\sqrt{2} + (n+4)\sqrt{3} + (n+2)\sqrt{6} = 0$$

Из утверждения, доказанного в пункте 2, следует, что таких $n, k \in \mathbb{Q}$ не существует. Значит, $\mathbb{Q}[\sqrt{2} + \sqrt{3} + \sqrt{6}] = 4$. ■

Теорема. Пусть $K \subset L$ – расширение полей. Все элементы L, алгебраичные над K, образуют подполе $\overline{K} \subset L$, называемое алгебраическим замыканием поля K в L. При этом $\overline{\overline{K}} = \overline{K}$.

Доказательство.
Пусть $a, b \in \overline{K}$, тогда расширение поля K, порожденное этими элементами: $K(a, b) \supseteq K$ является конечным (следует из теоремы о башне расширений, так как расширения в башне $K \subset K(a) \subset K(a, b)$ конечны).

Любой элемент конечного расширения является алгебраическим – в самом деле, пусть $M \subset N$ – конечное расширение полей степени n и $x \in N$. Так как $(N : M) = \dim_M N = n$, то элементы $1, x, x^2, \dots, x^{n-1}, x^n$ линейно зависимы, т.е. найдутся такие $a_0, \dots, a_n \in M$, что $a_0 + a_1 x + \dots + a_n x^n = 0$

Итак, $K(a, b)$ – конечное расширение, а в конечном расширении все элементы – алгебраические. Следовательно, для любых элементов $a, b \in L$, алгебраических над K

выполнено: в $K(a,b)$ содержатся элементы $a \pm b$, $a \cdot b$, a/b (если $b \neq 0$), следовательно, $a \pm b$, $a \cdot b$, a/b (если $b \neq 0$) являются алгебраическими над K, т.е. лежат в $\overline{K}$. Это и означает, что $\overline{K}$ – подполе L.

Докажем, что $\overline{K}$ алгебраически замкнуто. Пусть $c \in \overline{\overline{K}}$, т.е. c – корень некоторого многочлена с коэффициентами из $\overline{K}$: $f = c_0 + c_1 x + \cdots + c_n x^n$, $c_0, \dots, c_n \in \overline{K}$. Рассмотрим башню расширений:

$$K \subseteq K(c_0, \dots, c_n) \subseteq K(c_0, \dots, c_n, c)$$

Оба расширения $K \subseteq K(c_0, \dots, c_n)$ и $K(c_0, \dots, c_n) \subseteq K(c_0, \dots, c_n, c)$ будут конечны (следует из теоремы о башне расширений). Тогда расширение $K \subseteq K(c_0, \dots, c_n, c)$ также будет конечным (следует из теоремы о башне расширений), следовательно, $c \in \overline{K}$. ■

Лемма. Пусть K – поле, K^* – мультипликативная группа K. Пусть G – конечная группа, $G \subset K^*$. Тогда G – циклическая.

Доказательство.
Так как G – конечная абелева группа, то $\exists a$: $a = \exp(G)$ (т.е. $a = $ НОК всех элементов группы). Тогда $\forall x \in G$ выполнено $x^{\exp(G)} = 1 \Leftrightarrow x^{\exp(G)} - 1 = 0$. Пусть $|G| = q$, тогда многочлен $x^{\exp(G)} - 1$ имеет q корней. Но многочлен не может иметь корней больше, чем его степень, поэтому $\exp(G) \geq q$; с другой стороны, $\exp(G) \leq q$, так как порядок элемента не больше порядка группы. Следовательно, $\exp(G) = q$. Тогда $G = < a >$ - циклическая. ■

Из этой леммы следует задача 5:

Задача 5. Показать, что если $|F| = q$, то всякий элемент поля F удовлетворяет уравнению $x^q - x = 0$.

Решение.
Если $x = 0$, то утверждение задачи верно. Если $x \neq 0$, то $|F^*| = q - 1$, и по приведенной выше лемме выполнено $x^{q-1} - 1 = 0$. Домножая на x, получаем $x^q - x = 0$. ■

Автоморфизмы конечных полей.

На прошлом семинаре мы привели некоторые примеры автоморфизмов полей, в частности, автоморфизм Фробениуса: если $char\, K = 2$, тогда в нем выполнено $(a+b)^2 = a^2 + b^2$ и $(ab)^2 = a^2 b^2$, т.е. возведение в квадрат является автоморфизмом. Аналогично, если $char\, K = p$, тогда в нем выполнено $(a+b)^p = a^p + b^p$ и

$(ab)^p = a^p b^p$, т.е. возведение в p-ую степень задает автоморфизм конечных полей, который называется автоморфизмом Фробениуса.

В качестве иллюстрации этого факта мы рассматривали поле $\mathbb{F}_4$, сейчас рассмотрим $\mathbb{F}_8$: проверим, что отображение $x \mapsto x^2$ является автоморфизмом (для этого достаточно проверить инъективность): пусть $a \neq b$, но $a^2 = b^2$, тогда

$$a^2 - b^2 = 0 \Leftrightarrow a^2 + 2ab + b^2 = 0 \Leftrightarrow (a+b)^2 = 0 \Leftrightarrow a + b = 0 \Leftrightarrow a = b$$

- противоречие.

Группа $Aut(\mathbb{F}_8)$ конечна (например, потому, что она лежит в S_8). Найдем порядок элемента g: $x \mapsto x^2$ в $Aut(\mathbb{F}_8)$. Имеем:

- g: $x \mapsto x^2$
- g^2: $x \mapsto x^4$
- g^3: $x \mapsto x^8 = x$

- таким образом, $ord\ (g) = 3$.

Обобщим задачу – рассмотрим поле $\mathbb{F}_{p^n}$ и автоморфизм Фробениуса g: $x \mapsto x^p$. В $Aut(\mathbb{F}_{p^n})$ порядок элемента g равен n. В самом деле:

- g: $x \mapsto x^2$
- g^2: $x \mapsto x^{p^2}$
- …
- g^n: $x \mapsto x^{p^n} = x$

Все уравнения, получающиеся до n-го шага ($x^{p^n} - x = 0$), имеют степень меньше p^n, следовательно, соответствующие им автоморфизмы нетривиальны (не все элементы $\mathbb{F}_{p^n}$ удовлетворяют этим уравнениям). Таким образом, $ord\ (g) = n$.

Есть ли еще автоморфизмы конечных полей?

Утверждение. Пусть $K \subset L$ – конечное расширение полей. Тогда $ord\ (Aut_K L) \leq dim_K L = n$ (здесь $Aut_K L$ – группа автоморфизмов L, сохраняющих поле K).

Схема доказательства.
Пусть $a \in L$, $F = K(a)$ – расширение степени d, где d – делитель n. Значит, $K(a) = K[x]/P(x)$, где $\deg P = d$ и $P(a) = 0$. Так как для выбора a существует не более d вариантов, то из теоремы о башне расширений следует, что $ord\ (Aut_K L) \leq n$. ■

Из этого утверждения следует, что любой автоморфизм $\mathbb{F}_{p^n}$ сохраняет $\mathbb{F}_p$ (так как при автоморфизме 1 переходит в 1). Значит, $\left|Aut(\mathbb{F}_{p^n})\right| \leq dim_{\mathbb{F}_p}\mathbb{F}_{p^n} = n$. С другой стороны, мы знаем, что в $Aut(\mathbb{F}_{p^n})$ есть элемент порядка n (автоморфизм Фробениуса), следовательно,

$$Aut(\mathbb{F}_{p^n}) \cong \mathbb{Z}/n\mathbb{Z},$$

- группа, порожденная автоморфизмом Фробениуса $x \mapsto x^p$.

