ГОМОМОРФИЗМЫ

Вместе с каждым классом объектов естественно рассматривать допустимый класс преобразований этих объектов, согласованный с их структурой. В случае групп и других алгебраических систем такие преобразования обычно называются гомоморфизмами. Первым стал сознательно использовать гомоморфизмы групп Джон Непер в самом начале XVII века. Понятие гомоморфизма было явным образом введено А. Капелли под названием обобщенный изоморфизм, сам термин гомоморфизм предложен Ф. Клейном.

§ 1. Определение гомоморфизма, мономорфизма, эпиморфизма, изоморфизма, эндоморфизма и автоморфизма. Примеры.

1. Основные определения и обозначения.

Определение. Пусть G и H — две группы; обозначим операции в этих группах знаками $*_G$ и $*_H$ соответственно. Отображение $\varphi : H \longrightarrow G$ называется **гомоморфизмом**, если для любых $x, y \in H$ выполнено равенство $\varphi(x *_H y) = \varphi(x) *_G \varphi(y)$.

Если мы предполагаем, что обе группы записаны мультипликативно, и опускаем, как и в предыдущих лекциях, знаки операций, то равенство, определяющее гомоморфизм, принимает вид $\varphi(xy) = \varphi(x)\varphi(y)$. Если бы G и H были аддитивными группами, то это равенство приняло бы форму $\varphi(x+y) = \varphi(x)+\varphi(y)$, а если, например, G мультипликативна, а H аддитивна, то форму $\varphi(xy) = \varphi(x)+\varphi(y)$. Словом, в каждом случае образ результата применения операции к двум элементам первой группы должен совпадать с результатом применения операции во второй группе к их образам.
Отметим несколько специальных случаев гомоморфизмов, которые имеют отдельное название (впрочем, не обязательно запоминать их все сразу). Гомоморфизм φ называется:
• **мономорфизмом**, если φ инъективен (от греческого '$\mu \grave{o} \nu o \varsigma$' — единственный);
• **эпиморфизмом**, если φ сюръективен (от греческого '$\grave{\epsilon}\pi\grave{\iota}$' — на);
• **изоморфизмом**, если φ биективен;
• **эндоморфизмом**, если $G = H$ (от греческого '$\grave{\epsilon}\nu\delta o\nu$' — внутрь);
• **автоморфизмом**, если $G = H$, а φ биективен (от греческого '$\alpha\grave{\upsilon}\tau\grave{o}\varsigma$' — сам, как в словосочетаниях сам по себе, для себя самого, etc.).

Таким образом, изоморфизм — это такой гомоморфизм, который является одновременно мономорфизмом и эпиморфизмом; эндоморфизм — это гомоморфизм группы в себя, а автоморфизм – это изоморфизм группы на себя.

Множество всех гомоморфизмов из группы H в группу G обозначается через $\mathrm{Hom}(H, G)$. Таким образом, запись $\varphi \in \mathrm{Hom}(H, G)$ означает, что φ — гомоморфизм из H в G. Множество всех изоморфизмов из H в G будет обозначаться через $\mathrm{Iso}(H, G)$. Через $\mathrm{End}(G)$ обозначается множество всех эндоморфизмов группы G в себя, а через $\mathrm{Aut}(G)$ — множество всех автоморфизмов G на себя. Композиция отображений превращает $\mathrm{Aut}(G)$ в группу, которую мы изучим более подробно в следующей лекции.

2. Основные примеры гомоморфизмов.

Приведем несколько примеров гомоморфизмов.

1. **Абсолютная величина, или модуль, числа.** Отображение $| \; | : \mathbb{R}^* \longrightarrow \mathbb{R}_{>0}$, $x \mapsto |x|$, сопоставляющее вещественному числу его абсолютную величину, является эпиморфизмом мультипликативной группы ненулевых вещественных чисел на группу положительных вещественных чисел. В самом деле, эти отображение сюрьективно, и $|xy| = |x||y|$. То же самое можно сказать про модуль комплексного числа: $| \; | : \mathbb{C}^* \longrightarrow \mathbb{R}_{>0}$. При этом снова $|zw| = |z||w|$. С комплексными числами связан еще один гомоморфизм - аргумент $\arg : \mathbb{C}^* \longrightarrow \mathbb{T}$; действительно, $\arg(zw) = \arg(z) + \arg(w)$, если аргумент $\arg(z)$ рассматривается как угол с точностью до $2\pi k$, $k \in \mathbb{Z}$.

2. **Знак числа.** Отображение $\mathrm{sign} : \mathbb{R}^* \longrightarrow \{\pm 1\}$, сопоставляющее вещественному числу его знак $\mathrm{sign}(x)$ является эпиморфизмом $\mathbb{R}^*$ на группу $\{\pm 1\}$. Это отображение также сюрьективно, и $\mathrm{sign}(xy) = \mathrm{sign}(x)\,\mathrm{sign}(y)$.

3. **Определитель.** Отображение
$$\det : \mathrm{GL}(n,R) \longrightarrow R^*$$
из группы квадратных обратимых матриц $\mathrm{GL}(n,R)$ степени n над **коммутативным** кольцом R в группу R^* обратимых элементов кольца R, сопоставляющий матрице x ее определитель $\det(x)$. Ключевое свойство, которое, собственно, и оправдывает введение этого понятия, состоит в том, что определитель произведения равен произведению определителей: $\det(xy) = \det(x)\det(y)$.

4. **Знак перестановки.** Этот пример будет подробно обсуждаться в одной из следующих лекций. Каждой перестановке $\pi \in S_n$ сопоставляется знак $\mathrm{sgn}(\pi)$, задающий гомоморфизм $\mathrm{sgn} : S_n \longrightarrow \{\pm 1\}$. Иными словами знак произведения равен произведению знаков: $\mathrm{sgn}(\sigma\pi) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\pi)$.

   Отступление: p-адический показатель и p-адическое нормирование. Пусть $G = \mathbb{Q}^*$ – мультипликативная группа рациональных чисел. Зафиксируем простое число $p \in \mathbb{P}$ и зададим отображение v_p группы $\mathbb{Q}^*$ в аддитивную группу $\mathbb{Z}^+$ целых чисел (в дальнейшем обозначаемую просто через $\mathbb{Z}$) следующим образом. Заметим, что каждое рациональное число $x \in \mathbb{Q}^*$ единственным образом представляется в виде $x = p^a m/n$, где $a \in \mathbb{Z}$, а m и n взаимно просты с p, и положим $v_p(x) = a$. Так построенное отображение $v_p : \mathbb{Q}^* \longrightarrow \mathbb{Z}$ называется **p-адическим показателем**. Легко видеть, что v_p обладает свойством логарифма, т. е. является гомоморфизмом мультипликативной структуры $\mathbb{Q}^*$ в аддитивную структуру $\mathbb{Z}$, а именно, $v_p(xy) = v_p(x) + v_p(y)$.

