ТЕОРЕМЫ ОБ ИЗОМОРФИЗМЕ И ГРУППА АВТОМОРФИЗМОВ

§ 1. Теоремы об изоморфизме

В этом параграфе мы докажем несколько важнейших следствий теоремы о гомоморфизме, иллюстрирующих ее использование.

1. Первая Теорема об изоморфизме.

Сейчас мы докажем важнейший результат, обычно называемый в учебной литературе **первой теоремой об изоморфизме**. В специальной литературе его еще часто называют **теоремой Нетер об изоморфизме**. В общем виде, для произвольных групп с операторами этот результат был сформулирован в работе Эмми Нетер 1929 года. Впрочем, стоит отметить, что для конечных групп этот результат содержится уже в работе Гельдера 1889 года, а для абелевых групп — в приложении Дедекинда к изданию 1894 года лекций Дирихле по теории чисел.

Прежде всего заметим, что произведение по Минковскому

$$FH = \{fh \mid f \in F,\ h \in H\}$$

произвольной подгруппы $F \leq G$ на нормальную подгруппу $H \trianglelefteq G$ является подгруппой в G. Этот факт уже обсуждался ранее, но мы приведем другое доказательство. Пусть $\pi : G \longrightarrow G/H$ — каноническая проекция. Тогда $FH = \pi^{-1}(\pi(F)) = \cup fH$, $f \in F$. Как образ, так и прообраз подгруппы при гомоморфизме являются подгруппами (проверьте это!).

Теорема 1 (первая теорема об изоморфизме, теорема Нетер)**.** *Пусть $H \trianglelefteq G$ — нормальная подгруппа в группе G, а $F \leq G$ — произвольная подгруппа. Тогда $H \cap F \trianglelefteq F$ и имеет место изоморфизм*

$$F/F \cap H = FH/H.$$

Доказательство. Рассмотрим гомоморфизм

$$\varphi : F \longrightarrow FH \longrightarrow FH/H, \qquad f \mapsto fH,$$

являющийся композицией вложения и канонической проекции. Так как любой правый смежный класс FH по H представляется в виде $(fh)H = fH$ для некоторых $f \in F$, $h \in H$, гомоморфизм φ сюръективен. Ясно, что $f \in F$ в том и только том случае лежит в $\mathrm{Ker}(\varphi)$, когда $f \in H$. Таким образом $\mathrm{Ker}(\varphi) = F \cap H$, и для завершения доказательства осталось лишь сослаться на теорему о гомоморфизме. $\square$

Следующая задача иллюстрирует типичное использование теоремы Нетер.

Упражнение 1. Подгруппа $H \leq G$ называется **холловской**, если порядок $|H| = m$ подгруппы H взаимно прост с ее индексом $n = |G : H|$. Докажите, что если $H \trianglelefteq G$ — холловский нормальный делитель группы G, то H является *единственной* подгруппой в G порядка m.

Решение. Пусть $F \leq G$ — другая подгруппа порядка m. Тогда $|FH/H|$ делит $|G : H| = n$, а $|F : F \cap H|$ делит $|F| = m$. Но ведь из теоремы об изоморфизме следует, что $|FH/H| = |F : F \cap H|$. Тем самым $FH = H$ и, значит, $F \leq H$.

2. Вторая Теорема об изоморфизме.

Пусть $F \trianglelefteq G$. Из теоремы о гомоморфизме вытекает, что сопоставление $H \mapsto H/F$ определяет биекцию множества $L(G, F)$ **промежуточных подгрупп** H, $F \leq H \leq G$, с множеством $L(G/F, 1)$ **всех** подгрупп в фактор-группе G/F. Оказывается, при этом соответствии нормальным подгруппам отвечают нормальные подгруппы.

Лемма 2. *Пусть $F \leq H \leq G$, причем $F \trianglelefteq G$. Тогда $H \trianglelefteq G$ в том и только том случае, когда $H/F \trianglelefteq G/F$.*

Доказательство. Возьмем произвольные элементы $gF \in G/F$ и $hF \in H/F$, где $g \in G$ и $h \in F$ соответственно. Так как F нормальна в G, то

$$(gF)^{-1}(hF)(gF) = (g^{-1}hg)F.$$

Ясно, что этот класс в том и только том случае попадает в H/F, когда $g^{-1}hg \in H$. □

Следуюшая теорема иногда называется **теоремой фон Дика**. В действительности, в работе 1882 года фон Дик формулировал нечто, что сейчас истолковывается как частный случай этой теоремы, относящийся к ситуации, когда G свободная группа. Общий случай явно сформулирован де Сегье в 1904 году.