Задача 6. Найти все подполя в $\mathbb{F}_{1024}$.

Решение.
Условие $\mathbb{F}_{p^n} \supseteq \mathbb{F}_{p^m}$ равносильно тому, что $n \vdots m$. Так как $1024 = 2^{10}$ и 2 и 5 – все простые делители 10, то получаем следующие цепочки вложений:

$$\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_{2^1} \subset \mathbb{F}_{2^2} \subset \mathbb{F}_{2^{10}} = \mathbb{F}_{1024}$$

и

$$\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_{2^1} \subset \mathbb{F}_{2^5} \subset \mathbb{F}_{2^{10}} = \mathbb{F}_{1024}$$

■

При решении задачи 6 мы использовали следующее утверждение:

Утверждение. Поле $\mathbb{F}_q$ содержит подполе $F \simeq \mathbb{F}_r$ тогда и только тогда, когда $q = p^n$, $r = p^m$ и $n \vdots m$. При этом такое подполе F единственно.

Доказательство.
⇒:
Пусть $\mathbb{F}_q$ содержит $F \simeq \mathbb{F}_r$. Так как $\mathbb{F}_q$ конечно, то оно является расширением F.
Обозначим $(\mathbb{F}_q : F) = d$. Тогда $\mathbb{F}_q \simeq F^d$ как векторное пространство над F. Отсюда, в частности, следует, что

$$\left|\mathbb{F}_q\right| = |F|^d \Rightarrow q = r^d$$

Так как r – количество элементов в $\mathbb{F}_r$, то $r = p^m$, тогда $q = r^{md}$.

⇐:
Пусть $n = m \cdot d$, тогда $q = r^d$. Отсюда следует, что $q - 1$ делится на $r - 1$:

$$q - 1 = r^d - 1 = (r-1)(r^{d-1} + r^{d-2} + \cdots + r + 1)$$

Для краткости обозначим $r^{d-1} + r^{d-2} + \cdots + r + 1 = s$ и рассмотрим многочлен $x^q - x$:

$$x^q - x = x(x^{q-1} - 1) = x\left(x^{(r-1)s} - 1\right) =$$

$$= x(x^{r-1} - 1)\left(x^{(r-1)(s-1)} + x^{(r-1)(s-2)} + \cdots + x^{r-1} + 1\right) =$$

$$= (x^r - x)\left(x^{(r-1)(s-1)} + x^{(r-1)(s-2)} + \cdots + x^{r-1} + 1\right)$$

То есть, $x^q - x$ делится на $x^r - x$. Рассмотрим поле $\mathbb{F}_q$ – оно является полем разложения для многочлена $x^q - x$, но тогда $\mathbb{F}_q$ содержит и поле разложения F для $x^r - x$. Но $F \simeq \mathbb{F}_r$, также F состоит из всех корней многочлена $x^r - x$, откуда вытекает единственность F. ■

Как можно было заметить из доказательства этого утверждения, подполя в $\mathbb{F}_{p^n}$ образуют в точности элементы, неподвижные относительно автоморфизма Фробениуса (такие элементы называются инвариантами). Таким образом, между подполями и подгруппами в группе автоморфизмов поля существует соответствие.

Конечные поля характеристики p.

Ранее для построения полей мы присоединяли к уже имеющимся полям корень неприводимого многочлена. Как было доказано выше, существует и единственное $\overline{\mathbb{F}_p}$ – алгебраическое замыкание поля $\mathbb{F}_p$, в котором лежат все поля, получающиеся присоединением к $\mathbb{F}_p$ корней неприводимых многочленов. Также в алгебраическом замыкании всякий многочлен над $\mathbb{F}_p$ имеет корни – следовательно, многочлен $x^{p^n} - x$ будет иметь p^n корней в $\overline{\mathbb{F}_p}$, которые образуют подполе $\mathbb{F}_{p^n}$.

Эта конструкция позволяет утверждать о существовании поля из p^n элементов. Несложно понять, что все такие поля изоморфны друг другу: допустим, существуют два поля из p^n элементов, тогда каждый элемент из этих подполей удовлетворял бы уравнению $x^{p^n} - x = 0$ – но у этого уравнения p^n решений, значит, поля поточечно совпадают (т.е. оба они изоморфны подполю корней многочлена $x^{p^n} - x$ в $\overline{\mathbb{F}_p}$).

Как следствие, для любого n существует неприводимый многочлен степени n.

Семинар 18. Поле инвариантов. Расширения Галуа.

Поле инвариантов.

Напомним (дадим) некоторые определения, которые понадобятся нам в дальнейшем.

Определение. Автоморфизм f поля K – это биективное отображение $f\colon K \to K$, для которого: $\forall a, b \in K$:

- $f(a+b) = f(a) + f(b)$
- $f(a \cdot b) = f(a) \cdot f(b)$

Автоморфизмы поля K образуют группу $Aut(K)$ относительно композиции. Пусть $K \subset L$ – расширение полей. Обозначение: $Aut_K L$ – группа автоморфизмов L, сохраняющих поле K (т.е. $\forall k \in K$ выполнено $f(k) = k$).

Определение. Пусть $G \subset Aut(K)$. Элемент $a \in K$ называется инвариантом (G-инвариантом), если $\forall g \in G$ выполнено $g(a) = a$.

Утверждение. Инварианты образуют подполе в K, которое называется полем инвариантов и обозначается K^G.

Доказательство.
Пусть $a, b \in K$ и $\forall g \in G$ выполнено $g(a) = a$ и $g(b) = b$. Обозначим $g(a^{-1}) = u$, тогда:

- $1 = g(1) = g(a^{-1}a) = g(a^{-1})g(a) = ug(a) \Longrightarrow u = \big(g(a)\big)^{-1} = a^{-1}$

Также

- $g(a+b) = g(a) + g(b) = a + b$
- $g(ab) = g(a)g(b) = ab$

■

Примеры полей инвариантов.

1) Рассмотрим поле $K(x_1, \dots, x_n)$. На этом поле действует группа S_n: для $\forall \sigma \in S_n$ имеем $\sigma(x_i) = x_{\sigma(i)}$. Пусть $P(x) = x^n - a_{n-1}x^{n-1} + \dots + a_1 x + a_0$ – так как коэффициенты $P(x)$ являются симметрическими многочленами от его корней $x_1, \dots, x_n$, то симметрические многочлены являются кольцом инвариантов относительно действия группы S_n (соответственно, симметрические функции образуют поле инвариантов). Обозначим симметрические многочлены $\varphi_1, \dots, \varphi_n$. Оказывается, $K(x_1, \dots, x_n)^{S_n} \cong K(\varphi_1, \dots, \varphi_n)$.

2) Рассмотрим поле $K(x)$ и группу $G \cong \mathbb{Z}/2\mathbb{Z}$, состоящую из тождественного преобразования и элемента $g\colon\ x \mapsto -x$. Инвариантами будут все $a \in K$ и дроби вида $\frac{P(x^2)}{Q(x^2)}$. Таким образом, $K(x)^G \cong K(x^2) \cong K(y)$.

3) Рассмотрим поле $K(x)$ и группу $G \cong \mathbb{Z}/2\mathbb{Z}$, состоящую из тождественного преобразования и элемента $g\colon\ x \mapsto \frac{1}{x}$. Инвариантами будут все $a \in K$ и дроби вида $\frac{P\left(x+\frac{1}{x}\right)}{Q\left(x+\frac{1}{x}\right)}$. Таким образом, $K(x)^G \cong K(x+\frac{1}{x}) \cong K(y)$.