   Скомпоновав p-адический показатель с каким-либо гомоморфизмом, переводящим аддитивную структуру в мультипликативную, например, с обычной экспонентой с рациональным основанием из $\mathbb{Q}_+$, мы получим гомоморфизм мультипликативных групп. Обычно в качестве основания здесь выбирают $1/p$, так что $|x|_p = p^{-v_p(x)}$. Так построенное отображение $|\;|_p : \mathbb{Q}^* \longrightarrow \mathbb{Q}_+^*$ называется **p-адическим нормированием**. Ясно, что $|xy|_p = |x|_p|y|_p$. Легко проверить, что p-адическое нормирование обладает всеми обычными свойствами абсолютной величины (например, оно удовлетворяет **неравенству треугольника** $|x+y|_p \le |x|_p + |y|_p$ — а, в действительности, гораздо более замечательному **ультраметрическому неравенству** $|x+y|_p \le \max(|x|_p, |y|_p)$). Таким образом, $|\;|_p$ задает на $\mathbb{Q}$ метрику $d_p(x,y) = |x-y|_p$, называемую **p-адической метрикой**. Допределим $|\;|_p$ до гомоморфизма мультипликативных **моноидов** $\mathbb{Q} \longrightarrow \mathbb{Q}_+$ полагая $|0|_p = 0$). Пополнив $\mathbb{Q}$ относительно этой метрики, мы получаем поле $\mathbb{Q}_p$, называемое **полем p-адических чисел**, в котором можно развить аналог обычного вещественного анализа, называемый **p-адическим анализом**, играющий основную роль во многих разделах математики, особенно в теории чисел и алгебраической геометрии. В последнее время она все чаще используется в функциональном анализе и математической физике.

Сейчас мы приведем несколько примеров гомоморфизмов, естественно возникающих для любых групп.

5. Пусть H, G — две любые группы. Тогда отображение $1 : H \longrightarrow G$, переводящее все элементы группы H в единицу группы G является гомоморфизмом, который называется **тривиальным**.

   Упражнение 1. Покажите, что если H и G конечные группы взаимно простых порядков, то $\mathrm{Hom}(H,G) = \{1\}$.

6. Пусть G — любая группа. Тогда $\mathrm{id} : G \longrightarrow G$ является автоморфизмом группы G, называется **тождественным**.

7. **Степени элемента.** Легко видеть, что при фиксированном $g \in G$ отображение $\mathbb{Z} \longrightarrow G$, $n \mapsto g^n$, задает гомоморфизм аддитивной группы $\mathbb{Z}$ в G, иными словами, $g^{m+n} = g^m g^n$. Это значит, что для любого $g \in G$ существует единственный гомоморфизм $\mathbb{Z} \longrightarrow G$ такой, что $\varphi(1) = g$. Иными словами, $G \longleftrightarrow \mathrm{Hom}(\mathbb{Z}, G)$.

8. **Внутренние автоморфизмы.** Пусть G — любая группа и $g \in G$. Зададим для всех $x \in G$ их образ под действием отображения $I_g : G \longrightarrow G$ равенством $I_g(x) = gxg^{-1}$ (элемент gxg^{-1} часто обозначается также ${}^g x$ и называется сопряженным к x под действием g). Из ассоциативности умножения и свойств обратного элемента сразу вытекает, что I_g — гомоморфизм. В самом деле, для любых $x, y \in G$ имеем $I_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = I_g(x)I_g(y)$. Теперь из возможности сокращения в группе вытекает, что в действительности I_g является автоморфизмом. Автоморфизмы вида I_g называются **внутренними автоморфизмами** группы G. Обозначение I_g как раз и связано со словом `inner` — внутренний.

Пусть $H \leq G$ — любая подгруппа группы G. Тогда сопряжение при помощи любого $g \in N_G(H)$ оставляет H на месте и, следовательно, индуцирует автоморфизм $I_g|_H$ группы H. Важно обратить внимание, что с точки зрения самой группы H этот автоморфизм уже совсем не обязан быть внутренним! Особенно важен случай, когда $H \trianglelefteq G$, так что вообще любой элемент группы G индуцирует некоторый автоморфизм группы H.

Упражнение 2. Пусть $h, g \in G$. Определим отображение $I_{g+h} : G \longrightarrow G$, полагая

$$I_{h+g}(x) = {}^{h+g}x = {}^{h}x\,{}^{g}x = hxh^{-1}gxg^{-1}.$$

При каком условии это отображение будет эндоморфизмом группы G? Автоморфизмом этой группы?

Упражнение 3. Верно ли, что $I_{h+g} = I_{g+h}$?

Упражнение 4. Докажите, что $I_{f(g+h)} = I_{fg+fh}$ и $I_{(f+g)h} = I_{fh+gh}$.

Упражнение 5. При каком условии любой автоморфизм $I_g|_H$, $g \in N_G(H)$, является внутренним автоморфизмом группы H?

Ответ. Для этого необходимо и достаточно, чтобы имело место равенство $N_G(H) = HC_G(H)$.

9. **Гомоморфизмы, связанные с прямым произведением групп.** Пусть G и H — две произвольные группы. Рассмотрим множество всевозможных пар (g, h), состоящих из элемента g группы G и элемента h группы H. Это множество обозначается $G \times H$:

$$G \times H = \{(g, h) \mid g \in G,\ h \in H\}.$$

На множестве $G \times H$ рассмотрим операцию покомпонентного умножения:

$$(f_1, h_1)(f_2, h_2) = (f_1 f_2, h_2 h_2).$$

Кроме того, зададим $(f, h)^{-1} = (f^{-1}, h^{-1})$ и $e = (e, e)$. Ясно, что $G \times H$ относительно этих операций является группой. Эта группа называется **прямым произведением** групп G и H.

С прямым произведением групп $G \times H$ связаны четыре естественных гомоморфизма. Два гомоморфизма $\mathrm{pr}_G : G \times H \to G$, $(g, h) \mapsto g$, и $\mathrm{pr}_H : G \times H \to H$, $(g, h) \mapsto h$, называются **проекциями** $G \times H$ на G и H и являются эпиморфизмами. Еще два гомоморфизма являются мономорфизмами: $G \to G \times H$, $g \mapsto (g, e)$, и $H \to G \times H$, $h \mapsto (e, h)$. Более подробно прямое произведение групп будет обсуждаться в одной из следующих лекций.

3. Примеры гомоморфизмов, связанные с абелевыми группами.

В следующих примерах существенно, что группа G абелева.

1. **Обращение в абелевой группе.** Пусть G — аддитивно записанная абелева группа. Отображение $\mathrm{inv} : G \longrightarrow G$, переводящее элемент g в противоположный, является автоморфизмом этой группы.

2. **Возведение в степень в абелевой группе.** Зафиксируем $n \in \mathbb{Z}$ и рассмотрим отображение $\mathrm{pow}_n : G \longrightarrow G$, $g \mapsto g^n$. В случае, когда группа G абелева, это отображение является гомоморфизмом, т. е. $(hg)^n = h^n g^n$. В общем случае это, конечно, не обязательно так. Заметим, что если абелева группа G *конечна*, а n взаимно просто с $|G|$, то гомоморфизм $g \mapsto g^n$ является даже автоморфизмом (почему?).