Теорема 3. *Пусть $F, H \trianglelefteq G$ — нормальные подгруппы в G, причем $F \leq H$. Тогда имеет место канонический изоморфизм*

$$(G/F)/(H/F) \cong G/H.$$

Доказательство. Обозначим через $\pi : G \longrightarrow G/H$ каноническую проекцию. Так как $F \leq H = \mathrm{Ker}(\pi)$, по теореме об индуцированном гомоморфизме π индуцирует гомоморфизм $\overline{\pi} : G/F \longrightarrow G/H$, $gF \mapsto gH$. Ядро этого гомоморфизма равно $\mathrm{Ker}(\pi)/F = H/F$. Осталось применить теорему о гомоморфизме. □

3. Третья Теорема об изоморфизме.

Следующий результат описывает некоторые фактор-группы прямого произведения.

Теорема 4. *Пусть $H_1 \trianglelefteq G_1$ и $H_2 \trianglelefteq G_2$. Тогда $H_1 \times H_2 \trianglelefteq G_1 \times G_2$ и имеет место канонический изоморфизм*

$$G_1 \times G_2/H_1 \times H_2 \cong G_1/H_1 \times G_2/H_2.$$

Доказательство. То, что $H_1 \times H_2 \trianglelefteq G_1 \times G_2$ – очевидно (операции в прямом произведении покомпонентные!) Зададим теперь отображение $\pi = \pi_1 \times \pi_2 : G_1 \times G_2 \longrightarrow G_1/H_1 \times G_2/H_2$, где $\pi_i : G_i \longrightarrow G_i/H_i$ – каноническая проекция на фактор-группу. Иными словами, мы полагаем $\pi(g_1, g_2) = (g_1H_1, g_2H_2)$. Прямое произведение гомоморфизмов является гомоморфизмом, причем, так как g_1 и g_2 выбираются независимо, π сюръективен. Вычислим $\mathrm{Ker}(\pi)$. Равенство $\pi(g_1, g_2) = (e, e)$, означает в точности, что $g_1 \in H_1$ и $g_2 \in H_2$. Тем самым, $\mathrm{Ker}(\pi) = H_1 \times H_2$. Осталось сослаться на теорему о гомоморфизме. □

В связи с этой теоремой уместно проиллюстрировать еще одно типичное применение взаимной простоты. Верно ли, что и обратно, любой нормальный делитель $H \trianglelefteq G_1 \times G_2$ имеет вид $H_1 \times H_2$? Ясно, что вообще говоря, это совершенно не так (приведите пример). Однако это всегда так для конечных групп взаимно простых порядков.

Упражнение 2. Пусть $|G_1| = m$, $|G_2| = n$, причем m и n взаимно просты. Докажите, что тогда любая подгруппа $H \leq G_1 \times G_2$ имеет вид $H_1 \times H_2$ для некоторых $H_1 \leq G_1$ и $H_2 \leq G_2$.

Решение. В самом деле, пусть $(h, g) \in H$ для некоторых $h \in G_1$, $g \in G_2$. Тогда $(h, g)^m = (e, g^m) \in H$. Так как m и n взаимно просты, то найдется такое l, что $lm \equiv 1 \pmod{n}$, и, значит, $(e, g^m)^l = (e, g) \in H$.

§ 2. Группа автоморфизмов

4. Строение группы автоморфизмов.

Сейчас мы обсудим некоторые аспекты строения группы $\mathrm{Aut}(G)$, которые впервые начал изучать в 1893 году О. Гельдер. Именно он ввел группу $\mathrm{Inn}(G)$ внутренних изоморфизмов, заметил ее изоморфизм с $G/C(G)$ и то, что она нормальна в $\mathrm{Aut}(G)$, и начал рассматривать группу $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ внешних автоморфизмов.

Напомним, что для любой группы G множество ее автоморфизмов $\mathrm{Aut}(G)$ образует группу относительно операции композиции автоморфизмов. Отображение $I : G \longrightarrow \mathrm{Aut}(G)$, $g \mapsto I_g$, является гомоморфизмом, $I_{gh} = I_gI_h$. В самом деле,

$$I_{gh}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = I_g(hxh^{-1}) = I_g(I_h(x)) = I_gI_h(x).$$

Образ гомоморфизма I, то есть множество всех внутренних автоморфизмов, является подгруппой в $\mathrm{Aut}(G)$. Эта подгруппа $\mathrm{Inn}(G) = \{I_g \mid g \in G\}$ называется **группой внутренних автоморфизмов** группы G.