Во всех рассмотренных примерах мы получили, что поле инвариантов трансцендентного расширения поля изоморфно трансцендентному расширению этого поля. Оказывается, если G – конечная группа, действующая на $K(x)$, и сохраняющая K, то $K(x)^G \cong K(y)$. Кроме того, верно и более сильное утверждение: если G – конечная группа, действующая на $K(x,y)$, и сохраняющая K, причем $char\ K = 0$ и $\overline{K} = K$, то $K(x,y)^G \cong K(z,t)$.

Расширения Галуа.

Определение. Конечное расширение полей $L \supset K$ называется расширением Галуа, если $|Aut_K L| = dim_K L$. В этом случае группа $Aut_K L$ называется группой Галуа расширения и обозначается $Gal\ (L/K)$.

Замечание. $L^{Gal\ (L/K)} = K$.

Примеры расширений Галуа

- $\mathbb{C}/\mathbb{R}$
- $K(\sqrt{a})/K$, если $char\ K \neq 2$ – можем построить изоморфизм (аналогичный сопряжению), отправляющий $\sqrt{a}$ в $-\sqrt{a}$
- $\mathbb{F}_{p^n}/\mathbb{F}_p$ – см. конец прошлого семинара

Не является расширениями Галуа, например $\mathbb{Q}(\sqrt[3]{2})$ – группа автоморфизмов этого поля является тривиальной, так как элемент $\sqrt[3]{2}$ “некуда отправить”, т.е. нельзя придумать автоморфизм $\mathbb{Q}(\sqrt[3]{2})$, переводящий $\sqrt[3]{2}$ не в себя.

Определение. Пусть $P(x) \in K[x]$, $\deg P > 0$. Полем разложения многочлена $P(x)$ над полем K называется поле L, такое что:

- 1) $P(x)$ разлагается на линейные множители
- 2) Корни $P(x)$ порождают L

Для любого многочлена $P(x) \in K[x]$, $\deg f > 0$ существует единственное с точностью до изоморфизма поле разложения $P(x)$ над K. Обозначение: $L = K(P)$.

Утверждение. Поле разложения является расширением Галуа.

Примеры полей разложения.

1) Если $P(x)$ – квадратичный многочлен, не имеющий корней в $\mathbb{Q}$, то его поле разложения над $\mathbb{Q}$ будет расширением степени 2 (потому что с присоединением корня автоматически присоединяется и второй корень). Группа Галуа расширения будет состоять из двух элементов.

2) Рассмотрим $x^3 - 1/\mathbb{Q}$. Так как $x^3 - 1 = (x-1)(x^2 + x + 1)$, то его поле разложения над $\mathbb{Q}$ – это $\mathbb{Q}(\omega)/\mathbb{Q}$, где ω – первообразный корень степени 3 из единицы. Группа Галуа расширения будет состоять из двух элементов: тождественного автоморфизма и $g\colon\ \omega \mapsto \omega^2$.

3) Рассмотрим $x^3 - 2/\mathbb{Q}$. Многочлен $x^3 - 2$ не имеет корней в $\mathbb{Q}$. Рассмотрим поле $P = \mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2})$. Имеем: $dim_{\mathbb{Q}} P = 3$, но группа Галуа этого расширения будет состоять только из тривиального автоморфизма.

Продолжим построение поля разложения: $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$. Рассмотрим поле $L = P[x]/(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}) \cong \mathbb{Q}(\sqrt[3]{2}, \omega)$, где ω – первообразный корень степени 3 из единицы. Поле L будет полем разложения $x^3 - 2$ над $\mathbb{Q}$, так как оно содержит все корни $x^3 - 2$. Имеем: $dim_{\mathbb{Q}} L = 6$ (следует из теоремы о башне расширений), следовательно, группа Галуа $Aut_{\mathbb{Q}} L$ состоит из 6 элементов, т.е. это либо S_3, либо $\mathbb{Z}/6\mathbb{Z}$.

Для построения автоморфизма $f \in Aut_{\mathbb{Q}} L$ достаточно найти образы элементов $\sqrt[3]{2}$ и ω. Пусть $f \in Aut_{\mathbb{Q}} L$. Так как $\forall q \in \mathbb{Q}\colon\ f(q) = q$, то имеются следующие варианты:

$$f(\sqrt[3]{2}) = \begin{cases} \sqrt[3]{2} \\ \omega\sqrt[3]{2} \\ \omega^2\sqrt[3]{2} \end{cases} \qquad f(\omega) = \begin{cases} \omega \\ \omega^2 \end{cases}$$

- имеется 6 возможностей, и все они реализуются. Любой элемент группы Галуа $Aut_{\mathbb{Q}} L$ задает некоторую перестановку корней $x_1 = \sqrt[3]{2},\ x_2 = \omega\sqrt[3]{2},\ x_3 = \omega^2\sqrt[3]{2}$ многочлена $x^3 - 2$, причем эта группа некоммутативна, поэтому $Aut_{\mathbb{Q}} L \cong S_3$.

Вообще, группа Галуа многочлена степени n будет подгруппой в S_n, так как элементы этой группы определяются тем, куда при соответствующем автоморфизме переходят корни многочлена. В частности, группой Галуа кубического неприводимого многочлена может быть либо S_3, либо $\mathbb{Z}/3\mathbb{Z}$.

4) Рассмотрим $x^4 + 10x^2 + 1/\mathbb{Q}$. Как мы знаем, $x^4 + 10x^2 + 1$ – это минимальный многочлен элемента $\sqrt{2} + \sqrt{3}$ над $\mathbb{Q}$. Так как его степень равна 4, то и степень соответствующего расширения будет не меньше 4. С другой стороны, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ – поле, степень расширения которого равна 4, и которое содержит $\sqrt{2} + \sqrt{3}$. Значит, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ будет полем разложения $x^4 + 10x^2 + 1$ над $\mathbb{Q}$.

Для построения автоморфизма $f \in Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3})$ достаточно найти образы элементов $\sqrt{2}$ и $\sqrt{3}$. Имеются следующие варианты:

$$f(\sqrt{2}) = \begin{cases} \sqrt{2} \\ -\sqrt{2} \end{cases} \qquad f(\sqrt{3}) = \begin{cases} \sqrt{3} \\ -\sqrt{3} \end{cases}$$

Получаем $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3}) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Как мы отмечали на прошлом семинаре, между подполями и подгруппами в группе автоморфизмов поля существует соответствие. На рис. 18.1. изображены решетка подполей в $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ и соответствующая решетка подгрупп в $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3})$ – здесь $f \in Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $f(\sqrt{2}) = -\sqrt{2}$, $f(\sqrt{3}) = \sqrt{3}$ и $g \in Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $g(\sqrt{2}) = \sqrt{2}$, $g(\sqrt{3}) = -\sqrt{3}$.

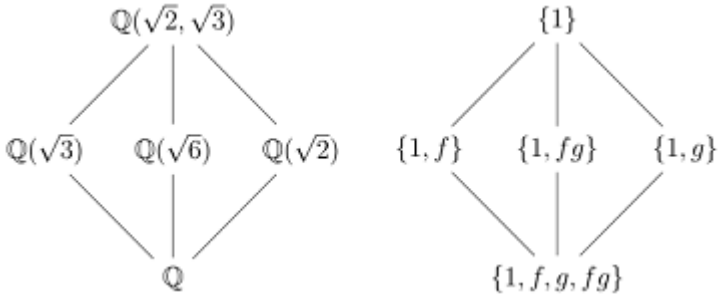

Рис. 18.1. Подполя в $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ и подгруппы в $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3})$

Аналогичная картина наблюдается и для поля разложения из примера 3, и т.д. Также можно заметить, что нормальным подгруппам (и только им) будут соответствовать расширение Галуа. Все эти соображения подводят нас к следующей очень важной теореме.