Упражнение 6. Обратно, покажите, что если pow_2 гомоморфизм, то группа G абелева. Верно ли то же самое для pow_n, $n \geq 3$?

Упражнение 7. Докажите, что количество групповых гомоморфизмов C_m в C_n равно $\gcd(m, n)$.

Предположение следующего упражнения автоматически выполнено для всех $n \in \mathbb{Z}$ в случае, когда G — абелева группа.

Упражнение 8 (Цассенхауз)**.** Предположим, что G — группа такая, что для некоторого $n \in \mathbb{N}$ и всех $x, y \in G$ имеет место равенство $(xy)^n = x^n y^n$. Обозначим через $G^n = \{x^n \mid x \in G\}$ подмножество всех n-х степеней в G, а через $G_n = \{x \in G \mid x^n = 1\}$ — множество всех элементов из G, порядок которых делит n. Показать, что $G^n, G_n \trianglelefteq G$ и $|G^n| = |G : G_n|$.

Решение. В предположениях теоремы pow_n является эндоморфизмом группы G, $G^n = \mathrm{Im}(\mathrm{pow}_n)$, $G_n = \mathrm{Ker}(\mathrm{pow}_n)$, так что $G^n, G_n \leq G$, причем G_n нормальна. Так как pow_n коммутирует с внутренними автоморфизмами I_g, $g \in G$, $gx^n g^{-1} = (gxg^{-1})^n$, то G^n тоже нормальна. Утверждение об индексе — это частный случай теоремы о гомоморфизме $G^n \cong G/G_n$.

3. **Гомоморфизмы в абелеву группу.** Предположим, что группа H абелева и рассмотрим гомоморфизмы $\varphi, \psi \in \mathrm{Hom}(G, H)$. Определим $\varphi\psi \in \mathrm{Hom}(G, H)$ обычной формулой $(\varphi\psi)(x) = \varphi(x)\psi(x)$. Убедитесь, что эта операция превращает $\mathrm{Hom}(G, H)$ в абелеву группу. В случае, когда H записывается аддитивно, операция в $\mathrm{Hom}(G, H)$ тоже записывается аддитивно, т.к. $(\varphi + \psi)(x) = \varphi(x) + \psi(x)$.

Отступление: группы с одним или двумя автоморфизмами. Следующая задача предполагает знакомство с векторными пространствами. В ее решении использованы три независимые идеи, каждая из которых в отдельности достаточно проста.

Упражнение 9. Доказать, что любая группа, содержащая по крайней мере 3 элемента, имеет нетривиальные автоморфизмы.

Решение. Вот эти три идеи.
• Если G неабелева, то у нее есть нетривиальный внутренний автоморфизм.

• Если G абелева, то inv является автоморфизмом, который нетривиален в том и только том случае, когда найдется элемент g такой, что $2g \neq 0$.
• Таким образом, мы можем считать, что группа G обладает свойством $2g = 0$ для всех $g \in G$ и, значит, является векторным пространством над полем $\mathbb{F}_2$ из двух элементов. В векторном пространстве можно выбрать базис X (этот факт следует из так называемой аксиомы выбора), а так как $|G| \geq 3$, то $|X| \geq 2$ и, значит, X допускает нетривиальные биекции на себя. Любая такая биекция однозначно продолжается по линейности до автоморфизма G.

Упражнение 10. Доказать, что единственными группами, у которых ровно два автоморфизма, являются циклические группы порядков 3, 4 и 6.

4. Изоморфизмы групп.

Группы H и G называются **изоморфными**, если между ними можно установить изоморфизм, т.е. если существует отображение $\varphi : H \to G$, которое является изоморфизмом. Если это выполнено, то пишут $H \cong G$.

С точки зрения алгебры изоморфные объекты устроены одинаково и на определенном этапе своего развития алгебра как раз и понималась как изучение алгебраических систем **с точностью до изоморфизма**.

Вот несколько несложных примеров изоморфизмов:

- $\mathbb{R}_{>0} \cong \mathbb{R}^+$ (изоморфизмом будет экспонента),
- $\mathbb{C}^+ \cong \mathbb{R}^+ \times \mathbb{R}^+$ (сопоставьте комплексному числу его вещественную и мнимую часть),
- $\mathbb{C}^* \cong \mathbb{T} \times \mathbb{R}_{>0}$ (аргумент и модуль комплексного числа),
- $\mathbb{Z}/m\mathbb{Z} \cong \mu_n$ (числу $n \in \mathbb{Z}/m\mathbb{Z}$ сопоставьте комплексное число $\cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$).

Однако в общем случае понятие изоморфности является чрезвычайно тонким. Так, например, можно показать, что $\mathbb{C}^* \cong \mathbb{T}$, хотя этот изоморфизм отнюдь не очевиден.

Экспонента и логарифм. Обсудим более подробно первый из приведенных выше примеров. Удивительное свойство вещественных чисел состоит в том, что относительно сложения и умножения они устроены почти совершенно одинаково. Точнее, экспонента и логарифм задают взаимно обратные изоморфизмы между аддитивной группой $\mathbb{R}^+$ и группой $\mathbb{R}_{>0}$ положительных вещественных чисел относительно умножения. В самом деле, пусть exp и log обозначают экспоненту и натуральный логарифм:

$$\begin{aligned} \exp : \mathbb{R}^+ \longrightarrow \mathbb{R}_{>0}, \qquad & x \mapsto e^x, \\ \log : \mathbb{R}_{>0} \longrightarrow \mathbb{R}^+, \qquad & x \mapsto \log_e(x). \end{aligned}$$

Тогда, как хорошо известно, $\exp(x+y) = \exp(x)\exp(y)$, так что экспонента является гомоморфизмом аддитивной структуры в мультипликативную, и $\log(xy) = \log(x)+\log(y)$, так что и log является гомоморфизмом, на сей раз мультипликативной структуры в аддитивную. При этом $\exp(\log(x)) = x$ и $\log(\exp(x)) = x$, так что exp и log взаимно обратны и являются биекциями.

Так как складывать числа обычно гораздо легче, чем умножать, в докомпьютерную эру эти изоморфизмы широко использовались для практических приближенных вычислений физиками и инженерами (“таблицы логарифмов”, “логарифмические линейки”). Заметим, что вообще, для любого $a > 0$ имеет место равенство $a^{x+y} = a^x a^y$, а если, кроме того, $a \neq 1$, то $\log_a(x+y) = \log_a(x) + \log_a(y)$. Таким образом, $\mathbb{R}^+ \longrightarrow \mathbb{R}^*$, $x \mapsto a^x$, и $\mathbb{R}_{>0} \longrightarrow \mathbb{R}^+$, $x \mapsto \log_a(x)$, являются гомоморфизмами между аддитивной и мультипликативной структурами $\mathbb{R}$. Можно доказать, что никаких других таких *непрерывных* гомоморфизмов нет.