Теорема 5. *Подгруппа* $\mathrm{Inn}(G)$ *нормальна в* $\mathrm{Aut}(G)$. *Имеет место изоморфизм* $\mathrm{Inn}(G) \cong G/C(G)$.

Доказательство. Для доказательства первого утверждения заметим, что вычисление

$$\varphi I_g \varphi^{-1}(x) = \varphi(g\varphi^{-1}(x)g^{-1}) = \varphi(g)x\varphi(x)^{-1}$$

показывает, что $\varphi I_g \varphi^{-1} = I_{\varphi(g)}$, так что любой автоморфизм, сопряженный с внутренним, сам является внутренним. Второе утверждение теоремы следует из теоремы о гомоморфизме, если заметить, что гомоморфизм I_g в том и только том случае тривиален, когда $g \in C(G)$, так что ядро гомоморфизма $G \longrightarrow \mathrm{Aut}(G)$, $g \mapsto I_g$, совпадает с $C(G)$. □

Следствие 6. *Группа без центра* G *изоморфно вкладывается в свою группу автоморфизмов* $\mathrm{Aut}(G)$.

Фактор-группа

$$\mathrm{Out}(G) = \mathrm{Aut}(G)/\,\mathrm{Inn}(G)$$

называется **группой внешних автоморфизмов** группы G. Для многих классов групп можно доказать, что $\mathrm{Out}(G) \neq 1$. Приведем пример классического результата в таком духе.

Теорема 7 (Гашюца)**.** *Пусть* G *— конечная группа, не являющаяся абелевой, и такая что* $|G|$ *является степенью простого числа. Тогда* $\mathrm{Out}(G) \neq 1$.

Уже эти простейшие наблюдения о строении группы $\mathrm{Aut}(G)$ позволяют вычислить эту группу в некоторых интересных случаях.

1. $\mathrm{Aut}(\mathbb{Z}^+) \cong \{\pm 1\} \cong \mathrm{Out}(\mathbb{Z}^+)$. Действительно, так как 1 — это элемент, порождающий $\mathbb{Z}^+$, и -1 — единственный другой такой элемент, при любом автоморфизме 1 переходит в ± 1, и все остальные значения автоморфизма однозначно определяются выбором этого образа. Так как $\mathbb{Z}$ — абелева группа, все ее автоморфизмы — внешние.

   Чуть сложнее доказывается, что $\mathrm{Aut}(\mathbb{Z}^n)$, где $\mathbb{Z}^n$ обозначает прямое произведение n копий группы $\mathbb{Z}^+$, изоморфно группе $\mathrm{GL}(n, \mathbb{Z})$ всех обратимых матриц $n \times n$ с целыми коэффициентами. Для этого нужно каждому автоморфизму поставить в соответствие матрицу, в i-ом столбце которой стоят целые числа, соответствующие образу элемента $(0, \ldots, 0, 1, 0, \ldots, 0)$ группы $\mathbb{Z}^n$, где 1 стоит в i-ой позиции.

2. **Группа автоморфизмов конечной циклической группы.** Пусть C_n — конечная циклическая группа порядка n. Рассматривая образ элемента, порождающего C_n, при произвольном автоморфизме, нетрудно убедиться, что $\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^*$ — группе обратимых остатков по модулю n с операцией умножения. Конкретизируем описание группы $(\mathbb{Z}/n\mathbb{Z})^*$, к которому очень часто приходится обращаться при решении задач по теории конечных групп. Такое описание обычно естественным образом возникает в университетских курсах по теории чисел. Мы не будем повторять здесь это вычисление, а лишь сформулируем получающийся результат. Прежде всего, если $n = p_1^{m_1} \ldots p_s^{m_s}$, где p_i — попарно взаимно простые простые числа, то **китайская теорема об остатках** утверждает, что

   $$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{m_1}\mathbb{Z})^* \oplus \ldots \oplus (\mathbb{Z}/p_s^{m_s}\mathbb{Z})^*.$$

   Таким образом, нам нужно только вычислить $\mathrm{Aut}(C_{p^m})$, где p — простое число. Здесь проявляется драматическое отличие случая $p = 2$ от всех остальных, которое отражается во всех аспектах строения конечных p-групп.