Основная теорема теории Галуа. Пусть L/K – расширение Галуа, $G = Gal\,(L/K)$ – его группа Галуа. Тогда:

- 1) Имеется биекция (соответствие Галуа) между множеством подгрупп $H \subseteq G$ и множеством подполей $F \subseteq L$, $F \supseteq K$: каждой подгруппе сопоставим поле ее инвариантов, а каждому подполю сопоставим подгруппу, состоящую из автоморфизмов расширения, оставляющих на месте все элементы подполя:

$$H \mapsto F = L^H$$
$$F \mapsto H = \{g \in G \mid g(a) = a, \forall a \in F\} = Gal\,(L/F)$$

- 2) Если $K \subseteq F \subseteq L$, F – подполе, то L/F – расширение Галуа, и соответствующая подгруппа $H \subseteq G$ – его группа Галуа.
- 3) Если $K \subseteq F \subseteq L$, F – подполе, то F/K – расширение Галуа $\Leftrightarrow H \lhd G$. При этом $Gal\,(F/K) \cong G/H$.

С помощью основной теоремы теории Галуа можно ответить на вопрос о разрешимости уравнний в радикалах.

Теорема Галуа. Пусть $char\,K = 0$, $f \in K[x]$, $L = K(f)$, $G = Aut\,(L/K)$. Тогда: уравнение $f(x) = 0$ разрешимо в радикалах $\Leftrightarrow G = Gal\,(L/K)$ разрешима.

Также теория Галуа используется при решении ряда классических задач о построениях циркулем и линейкой: с помощью циркуля и линейки можно извлекать только квадратные корни (т.е. можно построить отрезок, длина которого является квадратным корнем длины другого отрезка, при этом нельзя построить кубический корень и т.д.), поэтому длины всех отрезков, которые мы можем получить при помощи построений циркулем и линейкой, лежат в ряду квадратичных расширений поля $\mathbb{Q}$ (или какого-то другого данного в условии задачи поля, например, $\mathbb{Q}(\cos\alpha)$).

В частности, отсюда вытекает невозможность решения задачи о квадратуре круга, так как при ее решении нам необходимо построить отрезок длины $\sqrt{\pi}$, которое является трансцендентым числом. Также невозможно решить задачу об удвоени куба, так как $\sqrt[3]{2}$ не лежит в ряду квадратичных расширений поля $\mathbb{Q}$, нельзя решить задачу о трисекции угла и т.д.

Семинар 19. Поле разложения многочлена.

Разбор задач домашнего задания.

Задача 1. Можно ли $7+5\sqrt{2}$ представить в виде суммы чисел вида $(a_i+b_i\sqrt{2})^2$, где $a_i, b_i \in \mathbb{Q}$?

Решение.
Пусть

$$7+5\sqrt{2}=\sum_{i=1}^{n}(a_i+b_i\sqrt{2})^2,$$

тогда и

$$7-5\sqrt{2}=\sum_{i=1}^{n}\left(a_i-b_i\sqrt{2}\right)^2,$$

так как $\sqrt{2}\mapsto-\sqrt{2}$ – автоморфизм поля $\mathbb{Q}(\sqrt{2})$. Но $7-5\sqrt{2}<0$, а в правой части равенства стоит сумма квадратов, т.е. неотрицательное число – противоречие, значит, $7+5\sqrt{2}$ нельзя представить в требуемом виде. ■

Задача 2. Рассмотрим поле $\mathbb{C}(x_1,x_2,x_3)$. Найти не симметрический многочлен, инвариантный относительно действия группы, порожденной элементом $x_1\to x_2\to x_3\to x_1$. Существуют ли линейные не симметрические многочлены, инвариантные относительно действия этой группы?

Решение.
1) Например, $(x_1-x_2)(x_2-x_3)(x_3-x_1)$.

2) Нет. Рассмотрим векторное пространство $\mathbb{C}^3$ с базисом x_1,x_2,x_3, т.е. множество многочленов вида $ax_1+bx_2+cx_3$. Элемент $x_1\to x_2\to x_3\to x_1$ задает на этом векторном пространстве линейный оператор с матрицей

$$\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}$$

Собственные значения: $1,\omega,\omega^2$, где ω – первообразный корень степени 3 из единицы. Собственные векторы, соответствующие этим собственным значениям:

$$\begin{pmatrix}1\\1\\1\end{pmatrix}, \quad \begin{pmatrix}1\\\omega\\\omega^2\end{pmatrix}, \quad \begin{pmatrix}1\\\omega^2\\\omega\end{pmatrix}$$

Этим собственным векторам соответствуют многочлены $x_1+x_2+x_3$, $x_1+\omega x_2+\omega^2 x_3$ и $x_1+\omega^2 x_2+\omega x_3$. Многочлен $x_1+x_2+x_3$ является инвариантным (но он симметрический), а многочлены $x_1+\omega x_2+\omega^2 x_3$ и $x_1+\omega^2 x_2+\omega x_3$ являются полуинвариантными (при перестановке $x_1\to x_2\to x_3\to x_1$ они переходят в себя с умножением на ω и ω^2 соответственно).

Используя эти полуинвариантные многочлены, можно построить не симметрический многочлен второй степени (являющийся их произведением), инвариантный относительно перестановки $x_1\to x_2\to x_3\to x_1$:

$$(x_1+\omega x_2+\omega^2 x_3)(x_1+\omega^2 x_2+\omega x_3)=x_1^2+x_2^2+x_3^2-x_1x_2-x_1x_3-x_2x_3$$

■

Задача 3. Рассмотрим поле $K[x,y]$ и группу $G\cong\mathbb{Z}/2\mathbb{Z}$, состоящую из тождественного преобразования и автоморфизма $g\colon\ x\to -x, y\to -y$. Найти $(K[x,y])^G$ и $(K(x,y))^G$.

Решение.
1) Пусть $f\in(K[x,y])^G$, тогда $g\big(f(x,y)\big)=f(-x,-y)=f(x,y)$, откуда следует, что f является суммой одночленов вида ax^my^n, где $(m+n)\vdots 2$. Данное кольцо инвариантов порождается одночленами x^2,xy,y^2. Обозначив $x^2=a, xy=b, y^2=c$, получаем, что

$$(K[x,y])^G\cong K[a,b,c]/(ac-b^2)$$

2) Пусть $\frac{P(x,y)}{Q(x,y)}\in(K(x,y))^G$, тогда $g\left(\frac{P(x,y)}{Q(x,y)}\right)=\frac{P(-x,-y)}{Q(-x,-y)}=\frac{P(x,y)}{Q(x,y)}$. Возможны два случая:

- и $P(x,y)$, и $Q(x,y)$ являются инвариантными многочленами, т.е. состоят из одночленов вида ax^my^n, где $m+n$ четно
- и $P(x,y)$, и $Q(x,y)$ являются полуинвариантными многочленами, т.е. состоят из одночленов вида ax^my^n, где $m+n$ нечетно

Данное поле инвариантов порождается элементами xy, $\frac{x}{y}$. Получаем

$$(K(x,y))^G\cong K\left(xy,\frac{x}{y}\right)\cong K(x,y)$$

■

Задача 4. Найти поле разложения L многочлена x^p-1 (p – простое) над $\mathbb{Q}$ и найти $(L\colon\mathbb{Q})$.

Решение.
1) Корнями данного многочлена являются $\xi_p, \xi_p^2, \dots, \xi_p^{p-1}$, где ξ_p – некоторый корень p-ой степени из единицы. Следовательно, поле разложения многочлена $x^p - 1$ можно получить, добавив к полю $\mathbb{Q}$ любой (не равный 1) корень этого многочлена: $L = \mathbb{Q}[\xi_p]$.