Упражнение 11. В своей книге "Теория групп конечного порядка" У. Бернсайд приводит 8 примеров групп, которые на первый взгляд задаются совершенно различным образом, но при этом все изоморфны S_3. Вот его примеры III, IV и V (§ 17, pp. 17–19). Убедитесь, что в каждом из приведенных трех случаев перечисленные замены переменных образуют группу относительно композиции. Проверьте, что все эти группы изоморфны S_3.

• 6 рациональных замен одной переменной:

$$x \mapsto x,\ x \mapsto \frac{1}{x},\ x \mapsto 1-x,\ x \mapsto \frac{x}{x-1},\ x \mapsto \frac{x-1}{x},\ x \mapsto \frac{1}{1-x};$$

• 6 полиномиальных замен двух переменных, где $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ — комплексный корень третьей степени из 1:

$$(x,y) \mapsto (x,y),\ (x,y) \mapsto (y,x),\ (x,y) \mapsto (\omega x, \omega^2 y),$$
$$(x,y) \mapsto (\omega^2 x, \omega y),\ (x,y) \mapsto (\omega y, \omega^2 x),\ (x,y) \mapsto (\omega y, \omega^2 x);$$

• 6 полиномиальных замен одной переменной по модулю 3:

$$x \mapsto x,\ x \mapsto -x,\ x \mapsto x+1,\ x \mapsto x-1,\ x \mapsto -x+1,\ x \mapsto -x-1.$$

Приведенный только что пример — типичная ситуация того, как конечные группы проникают в геометрию, комплексный анализ, алгебраическую геометрию, теорию дифференциальных уравнений и т. д.

Упражнение 12. Докажите, что $\mathbb{Q}_{>0} \ncong \mathbb{Q}^+$.

Решение. В $\mathbb{Q}^+$ есть квадратные корни, а в $\mathbb{Q}_{>0}$ нет $\sqrt{2}$.

Следующий пример возникает в школьной тригонометрии. Рассмотрим группу, порожденную трансляциями и сменой знака аргумента. Нас интересует действие этой группы на пространстве функций с периодом 2π. Ясно, что трансляция $x \mapsto x + 2\pi$ задает на этом пространстве *тождественный* сдвиг. Сейчас мы рассмотрим подгруппу, переставляющую функции $\pm\cos$, $\pm\sin$.

Упражнение 13. Убедитесь, что относительно композиции преобразования функций с периодом 2π, задаваемые на аргументах посредством $x \mapsto \pi/2 \pm x$, $x \mapsto \pi \pm x$, $x \mapsto 3\pi/2 \pm x$, $x \mapsto 2\pi \pm x$, образуют группу. Что это за группа?

§ 2. Лемма о том, что гомоморфизмы сохраняют обратный и нейтральный элементы. Ядро и образ.

5. Лемма о сохранении обратного и нейтрального элемента.

В определении гомоморфизма мы потребовали, чтобы отображение φ сохраняло произведение, но на самом деле тогда он сохраняет всю структуру группы. В следующей лемме мы обозначаем единичные элементы в обеих группах через e, вместо педантичных e_G и e_H.

Лемма 1. *Пусть $\varphi : G \longrightarrow H$ — гомоморфизм групп. Тогда $\varphi(e) = e$ и для любого $x \in G$ имеем $\varphi(x^{-1}) = \varphi(x)^{-1}$.*

Доказательство. В самом деле, $\varphi(e)^2 = \varphi(e^2) = \varphi(e) = \varphi(e)e$. Сокращая это равенство на $\varphi(e)$, получаем первое утверждение леммы. Пусть теперь $x \in G$. По определению гомоморфизма и уже доказанному $\varphi(x^{-1})\varphi(x) = \varphi(x^{-1}x) = \varphi(e) = e$, что и завершает доказательство. □

6. Образ и ядро гомоморфизма.

Сейчас мы построим две важнейшие подгруппы, связанные с гомоморфизмом.

Определение. Пусть $\varphi : H \longrightarrow G$ — гомоморфизм групп. Тогда **образ** φ — это обычный образ φ как отображения. Тем самым,

$$\mathrm{Im}(\varphi) = \{y \in G \mid \exists x \in H, \varphi(x) = y\}.$$

Легко видеть, что $\varphi(H)$ — подгруппа в G. В самом деле, $e = \varphi(e) \in \mathrm{Im}(\varphi)$. Если $y, z \in \mathrm{Im}(\varphi)$, то существуют $x, u \in H$ такие, что $\varphi(x) = y$, $\varphi(u) = z$. Тогда $\varphi(xu) = \varphi(x)\varphi(u) = yz$, так что $yz \in \mathrm{Im}(\varphi)$. Аналогично, $\varphi(x^{-1}) = \varphi(x)^{-1} = y^{-1}$, так что $y^{-1} \in \mathrm{Im}(\varphi)$. Ясно однако, что ядро не обязано быть нормальной подгруппой. В самом деле, рассмотрим *произвольную* подгруппу H группы G. Тогда H является образом канонического вложения $H \hookrightarrow G$.

Свяжем теперь с гомоморфизмом φ некоторую подгруппу в H.

Определение. Ядром гомоморфизма φ называется полный прообраз нейтрального элемента e группы G при этом гомоморфизме:

$$\mathrm{Ker}(\varphi) = \{x \in H \mid \varphi(x) = e\}.$$

Сейчас мы покажем, что в отличие от образа, ядро всегда является *нормальной* подгруппой в H.

Предложение 2. *Для любого гомоморфизма $\varphi : H \longrightarrow G$ имеем $\mathrm{Ker}(\varphi) \trianglelefteq H$.*

Доказательство. Докажем вначале, что G является подгруппой. В самом деле, $\varphi(e) = e$, так что $e \in \mathrm{Ker}(\varphi)$. Если $x, y \in \mathrm{Ker}(\varphi)$, то $\varphi(xy) = \varphi(x)\varphi(y) = e \cdot e = e$, так что $xy \in \mathrm{Ker}(\varphi)$. Наконец, если $x \in \mathrm{Ker}(\varphi)$, то $\varphi(x^{-1}) = \varphi(x)^{-1} = e^{-1} = e$, так что $x^{-1} \in \mathrm{Ker}(\varphi)$. Это и значит, что $\mathrm{Ker}(\varphi) \leq H$.

С другой стороны, если $x \in \mathrm{Ker}(\varphi)$, а $y \in H$, то

$$\varphi(yxy^{-1}) = \varphi(y)\varphi(x)\varphi(y^{-1}) = \varphi(y)\varphi(y)^{-1} = e.$$

Это и значит, что $\mathrm{Ker}(\varphi) \trianglelefteq H$. □

Легко видеть, что верно и обратное: любая нормальная подгруппа является ядром некоторого гомоморфизма. А именно, с каждым нормальным делителем $H \trianglelefteq G$ связана каноническая проекция $\pi_H : G \longrightarrow G/H$, $g \mapsto gH$. Ясно, что $H = \mathrm{Ker}(\pi_H)$. Таким образом, класс ядер гомоморфизмов совпадает с классом нормальных подгрупп.