   Теорема 8. *Для нечетного* p *имеем*

   $$\mathrm{Aut}(C_{p^m}) \cong C_{(p-1)p^{m-1}}.$$

   При $p = 2$ *имеем* $\mathrm{Aut}(C_2) = 1$, $\mathrm{Aut}(C_4) \cong C_2$ *и* $\mathrm{Aut}(C_{2^m}) \cong C_2 \times C_{2^{m-2}}$.

   Таким образом, группа автоморфизмов циклической группы *нечетного* примарного порядка тоже циклическая, в то время как при любом $n \geq 3$ группа автоморфизмов циклической группы порядка 2^n таковой не является.

   Следствие 9. *Для любого простого* p *имеем* $\mathrm{Aut}(C_p) \cong C_{p-1}$.

Обратите внимание, что $\mathrm{Aut}(C_3) \cong \mathrm{Aut}(C_4) \cong C_2$. Можно доказать, что для данной конечной группы H существует только конечное число неизоморфных конечных групп G таких, что $\mathrm{Aut}(G) \cong H$. При этом далеко не всякая группа может быть представлена как группа автоморфизмов. Вот несколько простейших примеров групп H, для которых не существует группы G — конечной или бесконечной — такой, что $\mathrm{Aut}(G) \cong H$:

- Циклическая группа нечетного порядка C_{2l+1}.
- Симметрическая группа S_6 — это как раз то исключение, которое возникает в теореме Гельдера!
- Все нетривиальные знакопеременные группы A_n, кроме A_8.
- Многие другие группы, например, бесконечная циклическая группа $\mathbb{Z}$.

Упражнение 3. Убедитесь, что если G — конечная группа порядка n, то порядок $\mathrm{Aut}(G)$ не превосходит $(n-1)!$. Когда достигается эта граница?

3. Для группы перестановок, которая будет подробно обсуждаться в одной из следующих лекций, выполнен изоморфизм $\mathrm{Aut}(S_n) \cong S_n$ при $n \neq 2, 6$ (**теорема Гельдера**).

4. **Отступление: группа автоморфизмов диэдральной группы.** Теперь разберем еще один ключевой пример.

   Упражнение 4. Докажите, что $\mathrm{Aut}(D_3) \cong D_3$ и $\mathrm{Aut}(D_4) \cong D_4$. Какая гипотеза у Вас возникла? Теперь вычислите $\mathrm{Aut}(D_n)$.

   Решение. Гипотеза неверна уже для $D_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, так как

   $$\mathrm{Aut}(D_2) \cong S_3 \cong D_3.$$

   Пусть теперь $n \geq 3$. В этом случае группа D_n порождается элементом x порядка $n \geq 3$ и инволюцией y такой, что xy тоже является инволюцией. При этом $D_n = \{x^j, x^j y, j = 0, \ldots, n-1\}$, причем все элементы $x^j y$ являются инволюциями. Пусть $\varphi \in \mathrm{Aut}(D_n)$. Так как автоморфизмы сохраняют порядок, то $\varphi(x) = x^i$ для какого-то i взаимно простого с n и, следовательно, так как $\varphi(x)$ и $\varphi(y)$ должны порождать группу D_n, $\varphi(y) = x^j y$ для какого-то $j = 0, \ldots, n-1$. С другой стороны, очевидно, что любой такой выбор i и j приводит к автоморфизму D_n. Таким образом, $|\mathrm{Aut}(D_n)| = \varphi(n)n$. Небольшое дополнительное усилие позволяет проверить, что $\mathrm{Aut}(D_n)$ раскладывается в полупрямое произведение $\mathrm{Aut}(D_n) \cong C_{\varphi(n)} \leftthreetimes C_n$, где $C_{\varphi(n)}$ действует на C_n как группа автоморфизмов. Случаи $n = 3$ и $n = 4$, когда $\varphi(n) = 2$, являются *единственными* случаями, для которых $\mathrm{Aut}(D_n) \cong D_n$.

Упражнение 5. Вычислите группу автоморфизмов $\mathrm{Aut}(Q)$ группы кватернионов.

Упражнение 6. Докажите, что $\mathrm{Aut}(C_2 \oplus C_4) = D_4$. Вычислите $\mathrm{Aut}(C_2 \oplus C_n)$ для произвольного n.