2) Многочлен $\frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \dots + x + 1$ степени $p-1$ является аннулирующим для ξ_p и неприводим над $\mathbb{Q}$, поэтому $(L:\mathbb{Q}) = p-1$. То, что степень расширения $(L:\mathbb{Q})$ не может быть меньше $p-1$ следует из устройства группы $Gal\,(\mathbb{Q}[\xi_p]/\mathbb{Q})$ (более подробно см. семинар 21). ■

Задача 5. Пусть L – поле разложения многочлена $x^n - 1$ над $\mathbb{Q}$. Найти $Gal\,(L/\mathbb{Q})$.

Решение.
Пусть ξ_n – первообразный корень n-ой степени из единицы. При всяком автоморфизме из $Gal\,(L/\mathbb{Q})$ первообразный корень ξ_n должен переходить в первообразный корень, т.е. $\xi_n \mapsto \xi_n^a$, где a взаимно просто с n. Отсюда следует, что $|Gal\,(L/\mathbb{Q})| = \varphi(n)$, где φ – функция Эйлера (обоснование этого факта см. семинар 21).

Так как:

- всякий автоморфизм из $Gal\,(L/\mathbb{Q})$ индуцирует автоморфизм группы $(1, \xi_n, \xi_n^2, \dots, \xi_n^{n-1}) \cong \mathbb{Z}/n\mathbb{Z}$,
- $|Aut\,(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$,

то $Gal\,(L/\mathbb{Q}) \cong Aut\,(\mathbb{Z}/n\mathbb{Z})$. Воспользуемся результатом, полученным на семинаре 3: пусть $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, тогда

$$\varphi(n) = \prod_{i=1}^{k} \varphi\left(p_i^{a_i}\right) = \prod_{i=1}^{k} \varphi\left(p_i^{a_i}\right)(p_i - 1)$$

и

$$Gal\,(L/\mathbb{Q}) \cong Aut\,(\mathbb{Z}/n\mathbb{Z}) \cong Aut\,(\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times Aut\,(\mathbb{Z}/p_2^{a_2}\mathbb{Z}) \times \dots \times Aut\,(\mathbb{Z}/p_k^{a_k}\mathbb{Z}),$$

где:

- если p_i нечетное, то $Aut\,(\mathbb{Z}/p_i^{a_i}\mathbb{Z}) \cong \mathbb{Z}/p_i^{a_i-1}(p_i - 1)\mathbb{Z}$,
- если $p_i = 2$, то $Aut\,(\mathbb{Z}/2^{\alpha_0}\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha_0-2}\mathbb{Z})$.

■

Задача 6. Привести пример расширения Галуа L поля $\mathbb{Q}$, такого что $D_4 \subseteq Gal\,(L/\mathbb{Q})$.

Решение.
Например, $L = \mathbb{Q}\left(\sqrt[4]{2}, i\right)$.

В самом деле, рассмотрим башню расширений $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[4]{2}\right) \subset \mathbb{Q}\left(\sqrt[4]{2}, i\right)$. Так как $\left(\mathbb{Q}\left(\sqrt[4]{2}\right): \mathbb{Q}\right) = 4$ и $\left(\mathbb{Q}\left(\sqrt[4]{2}, i\right): \mathbb{Q}\left(\sqrt[4]{2}\right)\right) = 2$, то по теореме о башне расширений, $\left(\mathbb{Q}\left(\sqrt[4]{2}, i\right): \mathbb{Q}\right) = 8$.

Так как $L = \mathbb{Q}\left(\sqrt[4]{2}, i\right)$ является полем разложения многочлена $x^4 - 2$, то это расширение Галуа. Так как поле $\mathbb{Q}\left(\sqrt[4]{2}\right)$ не является расширением Галуа, то соответствующая ему подгруппа в L не будет нормальной, т.е. $Gal\,(L/\mathbb{Q})$ не абелева группа. Следовательно, $Gal\,(L/\mathbb{Q}) = D_4$ (так как существуют всего две неабелевы группы порядка 8: D_4 и Q_8, но все подгруппы Q_8 нормальны). ■

Семинар 20. Сопряженные элементы. Сепарабельность.

Сопряженные алгебраические элементы.

Продолжим изучать расширения Галуа. Еще со школы мы помним задачи, где нужно избавиться от иррациональности в знаменателе дроби – для этого числитель и знаменатель дроби нужно домножить на сопряженное к знаменателю число. Определим понятие сопряженного числа в общем случае.

- 1) Например, рассмотрим дробь

$$\frac{1}{\sqrt[3]{2}+\sqrt{5}}$$

Если бы в знаменателе стояло выражение $1+\sqrt{5}$, мы бы домножили числитель и знаменатель дроби на $1-\sqrt{5}$. Если бы в знаменателе стояло выражение $\sqrt[3]{2}+1$, мы бы домножили числитель и знаменатель дроби на $\sqrt[3]{4}-\sqrt[3]{2}+1$, т.е. дополнили бы знаменатель до суммы кубов. Если разложить на множители, получим $\sqrt[3]{4}-\sqrt[3]{2}+1=(\sqrt[3]{2}\omega+1)(\sqrt[3]{2}\omega^2+1)$, где ω – первообразный корень степени 3 из единицы.

Для $1+\sqrt{5}$ и $\sqrt[3]{2}+1$ у нас получалось избавляться от иррациональности в знаменателе, так как $1+\sqrt{5}$ и $1-\sqrt{5}$ образуют орбиту при действии группы Галуа расширения $\mathbb{Q}(\sqrt{5})$, а $\sqrt[3]{2}+1$, $\sqrt[3]{2}\omega+1$ и $\sqrt[3]{2}\omega^2+1$ образуют орбиту при действии группы Галуа расширения $\overline{\mathbb{Q}}(\sqrt[3]{2})$.

В общем случае это следует из основной теоремы теории Галуа: произведение всех элементов орбиты инвариантно относительно действия группы, следовательно, принадлежит $\mathbb{Q}$ (в общем случае – полю, расширение которого мы рассматриваем).

Определение. Пусть $K\subset L$ – расширение полей, элемент $\alpha\in L$ алгебраичен над K и L – поле разложения многочлена μ_α^K. Корни $a_1,\dots,a_n$ многочлена μ_α^K называются сопряженными с α над K.

Найдем сопряженные к $\sqrt[3]{2}+\sqrt{5}$ над $\mathbb{Q}$. Так как $\mathbb{Q}(\sqrt[3]{2},\sqrt{5})$ – поле разложения многочлена $\mu^{\mathbb{Q}}_{\sqrt[3]{2}+\sqrt{5}}$, и $(\mathbb{Q}(\sqrt[3]{2},\sqrt{5}):\mathbb{Q})=6$, то сопряженными к $\sqrt[3]{2}+\sqrt{5}$ будут 6 элементов: $\sqrt[3]{2}+\sqrt{5}$, $\omega\sqrt[3]{2}+\sqrt{5}$, $\omega^2\sqrt[3]{2}+\sqrt{5}$, $\sqrt[3]{2}-\sqrt{5}$, $\omega\sqrt[3]{2}-\sqrt{5}$, $\omega^2\sqrt[3]{2}-\sqrt{5}$.

- 2) Найдем сопряженные к $\sqrt{2}+\sqrt{3}+\sqrt{6}$ над $\mathbb{Q}$.

Так как $\mathbb{Q}(\sqrt{2},\sqrt{3})$ – поле разложения многочлена $\mu^{\mathbb{Q}}_{\sqrt{2}+\sqrt{3}+\sqrt{6}}$, и $(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}) = 4$, то сопряженными к $\sqrt{2}+\sqrt{3}+\sqrt{6}$ будут четыре элемента, которые находятся среди элементов вида $\pm\sqrt{2}\pm\sqrt{3}\pm\sqrt{6}$.