Укажем ядра нескольких важнейших гомоморфизмов.

1. Пусть $\mathrm{pow}_n : G \longrightarrow G$, $x \mapsto x^n$, — возведение в n-ю степень. Тогда $\mathrm{Ker}(\mathrm{pow}_n) = G_n$ — множество элементов в G, порядок которых делит n.

2. Пусть $I : G \longrightarrow \mathrm{Aut}(G)$, $g \mapsto I_g$, гомоморфизм, сопоставляющий каждому элементу $g \in G$ соответствующий внутренний автоморфизм I_g. Тогда $\mathrm{Ker}(I) = C(G)$ — центр группы G.

3. Пусть $\det : \mathrm{GL}(n, K) \longrightarrow K^*$ — определитель, тогда $\mathrm{Ker}(\det) = \mathrm{SL}(n, K)$ — специальная линейная группа.

4. Пусть $\mathrm{sgn} : S_n \longrightarrow \{\pm 1\}$ — знак перестановки, тогда $\mathrm{Ker}(\mathrm{sgn}) = A_n$ — так называемая знакопеременная группа; мы обсудим этот пример более подробно в одной из следующих лекций.

§ 3. Теорема о гомоморфизме.

7. Теорема о гомоморфизме.

Сейчас мы покажем, что факторизация отображений замечательным образом согласована со структурой группы. Следующая теорема является одним из наиболее типичных и характерных результатов общей алгебры. В полной общности она была впервые сформулирована Эмми Нетер.

Теорема 3 (о гомоморфизме)**.** *Пусть $\varphi : H \longrightarrow G$ — гомоморфизм групп. Тогда*

$$\mathrm{Im}(\varphi) \cong H/\,\mathrm{Ker}(\varphi).$$

Доказательство. С каждым отображением $\varphi : H \longrightarrow G$ связано разбиение H на слои отображения φ, т.е. полные прообразы $\varphi^{-1}(g)$ различных элементов $g \in G$. Покажем, прежде всего, что в случае, когда φ является гомоморфизмом, слои являются в точности смежными классами по $\mathrm{Ker}(\varphi)$. Кстати, это объясняет, почему мы называем ядром гомоморфизма слой, содержащий e: в отличие от произвольных отображений для гомоморфизмов задание одного слоя однозначно определяет **все** остальные слои. В самом деле, если $\varphi(x) = \varphi(y)$, то $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = 1$ так что $xy^{-1} \in \mathrm{Ker}(\varphi)$. Но это и значит, что $x\,\mathrm{Ker}(\varphi) = y\,\mathrm{Ker}(\varphi)$ (вспомним, что ядро является нормальной подгруппой, так что безразлично, говорить о левых смежных классах или о правых). Обратно, если $x\,\mathrm{Ker}(\varphi) = y\,\mathrm{Ker}(\varphi)$, то $y = xh$ для некоторого $h \in \mathrm{Ker}(\varphi)$, так что $\varphi(y) = \varphi(xh) = \varphi(x)\varphi(h) = \varphi(x)$.

Эти соображения показывают, что сопоставление

$$\overline{x} = x\,\mathrm{Ker}(\varphi) \mapsto \varphi(x)$$

корректно определяет инъективное отображение $\overline{\varphi} : H/\,\mathrm{Ker}(\varphi) \longrightarrow G$, образ которого совпадает с $\mathrm{Im}(\varphi)$. Для завершения доказательства теоремы нам остается лишь проверить, что $\overline{\varphi}$ — гомоморфизм. В самом деле, пользуясь определением произведения классов, определением $\overline{\varphi}$ и тем, что φ — гомоморфизм, получаем

$$\overline{\varphi}(\overline{x} \cdot \overline{y}) = \overline{\varphi}(\overline{xy}) = \varphi(xy) = \varphi(x)\varphi(y) = \overline{\varphi}(\overline{x})\overline{\varphi}(\overline{y}),$$

что и завершает доказательство. □

Следствие 4. *Если $\varphi : H \longrightarrow G$ — эпиморфизм, то $G \cong H/\,\mathrm{Ker}(\varphi)$.*

8. Теорема об индуцированном гомоморфизме.

Теорема 5. *Пусть $\psi : G \longrightarrow G'$ — гомоморфизм групп, а нормальные подгруппы $H \trianglelefteq G$, $H' \trianglelefteq G'$ таковы, что $\psi(H) \leq H'$. Тогда ψ индуцирует гомоморфизм $\overline{\psi} : G/H \longrightarrow G'/H'$, $\overline{\psi}(xH) = \psi(x)H'$.*

Доказательство. Прежде всего, необходимо проверить корректность этого определения. Для этого заметим, что если $xH = yH$, то по условию на ψ имеем $\psi(x)^{-1}\psi(y) = \psi(x^{-1}y) \in H'$, так что $\psi(x)H' = \psi(y)H'$. Осталось убедиться в том, что $\overline{\psi}$ гомоморфизм. В самом деле,

$$\overline{\psi}(xH \cdot yH) = \overline{\psi}(xyH) = \psi(xy)H' = \psi(x)\psi(y)H' = (\psi(x)H')(\psi(y)H') = \overline{\psi}(xH)\overline{\psi}(yH).$$

□

Следствие 6. *Если в условиях теоремы $H = \psi^{-1}(H')$, то гомоморфизм $\overline{\psi} : G/H \longrightarrow G'/H'$ инъективен. Если, кроме того, ψ сюръективен, то $\overline{\psi}$ изоморфизм.*

9. Примеры применения теоремы о гомоморфизме. Фактически, некоторые примеры применения теоремы о гомоморфизме уже возникали ранее, когда мы обсуждали примеры фактор-групп. Вот еще несколько типичных примеров.

1. **Гомоморфизмы знака и модуля числа.** Напомним, что мы ввели эпиморфизм $|\ | : \mathbb{R}^* \longrightarrow \mathbb{R}_{>0}$, $x \mapsto |x|$, сопоставляющий вещественному числу его абсолютную величину. Так как $\mathrm{Ker}(|\ |) = \{\pm 1\}$, по следствию из теоремы о гомоморфизме имеем $\mathbb{R}^*/\{\pm 1\} \cong \mathbb{R}_{>0}$. Аналогично, эпиморфизм $\mathrm{sign} : \mathbb{R}^* \longrightarrow \{\pm 1\}$, сопоставляющее вещественному числу его знак, индуцирует изоморфизм $\mathbb{R}^*/\mathbb{R}_{>0} \cong \{\pm 1\}$. На самом деле, конечно, $\mathbb{R}^* \cong \mathbb{R}_{>0} \times \{\pm 1\}$, и рассмотренные гомоморфизмы соотвествуют проекциям прямого произведения.

2. **Параметризация группы поворотов.** Рассмотрим гомоморфизм $\mathbb{R}^+ \to \mathbb{T}$, который сопоставляет вещественному числу x поворот на x радиан вокруг некоторой фиксированной точки плоскости. Ясно, что ядро этого гомоморфизма состоит из целых кратных числа 2π. Следовательно, по теореме о гомоморфизме (или по ее следствию) имеет место $\mathbb{R}^+/2\pi\mathbb{Z} \cong \mathbb{T}$.