Упражнение 7. Докажите, что если $\mathrm{Aut}(G)$ — циклическая, то G — абелева.

Упражнение 8. Докажите, что не существует группы G такой, что $\mathrm{Aut}(G)$ — циклическая группа *нечетного* порядка.

5. Характеристические подгруппы.

Нормальная подгруппа $H \trianglelefteq G$ — это подгруппа, устойчивая под действием *внутренних* автоморфизмов. Субнормальность является *ослаблением* понятия нормальности. Однако в настоящее время нас интересует вопрос, можно ли таким образом *усилить* понятие нормальности, чтобы все же быть в состоянии заключить, что подгруппа $F \trianglelefteq H$ нормальна в G?

Определение. Подгруппа $H \leq G$ называется **характеристической**, если $\varphi(H) \leq H$ для любого **автоморфизма** $\varphi \in \mathrm{Aut}(G)$.

По определению любая характеристическая подгруппа является нормальной:

характеристическая $\Longrightarrow$ нормальная $\Longrightarrow$ субнормальная.

Чуть ниже мы приведем примеры, показывающие, что не всякая субнормальная подгруппа является нормальной, и не всякая нормальная подгруппа является характеристической.

Понятие характеристической подгруппы было введено в 1895 году Ф. Г. Фробениусом. Он называл нормальную подгруппу $F \trianglelefteq H$ характеристической, если она продолжает оставаться нормальной в любой группе G такой, что $H \trianglelefteq G$. Сейчас мы убедимся, что наше определение эквивалентно этому.

Предложение 10. *Имеют место следующие импликации:*
• *Характеристическая подгруппа $F \leq H$ нормальной подгруппы $H \trianglelefteq G$ нормальна в G.*
• *Характеристическая подгруппа $F \leq H$ характеристической подгруппы $H \leq G$ является характеристической подгруппой в G.*
• *Пусть $F \leq H \leq G$, причем F характеристическая в G и H/F характеристическая в G/F. Тогда H является характеристической подгруппой в G.*

Доказательство. Докажем для иллюстрации первое утверждение, доказательство двух других совершенно аналогично. Итак, пусть $H \trianglelefteq G$, а F — характеристическая подгруппа в H. Тогда для любого $g \in G$ ограничение I_g на H является автоморфизмом H и, следовательно, так как F характеристическая, то $I_g(F) \leq F$. Но это и значит, что $F \trianglelefteq G$. □

Приведем несколько очевидных примеров характеристических и нехарактеристических подгрупп.

1. Центр $C(G)$ любой группы G является ее характеристической подгруппой.

2. Если G — абелева группа, то ее подгруппа G_n, состоящая из элементов, порядок которых делит n, является характеристической. В частности, все подгруппы конечной циклической группы являются характеристическими.

3. Подгруппа $\mathbb{Z} \times \{e\}$ группы $\mathbb{Z} \times \mathbb{Z}$ является нормальной, но не характеристической. Действительно, она не сохраняется автоморфизмом $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$, $(g, h) \mapsto (h, g)$.

4. В одной из следующих лекций мы построим подгруппу $[G, G]$ произвольной группы G, называемую коммутантом G. Эта подгруппа тоже является характеристической. В частности, коммутант $\mathrm{GL}(n, K)$, где K — поле, совпадает с $\mathrm{SL}(n, K)$, а коммутант S_n — с A_n. Поэтому эти две подгруппы являются характеристическими.

5. Подгруппа G^n, порожденная n-ми степенями элементов группы G, является характеристической.

Последние два примера — это так называемые **вербальные** подгруппы, порожденных значениями некоторых слов в группе G: в первом случае слова $[x, y]$, а во втором — слова x^n. Вот еще несколько примеров характеристических подгрупп (во всех этих примерах мы рассматриваем подгрупппы фиксированной группы G):
• **подгруппа Фраттини** $\Phi(G)$, т. е. пересечение всех максимальных подгрупп;
• **подгруппа Виландта** $\Psi(G)$, т. е. порождение всех минимальных подгрупп;
• пересечение всех подгрупп индекса n;
• пересечение всех подгрупп индекса $\leq n$;
• пересечение всех нормальных подгрупп индекса n;
• пересечение всех нормальных подгрупп индекса $\leq n$;
• **подгруппа Томпсона** $J(P)$ конечной p-группы P, т. е. подгруппа, порожденная всеми абелевыми подгруппами P максимального порядка.