При автоморфизме $\sqrt{2}$ переходит в $\sqrt{2}$ или $-\sqrt{2}$, также $\sqrt{3}$ переходит в $\sqrt{3}$ или $-\sqrt{3}$. Учитывая, что $\sqrt{6} = \sqrt{2}\cdot\sqrt{3}$, т.е. знак $\sqrt{6}$ является произведением знаков $\sqrt{2}$ и $\sqrt{3}$, получаем, что сопряженными к $\sqrt{2}+\sqrt{3}+\sqrt{6}$ над $\mathbb{Q}$ будут следующие элементы: $\sqrt{2}+\sqrt{3}+\sqrt{6}$, $\sqrt{2}-\sqrt{3}-\sqrt{6}$, $-\sqrt{2}+\sqrt{3}-\sqrt{6}$, $-\sqrt{2}-\sqrt{3}+\sqrt{6}$.

Перейдем к другим вопросам, связанным с теорией Галуа.

Задача. Рассмотрим группу $SL_2(K)$, $char\, K = 0$. Для каких n в $SL_2(K)$ существуют элементы порядка n?

Решение.
Отметим, что если $K = \mathbb{R}$, то для любого n в $SL_2(\mathbb{R})$ существуют элементы порядка n (матрицы поворота на угол $\frac{2\pi}{n}$). Также ранее (см. семинар 4) мы выяснили, что в $GL_2(\mathbb{Z})$ элементов конечного порядка, отличных от $1, 2, 3, 4, 6$ не существует, так как нельзя подобрать целочисленные матрицы с определителем ±1, след которых также был бы целочисленным.

В общем случае воспользуемся следующим рассуждением: рассмотрим $\overline{K}$ – алгебраическое замыкание поля K. Поле $\overline{K}$ содержит корни любого многочлена над K, в частности, ξ_n – корни степени n из единицы, поэтому любая матрица конечного порядка $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\overline{K})$ будет сопряжена матрице вида $\begin{pmatrix} \xi_n^u & 0 \\ 0 & \xi_n^v \end{pmatrix} \in SL_2(\overline{K})$ (так как жорданова форма матрицы конечного порядка диагональна). Так как операция сопряжения сохраняет определитель матрицы и ее след, то $tr\, A = \xi_n^u + \xi_n^v \in K$ и $\det A = \xi_n^{u+v} \in K$.

Если $\xi_n \in K$, то $\xi_n^u + \xi_n^v \in K$ и $\xi_n^{u+v} \in K$, и элементы порядка n существуют в $SL_2(K)$ для любых n. Пусть $\xi_n \notin K$, а $\xi_n^u + \xi_n^v \in K$ и $\xi_n^{u+v} \in K$. Имеем:

- $\xi_n^{u+v} = 1$, откуда $u = -v\ (mod\ n)$ (иначе в поле K лежит какой-то корень степени n из единицы, отличный от ξ_n, и элементы порядка n существуют в $GL_2(K)$ для любых n)
- $\xi_n^u + \xi_n^{-u} \in K$, т.е. $2\cos\frac{2\pi u}{n} \in K$.

Получаем систему:

$$\begin{cases} a+d = 2\cos\frac{2\pi u}{n} \\ ad-bc = 1 \end{cases}$$

Заметим, что этой системе удовлетворяет матрица поворота на угол $\frac{2\pi u}{n}$:

$$\begin{pmatrix} \cos\frac{2\pi u}{n} & -\sin\frac{2\pi u}{n} \\ \sin\frac{2\pi u}{n} & \cos\frac{2\pi u}{n} \end{pmatrix}$$

Однако, $\sin\frac{2\pi u}{n}$ может не принадлежать K, зато K заведомо принадлежит $\sin^2\frac{2\pi u}{n} = 1-\cos^2\frac{2\pi u}{n}$, поэтому в качестве решения выберем матрицу

$$\begin{pmatrix} \cos\frac{2\pi u}{n} & -\sin^2\frac{2\pi u}{n} \\ 1 & \cos\frac{2\pi u}{n} \end{pmatrix}$$

Итак, верен следующий вывод: в $SL_2(K)$ есть элемент порядка $n \Leftrightarrow \cos\frac{2\pi}{n} \in K$. ■

На результат этой задачи можно смотреть следующим образом: рассмотрим действие группы $SL_2(K)$ на плоскости: элементу конечного порядка этой группы соответствует пара собственных векторов, т.е. пара собственных прямых, которые в общем случае определены над $\overline{K}$. Эти прямые переставляются группой Галуа. Пара собственных значений, соответствующих этим собственным прямым, определена над основным полем (т.е. над K определены их сумма и произведение).

Такой подход к решению геометрических задач над незамкнутым полем состоит в том, что мы переходим к алгебраическому замыканию поля, в результате чего добавляется действие группы Галуа – если какой-то объект является инвариантным относительно действия группы Галуа, то этот объект является определенным над основным полем. Например, ни одна из собственных прямых в нашей задаче не определена над K, но пара этих прямых уже определена над K, значит, определена, например, и их точка пересечения.

Несепарабельные расширения.

Проблемы в данном рассуждении возникают, когда мы рассматриваем поле положительной характеристики. Например, рассмотрим $\mathbb{F}_2(t)$ – поле рациональных дробей над $\mathbb{F}_2$. Оказывается, что алгебраическое замыкание этого поля уже не будет

расширением Галуа (и вообще, не всякие конечные расширения будут расширениями Галуа).

В самом деле, рассмотрим многочлен $x^2 - t$ – он неприводим над $\mathbb{F}_2(t)$, поэтому $\mathbb{F}_2(t)[x]/(x^2 - t\ )$ – поле. Обозначим его $\mathbb{F}_2(\sqrt{t})$ – это расширение степени 2 поля $\mathbb{F}_2(t)$. Ранее, когда мы рассматривали расширения степени 2, то при автоморфизме поля один из корней соответствующего квадратного трехчлена отображался в другой, но у $\mathbb{F}_2(\sqrt{t})$ нет нетривиальных автоморфизмов, сохраняющих $\mathbb{F}_2(t)$: в самом деле, при автоморфизме $\sqrt{t}$ может перейти только в $\sqrt{t}$, поскольку $x^2 - t = (x - \sqrt{t})^2$

Проблема состоит в том, что $\sqrt{t}$ нельзя определить над полем $\mathbb{F}_2(t)$ (как мы это делали раньше для полей характеристики 0). Итак, $\mathbb{F}_2(\sqrt{t})$ – это расширение степени 2, которое не является расширением Галуа, кроме того, его нельзя поместить ни в какое расширение Галуа, несмотря на то, что это поле разложения многочлена $x^2 - t$ над $\mathbb{F}_2(t)$. Такие расширения называются несепарабельными (строгое определение сепарабельности см. ниже).

Определение. Многочлен $P(x) \in K[x]$ сепарабелен, если P не имеет кратных корней ни в каком расширении поля K. Эквивалентно: $(P, P') = 1$.

Бывают ли неприводимые несепарабельные многочлены? Пусть есть $P(x)$, такой что $(P(x), P'(x)) = Q(x)$, $\deg Q(x) > 0$. Отсюда следует, что $P(x)$ делится на $Q(x)$, т.е. $P(x) = \lambda Q(x)$, где $\lambda \in K$. Но $\deg P'(x) < \deg Q(x) = \deg P(x)$.

Ответ: неприводимые несепарабельные многочлены $\Longrightarrow P'(x) = 0$. В частности, $char\ K$ должна быть положительной (пусть она равна p), а сам многочлен имеет вид $a_n x^{np} + a_{n-1} x^{(n-1)p} + \cdots + a_1 x^p + a_0$.