3. **Классификация циклических групп.** Пусть G — произвольная группа. Каждому $g \in G$ соответствует гомоморфизм $\varphi : \mathbb{Z} \longrightarrow G$, $n \mapsto g^n$. По теореме о гомоморфизме $\mathbb{Z}/\mathrm{Ker}(\varphi) \cong \langle g \rangle$, где $\langle g \rangle$ — подгруппа группы G, порожденная g. Если g имеет бесконечный порядок, то $\mathrm{Ker}(\varphi) = \{0\}$, и $\mathbb{Z} \cong \langle g \rangle$. Если же $\mathrm{o}(g) = m$, то $\mathrm{Ker}(\varphi) = m\mathbb{Z}$, и $\mathbb{Z}/m\mathbb{Z} \cong \langle g \rangle$. Отсюда легко вытекает следующая теорема.

Теорема 7. *Пусть G — циклическая группа. Если порядок G бесконечен, то $G \cong \mathbb{Z}$. Если $|G| = m$, то $G \cong \mathbb{Z}/m\mathbb{Z}$.*

Дополнение 1: Матричные гомоморфизмы

Следующие примеры гомоморфизмов предполагают знакомство с умножением матриц.
• **Однопараметрические подгруппы.** Пусть R — произвольное кольцо (например, $\mathbb{Z}$ или $\mathbb{R}$), тогда отображение

$$d_{12} : R^* \longrightarrow \mathrm{GL}(2, R), \qquad x \mapsto \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix},$$

является гомоморфизмом, т. е. $d_{12}(xy) = d_{12}(x)d_{12}(y)$ для любых $x, y \in R^*$.
• **Однопараметрические подгруппы, bis.** Следующий исключительно важный пример показывает, что в умножение матриц вплетено не только умножение, но и *сложение* в основном кольце. Отображение

$$t_{12} : R^+ \longrightarrow \mathrm{GL}(2, R), \qquad x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$

является гомоморфизмом аддитивной структуры в мультипликативную, т. е. $t_{12}(x + y) = t_{12}(x)t_{12}(y)$ для любых $x, y \in R$.
• Пусть K — поле характеристики $\neq 2$. Тогда

$$K^+ \longrightarrow \mathrm{SL}(2, K), \qquad x \mapsto \frac{1}{2}\begin{pmatrix} x + x^{-1} & x - x^{-1} \\ x - x^{-1} & x + x^{-1} \end{pmatrix},$$

является гомоморфизмом групп (проверьте!)

Сейчас для поля $K = \mathbb{R}$ вещественных чисел мы построим еще два примера гомоморфизмов из аддитивной группы поля в мультипликативную группу матриц. Это вытекает из теорем сложения для тригонометрических и гиперболических функций соответственно.
• **Тригонометрические функции.** Отображение

$$\mathbb{R}^+ \longrightarrow \mathrm{GL}(2, \mathbb{R}), \qquad x \mapsto \begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix},$$

является гомоморфизмом. Этот гомоморфизм сопоставляет x эвклидов поворот на угол x.
• **Гиперболические функции.** Отображение

$$\mathbb{R}^+ \longrightarrow \mathrm{GL}(2,\mathbb{R}), \qquad x \mapsto \begin{pmatrix} \mathrm{ch}(x) & \mathrm{sh}(x) \\ \mathrm{sh}(x) & \mathrm{ch}(x) \end{pmatrix},$$

является гомоморфизмом. Этот гомоморфизм сопоставляет x лоренцев поворот на угол x.

В действительности, не будет большим преувеличением сказать, что **все** классические функции **только** потому и интересны, что они являются гомоморфизмами или компонентами гомоморфизмов важнейших алгебраических структур.

Упражнение 14 (пифагоровы тройки)**.** Пусть K — поле характеристики $\neq 2$, в котором -1 не является квадратом (например, $K = \mathbb{R}$). Определим на множестве K^2 умножение по правилу умножения комплексных чисел $(a,b)(c,d) = (ac - bd, ad + bc)$. Убедитесь, что отображение

$$K^2 \setminus \{(0,0)\} \longrightarrow \mathrm{SL}(2,K), \qquad x \mapsto \frac{1}{a^2+b^2} \begin{pmatrix} a^2 - b^2 & 2ab \\ -2ab & a^2 - b^2 \end{pmatrix},$$

является гомоморфизмом групп.

Упражнение 15 (присоединенное представление SL_2)**.** Пусть R — коммутативное кольцо с 1. Доказать, что отображение

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{pmatrix}$$

представляет собой гомоморфизм групп $\mathrm{GL}(2,R) \longrightarrow \mathrm{GL}(3,R)$.

• **Миноры.** Сопоставим матрице $x \in \mathrm{GL}(n,R)$ матрицу $\bigwedge^m(x)$, составленную из всех ее миноров m-го порядка, упорядоченных лексикографически. Матрица $\bigwedge^m(x)$ называется **m-й внешней степенью** матрицы x. Одна из основных теорем теории определителей, **теорема Бине—Коши**, утверждает, что отображение $\bigwedge^m$ является гомоморфизмом группы $\mathrm{GL}(n,R)$ в группу $\mathrm{GL}(C_n^m, R)$, а именно,

$$\textstyle\bigwedge^m(xy) = \bigwedge^m(x)\bigwedge^m(y).$$

Дополнение 2: Линейные представления групп

Сейчас мы на чисто лингвистическом уровне введем понятие линейного представления группы. Это понятие существовало всегда, но было впервые *явно* определено в работе Георга Фробениуса 1896 года в процессе размышлений над задачей о групповых определителях, предложенной Дедекиндом. В 1896–1910 годах Фробениус, Бернсайд и Шур в основных чертах завершили создание классической (полупростой) теории представлений *конечных* групп, по существу эквивалентной теории полупростых алгебр, созданной примерно в то же время, в 1893–1908 годах, Федором Молиным, Эли Картаном и Веддербарном.

1. Линейные представления. Пусть R — коммутативное кольцо с $1 \neq 0$. В действительности, при доказательстве большинства содержательных результатов предполагается, что основное кольцо $R = K$ является полем — или, по крайней мере, областью целостности. Гомоморфизм $\varphi : G \longrightarrow \mathrm{GL}(n,R)$ называется **представлением** группы G над кольцом R, при этом n называется **степенью** этого представления.

Образ $\varphi(g)$ элемента $g \in G$ под действием φ будем обозначать через φ_g. По определению $\varphi_{hg} = \varphi_h\varphi_g$ для любых $h, g \in G$. Тем самым, $\varphi_e = e$ и $\varphi_{g^{-1}} = (\varphi_g)^{-1}$. К представлениям применима вся обычная терминология, используемая для гомоморфизмов, например, совершенно ясно, что подразумевается под ядром или образом представления. Если φ — мономорфизм, то такое представление называется **точным**.