Определение. Поле K совершенно, если все неприводимые многочлены над K сепарабельны.

Замечание. Все конечные поля совершенны. В самом деле: автоморфизм Фробениуса Ф: $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ сюръективен, т.е. из любого элемента $\mathbb{F}_{p^n}$ можно извлечь корень p-ой степени. Поэтому для конечных полей

$$a_n x^{np} + a_{n-1} x^{(n-1)p} + \cdots + a_1 x^p + a_0 = (\sqrt[p]{a_n} x^n + \sqrt[p]{a_{n-1}} x^{n-1} + \cdots + \sqrt[p]{a_1} x + \sqrt[p]{a_0})^p$$

Определение. Элемент $a \in L \supseteq K$ сепарабелен над K, если a – корень сепарабельного многочлена f над K. Эквивалентно: μ_a сепарабелен.

Определение. Расширение $L \supseteq K$ сепарабельно, если $\forall a \in L$ сепарабелен над K.

Замечание. Если $char\ K = 0$, то все неприводимые многочлены над K сепарабельны (если P – неприводимый многочлен, то P' - многочлен ненулевой степени, и условие $(P, P') = 1$ выполнено всегда). Следовательно, если $char\ K = 0$, то все алгебраические расширения сепарабельны.

Семинар 21. Некоторые вопросы теории Галуа.

Приведем решение задачи 5 из семинара 19:

Задача 5. Пусть L – поле разложения многочлена $x^n - 1$ над $\mathbb{Q}$. Найти $Gal\,(L/\mathbb{Q})$.

Решение.
Пусть ξ_n – первообразный корень n-ой степени из единицы. При всяком автоморфизме из $Gal\,(L/\mathbb{Q})$ первообразный корень ξ_n должен переходить в первообразный корень, т.е. $\xi_n \mapsto \xi_n^a$, где a взаимно просто с n. Отсюда следует, что $|Gal\,(L/\mathbb{Q})| = \varphi(n)$, где φ – функция Эйлера.

Так как:

- всякий автоморфизм из $Gal\,(L/\mathbb{Q})$ индуцирует автоморфизм группы $(1, \xi_n, \xi_n^2, \dots, \xi_n^{n-1}) \cong \mathbb{Z}/n\mathbb{Z}$,
- $|Aut\,(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$,

то $Gal\,(L/\mathbb{Q}) \cong Aut\,(\mathbb{Z}/n\mathbb{Z})$. Воспользуемся результатом, полученным на семинаре 3: пусть $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, тогда

$$\varphi(n) = \prod_{i=1}^{k} \varphi\left(p_i^{a_i}\right) = \prod_{i=1}^{k} \varphi\left(p_i^{a_i}\right)(p_i - 1)$$

и

$$Gal\,(L/\mathbb{Q}) \cong Aut\,(\mathbb{Z}/n\mathbb{Z}) \cong Aut\,(\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times Aut\,(\mathbb{Z}/p_2^{a_2}\mathbb{Z}) \times \cdots \times Aut\,(\mathbb{Z}/p_k^{a_k}\mathbb{Z}),$$

где:

- если p_i нечетное, то $Aut\,(\mathbb{Z}/p_i^{a_i}\mathbb{Z}) \cong \mathbb{Z}/p_i^{a_i-1}(p_i - 1)\mathbb{Z}$,
- если $p_i = 2$, то $Aut\,(\mathbb{Z}/2^{\alpha_0}\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha_0-2}\mathbb{Z})$.

■

При решении этой задачи мы использовали тот факт, что всякий автоморфизм имеет вид $\xi_n \mapsto \xi_n^a$, где a взаимно просто с n. Отсюда следует, что $|Gal\,(L/\mathbb{Q})| \leq \varphi(n)$. Докажем, что на самом деле $|Gal\,(L/\mathbb{Q})| = \varphi(n)$ (факт, который при решении задачи мы использовали без доказательства). Вначале докажем следующую лемму:

Лемма (Гаусса). Если $P(x)$ – многочлен с целыми коффициентами и $P(x) = f(x)g(x)$ над $\mathbb{Q}$, то его можно разложить на множители над $\mathbb{Z}$.

Доказательство.

Пусть $P(x) = f(x)g(x)$. Выберем $\tilde{f}(x)$, пропорциональный $f(x)$ так, что $\tilde{f}(x) \in \mathbb{Z}[x]$ и НОД коэффициентов $\tilde{f}(x)$ равен 1. Аналогично выберем $\tilde{g}(x)$ – получим $f(x) = a_1\tilde{f}(x)$ и $g(x) = a_2\tilde{g}(x)$, т.е. $P(x) = a_1a_2\tilde{f}(x)\tilde{g}(x)$.

Пусть $a_1a_2 = \frac{m}{n}$ – несократимая дробь, тогда $nP(x) = m\tilde{f}(x)\tilde{g}(x)$. Пусть k – простой делитель n, тогда рассматривая это равенство по модулю k, получаем $0 = \overline{m}\overline{\tilde{f}(x)}\overline{\tilde{g}(x)}$, при этом $\overline{m} \neq 0$, так как m и n взаимно просты, а $\overline{\tilde{f}(x)} \neq 0$ и $\overline{\tilde{g}(x)} \neq 0$, так как НОД коэффициентов $\tilde{f}(x)$ равен 1 и НОД коэффициентов $\tilde{g}(x)$ равен 1, т.е. все коффициенты этих многочленов не могут одновременно делиться на k. Получили противоречие (так как в $\mathbb{F}_k[x]$ нет делителей нуля), следовательно, у n нет простых делителей и $n = \pm 1$.

Итак, $P(x) = m\tilde{f}(x)\tilde{g}(x)$ – получили разложение $P(x)$ над $\mathbb{Z}$. ■

Пусть $f(x)$ – минимальный многочлен ξ_n, тогда $x^n - 1 = f(x)g(x)$ и можно считать, что у многочленов $f(x)$ и $g(x)$ целые коэффициенты. Покажем, что для любого p, взаимно простого с n, число ξ_n^p является корнем многочлена $f(x)$.

Так как многочлен $x^n - 1$ является сепарабельным: НОД$(x^n - 1, nx^{n-1}) = 1$, то он не имеет кратных корней. Пусть ξ_n^p – корень многочлена $g(x)$ над $\mathbb{Q}$, тогда ξ_n – корень многочлена $g(x^p)$ над $\mathbb{Q}$. Значит, $g(x^p)$ делится на $f(x)$ над $\mathbb{Q}$, но тогда $g(x^p)$ делится на $f(x)$ над $\mathbb{F}_p$, следовательно, и $(g(x))^p$ делится на $f(x)$ над $\mathbb{F}_p$. Значит, $(f(x), g(x)) \neq 1$, т.е. многочлен $x^n - 1$ не сепарабельный над $\mathbb{F}_p$ – противоречие. Таким образом, для любого p, взаимно простого с n, число ξ_n^p является корнем многочлена $f(x)$.

Следовательно, $f(x)$ – мимнимальный многочлен ξ_n и $\forall a$: $(a, n) = 1$ выполнено: ξ_n^a – корень $f(x)$, поэтому $\deg f(x) \geq \varphi(n)$. Рассмотрим L – поле разложения многочлена $x^n - 1$ над $\mathbb{Q}$. Имеем: $L \supset \mathbb{Q}(\xi_n) = \mathbb{Q}[x]/(f(x))$ – расширение степени $\geq \varphi(n)$. Но L – расширение Галуа, и $|Gal\,(L/\mathbb{Q})| \leq \varphi(n)$. Значит, $\mathbb{Q}(\xi_n) = L$, $|Gal\,(L/\mathbb{Q})| = \varphi(n)$, и все автоморфизмы L имеют вид $\xi_n \mapsto \xi_n^a$, где a взаимно просто с n.

Попутно мы доказали, что если $n \in \mathbb{N}$, то все первообразные корни n-ой степени из единицы являются корнями неприводимого многочлена с целыми коэффициентами. Этот многочлен называется круговым многочленом (многочленом деления круга). Приведем примеры нескольких круговых многочленов:

- $\Phi_1(x) = x - 1$
- $\Phi_2(x) = x + 1$
- $\Phi_3(x) = x^2 + x - 1$
- $\Phi_4(x) = x^2 + 1$
- $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

- $\Phi_6(x) = x^2 - x + 1$
- $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
- $\Phi_8(x) = x^4 + 1$

Задача. Пусть L – поле разложения многочлена $x^n - a$ над $\mathbb{Q}$. Какова степень расширения $L/\mathbb{Q}$?

Решение.
Корни многочлена $x^n - a$ – это $\sqrt[n]{a}$, $\xi_n\sqrt[n]{a}, \dots, \xi_n^{n-1}\sqrt[n]{a}$, следовательно, $\xi_n \in L$. Рассмотрим башню расширений $\mathbb{Q} \subset \mathbb{Q}(\xi_n) \subset L$. Имеем: $(\mathbb{Q}(\xi_n):\mathbb{Q}) = \varphi(n)$, также "в общем случае" $\big(L:\mathbb{Q}(\xi_n)\big) = n$, т.е. если многочлен $x^n - a$ неприводим над $\mathbb{Q}(\xi_n)$. Тогда по теореме о башне расширений получаем $(L:\mathbb{Q}) = n\varphi(n)$.

Однако, при присоединении ξ_n к полю $\mathbb{Q}$ многочлен $x^n - a$ мог перестать неприводимым над $\mathbb{Q}$. Например, рассмотрим многочлен $x^{10} - 5$. Имеем: $\mathbb{Q} \subset \mathbb{Q}(\xi_5)$ – расширение степени 4. Над $\mathbb{Q}(\xi_5)$ многочлен $x^{10} - 5$ уже раскладывается на множители:

$$x^{10} - 5 = \big(x^5 - \sqrt{5}\big)\big(x^5 + \sqrt{5}\big),$$

так как $\mathbb{Q}(\xi_5) \ni \frac{\xi_5 + \xi_5^4}{2} = \cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$, следовательно, $\sqrt{5} \in \mathbb{Q}(\xi_5)$.

Получаем $(L:\mathbb{Q}) = 20$ (а не $10 \cdot \varphi(10) = 40$). В самом деле, рассмотрим $\mathbb{Q}[x]/(x^{10} - 5) \cong \mathbb{Q}\big(\sqrt[10]{5}\big)$ – расширение степени 10. Так как степень расширения $L/\mathbb{Q}$ должна делиться на $(\mathbb{Q}(\xi_5):\mathbb{Q}) = 4$ и $\big(\mathbb{Q}\big(\sqrt[10]{5}\big):\mathbb{Q}\big) = 10$, то она должна делиться на $\text{НОК}\,(10, 4) = 20$. Больше 20 она тоже быть не может, так как многочлены $x^5 - \sqrt{5}$ и $x^5 + \sqrt{5}$ неприводимы над $\mathbb{Q}(\xi_5)$.

Отметим, что если L – поле разложения многочлена $x^p - a$ над $\mathbb{Q}$ (p – простое), то степень расширения $L/\mathbb{Q}$ всегда равна $p\varphi(p) = p(p-1)$. В самом деле, рассмотрим две башни расширений: $\mathbb{Q} \subset \mathbb{Q}(\xi_p) \subset L$ и $\mathbb{Q} \subset \mathbb{Q}(\sqrt[p]{a}) \subset L$. Имеем:

- $\big(\mathbb{Q}\big(\xi_p\big):\mathbb{Q}\big) = p - 1$ (так как $\varphi(p) = p - 1$)
- $\big(\mathbb{Q}\big(\sqrt[p]{a}\big):\mathbb{Q}\big) = p$ (так как многочлен $x^p - a$ неприводим над $\mathbb{Q}$, $\deg(x^p - a) = p$)

Так как числа p и $p-1$ взаимно просты, то $(L:\mathbb{Q}) \geq p(p-1)$, сдругой стороны, $(L:\mathbb{Q}) \leq p(p-1)$, так как $L \subseteq \mathbb{Q}\big(\sqrt[p]{a}, \xi_p\big)$. Следовательно, $(L:\mathbb{Q}) = p(p-1)$. ■

Задача. Найти минимальный многочлен $\xi_5 + \sqrt{5}$ над $\mathbb{Q}$.

Решение.

Как мы знаем, минимальный многочлен элемента a – это многочлен, корнями которого являются все элементы из орбиты действия группы Галуа, которой a принадлежит. Элементы, сопряженные ξ_5 – это $\xi_5,\ \xi_5^2,\ \xi_5^3,\ \xi_5^4$, элементы, сопряженные $\sqrt{5}$ – это $\pm\sqrt{5}$. Ранее мы выяснили, что $\sqrt{5} \in \mathbb{Q}(\xi_5)$, поэтому сопряженными для $\xi_5 + \sqrt{5}$ над $\mathbb{Q}$ будут числа $\xi_5 + \sqrt{5},\ \xi_5^2 - \sqrt{5},\ \xi_5^3 - \sqrt{5},\ \xi_5^4 + \sqrt{5}$. Тогда

$$\mu^{\mathbb{Q}}_{\xi_5+\sqrt{5}}(x) = \left(x - \xi_5 - \sqrt{5}\right)\left(x - \xi_5^2 + \sqrt{5}\right)\left(x - \xi_5^3 + \sqrt{5}\right)\left(x - \xi_5^4 - \sqrt{5}\right)$$

■

Напоследок скажем пару слов об определении расширения Галуа, использующем понятие сепарабельности. Как мы знаем, в поле характеристики 0 все неприводимые многочлены являются сепарабельными, а в поле характеристики p это не так. Пример неприводимого несепарабельного многочлена мы рассматривали на прошлом семинаре: это $x^2 - t$ для поля $\mathbb{F}_2(t)$.

Определение. Элемент $a \in L \supseteq K$ сепарабелен над K, если a – корень сепарабельного многочлена f над K. Эквивалентно: μ_a сепарабелен.

Определение. Элемент $a \in L \supseteq K$ чисто несепарабелен над K, если $\exists k\colon\ a^{p^k} \in K$.

Замечание. Не всякий чисто несепарабельный элемент является несепарабельным (элементы K являются сепарабельными, но при этом чисто несепарабельными).

Такая классификация хороша тем, что если $K \subset L$ – расширение полей, то все сепарабельные над K элементы образуют подполе в L, которое можно поместить в расширение Галуа. В свою очередь, чисто несепарабельные элементы тоже образуют подполе в L. Ранее мы давали такое определение расширения Галуа:

Определение. Конечное расширение полей $L \supset K$ называется расширением Галуа, если $|Aut_K L| = dim_K L$.

Это определение можно считать свойством, а определить расширение Галуа так:

Определение. Расширение $L \supset K$ сепарабельно, если все его элементы сепарабельны.

Определение. Расширение $L \supset K$ нормально, если любой минимальный многочлен элемента раскладывается на линейные множители.

Определение. Расширение $L \supset K$ называется расширением Галуа, если оно нормально и сепарабельно.

МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in

ЛЕКЦИИ УЧЕНЫХ МГУ