Напомним, что как обычно, через x_{ij} обозначается элемент матрицы x в позиции (i,j), $1 \leq i,j \leq n$. Таким образом, $x = (x_{ij})$. Функция $\varphi_{ij} : G \longrightarrow R$, $g \mapsto \varphi(g)_{ij}$, называется **матричным элементом** представления. По определению $\varphi_{ij}(g) = \varphi(g)_{ij}$.

Упражнение 16. Напишите, какие условия на φ_{ij} накладываются тем условием, что φ — гомоморфизм.

Комментарий. Математики часто называют **представлением** группы G ее гомоморфизм в *какую-то* группу, в которой они умеют считать. Особенно часто этот термин используется для гомоморфизмов в группу преобразований *какого-то* множества X — совсем не обязательно векторного пространства или модуля! Так, в теории групп

принято говорить о **перестановочных представлениях**, т. е. гомоморфизмах $G \longrightarrow S_n$ в симметрическую группу, **представлениях автоморфизмами**, т. е. гомоморфизмах $G \longrightarrow \mathrm{Aut}(H)$, в группу автоморфизмов какой-то другой группы H и т. д. Вообще, группы *представляют* практически чем угодно: симметриями геометрических объектов; бирациональными преобразованиями; преобразованиями, сохраняющими порядок и т. д. В этом случае, чтобы подчеркнуть, что речь идет именно о гомоморфизмах в полную линейную группу, используется термин **линейные представления** или **матричные представления**.
Вот важнейший пример представления, которое есть у любой группы:

• Отображение $G \mapsto R^* = \mathrm{GL}(n, R)$, переводящее каждый элемент группы G в e, называется **тривиальным** представлением. Тривиальное представление размерности 1 называется **единичным** или **главным**.
В действительности, у *общих* групп никаких других (конечномерных) представлений, кроме тривиальных, может и не быть. Однако, например, у конечных групп много интересных представлений.

2. Эквивалентность представлений. Классическая теория всегда рассматривает представления *с точностью до сопряженности* в $\mathrm{GL}(n, R)$. Линейные представления, которые сопряжены как гомоморфизмы, принято называть **эквивалентными**. Иными словами, если $\varphi \sim \psi$ два эквивалентных представления, то найдется $x \in \mathrm{GL}(n, R)$ такое, что $x\varphi_g x^{-1} = \psi_g$. Важно подчеркнуть, что это x одно и то же для всех g. Условие эквивалентности можно переписать в виде $x\varphi_g = \psi_g x$. Матрица x, удовлетворяющая этому условию, называется **сплетающим оператором**. Таким образом, два представления эквивалентны, если для них существует *обратимый* сплетающий оператор.

В дальнейшем мы не будем различать эквивалентные представления. Например, когда мы говорим, что φ и ψ — *различные* представления, конечно имеется в виду, что они *не эквивалентны*.

Упражнение 17. Пусть $G = \langle g \rangle \cong C_2$, а $R = \mathbb{Z}$. Сколько различных среди представлений

$$g \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad g \mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad g \mapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad g \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}?$$

3. Разложимость и приводимость представлений. Сейчас мы введем простейшую конструкцию над представлениями. Пусть $\varphi : G \longrightarrow \mathrm{GL}(m, R)$ и $\psi : G \longrightarrow \mathrm{GL}(n, R)$ — два представления одной и той же группы G над одним и тем же кольцом R, степеней m и n, соответственно. Тогда их **прямая сумма** $\varphi \oplus \psi$ — это следующее представление степени $m + n$:

$$\varphi \oplus \psi : G \longrightarrow \mathrm{GL}(m + n, R), \qquad g \mapsto \varphi(g) \oplus \psi(g) = \begin{pmatrix} \varphi(g) & 0 \\ 0 & \psi(g) \end{pmatrix}.$$

Представление называется **неразложимым**, если его нельзя разложить в прямую сумму двух представлений, в противном случае оно называется **разложимым**. Напомним, что представления всегда рассматриваются с точностью до сопряженности в $\mathrm{GL}(n, R)$. Поэтому условие неразложимости означает, что не существует матрицы $x \in \mathrm{GL}(n, R)$, сопряжение при помощи которой одновременно приводит все матрицы из $\varphi(G)$ к одному и тому же клеточно-диагональному виду:

$$x\varphi(G)x^{-1} \leq \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$$

Пусть теперь $R = K$ — поле. Введем важнейший класс представлений более узкий, чем класс неразложимых представлений. Представление $\varphi : G \longrightarrow \mathrm{GL}(n, K)$ называется **неприводимым**, если не существует такой матрицы $x \in \mathrm{GL}(n, R)$, чтобы все матрицы из $\varphi(G)$ одновременно приводились к (одному и тому же) клеточно-треугольному виду $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. В противном случае представление называется **приводимым**.
Представление, являющееся конечной прямой суммой неприводимых, называется **вполне приводимым**.

Из определения ясно, что каждое неприводимое представление неразложимо, но, как показывают элементарные примеры, обратное *безнадежно* неверно. Пусть, скажем, $p \in \mathbb{P}$, $G = \langle g \rangle \cong C_p$, а $K = \mathbb{F}_p$ — поле из p элементов. Приводимое представление

$$G \longrightarrow \mathrm{GL}(2, K), \qquad g \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

неразложимо (в группе $\mathbb{F}_p^*$ нет элементов порядка p, и поэтому матрица порядка p не может быть диагонализована).

Пусть φ — приводимое представление группы G степени n. По определению найдется такое $x \in \mathrm{GL}(n,K)$, что все элементы $\varphi(g)$, $g \in G$, одновременно приводятся к одному и тому же *верхнему* клеточно-треугольному виду

$$x\varphi(g)x^{-1} = \begin{pmatrix} \psi(g) & * \\ 0 & \rho(g) \end{pmatrix},$$

где $\psi(g) \in \mathrm{GL}(m,K)$, а $\rho(g) \in \mathrm{GL}(n-m,K)$, для некоторого m, $1 \le m \le n-1$. Легко видеть, что ψ и ρ являются представлениями группы G степеней m и $n-m$, соответственно. При этом, как мы только что заметили, в общем случае нельзя ожидать, чтобы все $*$ в правом верхем углу равнялись 0. Если этого все же можно добиться, то это, как раз, и будет значить, что представление φ является прямой суммой ψ и ρ, которые входят в него на равных правах.

В общем случае, однако, роль ψ и ρ совершенно разная. При этом ψ называется **подпредставлением** φ, а ρ — **фактор-представлением** φ. Как запомнить, кто есть кто? Ну, это будет ясно после чтения следующего параграфа. А пока постарайтесь понять, кто будет подпредставлением, а кто фактор-представлением, если все матрицы $\varphi(g)$ одновременно приведены к *нижнему* клеточно-треугольному виду:

$$x\varphi(g)x^{-1} = \begin{pmatrix} \psi(g) & 0 \\ & \rho(g) \end{pmatrix}.$$

Если же всякое фактор-представление одновременно является подпредставлением, или, что то же самое, всякое неразложимое представление автоматически неприводимо (в сочетании с некоторыми условиями минимальности, гарантирующими выполнение теоремы Крулля—Ремака—Шмидта), то говорят о **полной приводимости**.

4. Представления конечных групп.

Сейчас мы немного поговорим о представлениях конечных групп, чтобы понимать, что имеется в виду, когда говорят, что какой-то результат о конечных группах доказывается с помощью теории представлений. Доказательства всех этих и многих других близких результатов можно найти в любом учебнике по теории представлений конечных групп.

Любая конечная группа G имеет привилегированное представление, содержащее в себе все неприводимые представления. А именно, пусть $V = R[G]$, по определению V представляет собой свободный R-модуль ранга $|G|$ с базисом из элементов $h \in G$ (если R — поле, то V — векторное пространство размерности $|G|$). Группа G действует на V *слева* несколькими различными *естественными* способами. Отметим два из них:

• $g(\sum a_h h) = \sum a_h gh$. Получающийся при этом G-модуль V называется **левым регулярным представлением** группы G.

• $g(\sum a_h h) = \sum a_h hg^{-1}$. Получающийся при этом G-модуль V называется **правым регулярным представлением** группы G.

Обратите внимание на переход к обратному во втором из этих примеров! Это делается потому, что мы хотим построить именно *гомоморфизм* $G \longrightarrow \mathrm{GL}(n,R)$. А теперь ответьте на следующий вопрос: левое и правое регулярное представление — это два *разных* представления или одно и то же? В дальнейшем регулярное представление группы G обозначается через reg_G.

Полезно понять, как именно это представление выглядит в матрицах. Сделать это можно либо концептуально, либо формульно. Формула выглядит примерно так. Пусть $\delta = \delta_e : G \longrightarrow R$ — **дельта-функция**, сконцентрированная в $e \in G$. Напомним, что $\delta(g) = 1$, если $g = e$, и $\delta(g) = 0$ иначе.

Упражнение 18. Докажите, что если $G = \{g_1, g_2, \dots, g_n\}$, то в базисе $g_1, \dots, g_n$ левое регулярное представление задается следующим образом:

$$g \mapsto \begin{pmatrix} \delta(g_1^{-1}gg_1) & \delta(g_1^{-1}gg_2) & \dots & \delta(g_1^{-1}gg_n) \\ \delta(g_2^{-1}gg_1) & \delta(g_2^{-1}gg_2) & \dots & \delta(g_2^{-1}gg_n) \\ \dots & \dots & \dots & \dots \\ \delta(g_n^{-1}gg_1) & \delta(g_n^{-1}gg_2) & \dots & \delta(g_n^{-1}gg_n) \end{pmatrix}$$

Напишите аналогичную формулу для правого регулярного представления.

А *на самом деле* происходит следующее. Группа G действует левыми (или правыми) сдвигами на себе.

Это определяет *перестановочное* представление $G \longrightarrow S_n$. Сопоставляя каждой перестановке соответствующую матрицу перестановки, мы и получим левое/правое регулярное представление.

Следующий результат быз доказан Х. Машке в 1898 году.

Теорема 8 (Машке). *Пусть G — конечная группа, а K — поле характеристики p. Если p не делит $|G|$, то для представлений G над K неразложимость эквивалентна неприводимости.*

В частности, в этой ситуации *все* представления вполне приводимы! В случае, когда p не делит $|G|$ принято говорить об **обыкновенных представлениях**. Им противопоставляются **модулярные представления**, изучение которых было начато Рихардом Брауэром, т. е. представления над полем характеристики p, делящей $|G|$. Для модулярных представлений утверждение теоремы становится безнадежно неверным.

Предположим теперь, что K — алгебраически замкнутое поле, характеристика которого не делит $|G|$. В качестве поля K заведомо можно взять, например, поле $\mathbb{C}$ комплексных чисел. Следующие результаты были в основном доказаны Фробениусом и Бернсайдом между 1896 и 1904 годами.

• Количество различных неприводимых представлений G над K равно количеству классов сопряженности элементов группы G.

В контексте теории колец следующие утверждения иногда называются **теоремой Веддербарна**.

• Каждое неприводимое представление G над K входит в разложение reg_G в качестве прямого слагаемого с кратностью, равной его степени.

• Пусть теперь $\varphi_1, \ldots, \varphi_s$ суть все различные неприводимые представления группы G над полем K, а $n_1, \ldots, n_s$ — степени этих представлений. Тогда

$$|G| = n_1^2 + \ldots + n_s^2.$$

А вот последний элемент, которого в сочетании с двумя предыдущими обычно достаточно, чтобы определить степени всех неприводимых представлений для небольших групп.

• Если $H \trianglelefteq G$ — *абелев* нормальный делитель G, то степень n любого неприводимого представления группы G делит $|G : H|$. В частности, n делит $|G : C(G)|$.

Часто достаточно даже того, что n делит $|G|$. Скажем, в группе S_3 три класса сопряженных элементов. Поэтому у группы S_3 ровно три неприводимых комплексных представления, а их степени n_1, n_2, n_3 подчинены условию $n_1^2 + n_2^2 + n_3^2 = 6$. Ясно, что единственной возможностью является случай $n_1 = n_2 = 1$ и $n_3 = 2$. Разумеется, все эти представления нам уже известны, это главное представление, знак и представление S_3 как группы симметрий правильного треугольника.

Фробениус также ввел специальный инструмент, позволяющий не различать эквивалентные представления. А именно, **характером** представления $\varphi : G \longrightarrow \mathrm{GL}(n, R)$ называется функция $\chi_\varphi : G \longrightarrow R$, $g \mapsto \mathrm{tr}(\varphi_g)$. Ясно, что характер постоянен на классах сопряженных элементов. Характер неприводимого представления называется **неприводимым характером**.

Следующий результат объясняет, что для *конечных* групп над полем характеристики 0 вместо классов эквивалентности представлений можно говорить о характерах.

Теорема 9. *Если G — конечная группа, а K — поле характеристики 0, то*

$$\varphi \sim \psi \quad \Longleftrightarrow \quad \chi_\varphi = \chi_\psi.$$

Пусть теперь K — алгебраически замкнутое поле характеристки 0. В этом случае число различных неприводимых характеров равно числу классов сопряженности группы G, которое, в свою очередь, равно размерности пространства центральных функций на G. Совпадение двух чисел в математике редко бывает случайным. И действительно, Фробениус доказал, что в этом случае неприводимые характеры образуют базис пространства центральных функций. На этом, в сочетании с различными уравнениями, связывающими значения неприводимых характеров (соотношения ортогональности и т. д.) вкупе с арифметическими условиями на эти значения (целочисленность, делимость и т. д.) как раз и основаны небанальные приложения теории представлений в теории конечных групп. Например, пользуясь этими условиями часто удается строить в группе G нетривиальные нормальные подгруппы (как ядра неприводимых представлений). Именно так и доказываются теорема Фробениуса о нормальном дополнении и pq-теорема Бернсайда.