Упражнение 9. Напомним, что подгруппа H конечной группы G называется **холловской**, если ее порядок и индекс взаимно просты. Докажите, что любая нормальная холловская подгруппа H конечной группы G является характеристической.

Решение. В самом деле, пусть $\varphi \in \mathrm{Aut}(G)$. Тогда $H\varphi(H) \leq G$ является подгруппой в G, так что $|H\varphi(H)|$ делит G. По формуле произведения

$$|H\varphi(H)| = \frac{|H||\varphi(H)|}{|H \cap \varphi(H)|} = |H||\varphi(H) : H \cap \varphi(H)|,$$

так что $|\varphi(H) : H \cap \varphi(H)|$ одновременно делит как $|H|$, так и $|G : H|$. Тем самым этот индекс равен 1, но это и значит, что $\varphi(H) \leq H$.

6. Пример субнормальной, но не нормальной подгруппы. Чтобы построить пример субнормальной, но не нормальной подгруппы, мы воспользуемся той же идеей, что и в приведенном выше примере подгруппы нормальной, но не характеристической. А именно, мы используем прямой квадрат группы и его автоморфизм, переставляющий сомножители. В качестве исходной группы мы возьмем группу $D_3 \cong S_3$ — группу симметрий правильного треугольника на плоскости, или, что то же самое, группу перестановок трех элементов (которые можно отождествить с вершинами этого треугольника).

Рассмотрим группу $G = S_3 \times S_3$. Так как $C(S_3) = \{e\}$, нетрудно убедиться, что $C(G) = \{(e,e)\} = \{e\}$, то есть G — группа без центра. Тогда $I : G \longrightarrow \mathrm{Inn}(G)$ является изоморфизмом групп. Так как $S_3 \times \{e\}$ — нормальная подгруппа в G, ее изоморфный образ $I(S_3 \times \{e\})$ является нормальной подгруппой в $\mathrm{Inn}(G)$.

Так как $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$, мы видим, что $I(S_3 \times \{e\})$ является субнормальной подгруппой в $\mathrm{Aut}(G)$:

$$I(S_3 \times \{e\}) \trianglelefteq \mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G).$$

Однако, группа $I(S_3 \times \{e\})$ не является нормальной подгруппой в $\mathrm{Aut}(G)$, поскольку автоморфизм $\tau : G \longrightarrow G$, $(g,h) \mapsto (h,g)$, не сохраняет $S_3 \times \{e\}$.

Дополнение 1: эндоморфизмы $\mathbb{Q}^+$ и $\mathbb{R}^+$.

1. Эндоморфизмы $\mathbb{Q}^+$. Ранее мы заметили, что $\mathrm{Aut}(\mathbb{Z}^+) \cong \{\pm 1\}$. Пользуясь теми же методами, легко видеть, что $\mathrm{End}(\mathbb{Z}^+) \cong \mathbb{Z}$.

Упражнение 10. Убедитесь, что $\mathrm{End}(\mathbb{Q}^+) \cong \mathbb{Q}$.

Решение. Пусть φ — эндоморфизм $\mathbb{Q}^+$, $\varphi(1) = c \in \mathbb{Q}$. Покажем, что тогда $\varphi(x) = cx$ для всех $x \in \mathbb{Q}$. В самом деле, для любого $m \in \mathbb{Z}$ имеем $\varphi(m) = m\varphi(1) = cm$. Кроме того, для любого $n \in \mathbb{Z}$, выполняется $n\varphi(m/n) = \varphi(n \cdot m/n) = \varphi(m) = cm$, так что действительно $\varphi(m/n) = c(m/n)$.
Мы уже знали, что $\mathrm{Hom}(\mathbb{Z}, \mathbb{Q}) = \mathbb{Q}$, решение задачи состояло в том, что мы заметили, что любой эндоморфизм $\mathbb{Q}$ полностью определяется своим ограничением на $\mathbb{Z}$.

Следствие 11. $\mathrm{Aut}(\mathbb{Q}^+) = \mathbb{Q}^*$.

Следствие 12. *Две подгруппы $A, B \leq \mathbb{Q}^+$ тогда и только тогда изоморфны, когда найдется $x \in \mathbb{Q}^*$ такое, что $A = xB$.*

Легко видеть, что аддитивные подгруппы в $\mathbb{Q}$ устроены так. Для каждого простого зададим $m_p \in \mathbb{Z} \cup \{\pm\infty\}$:

$$A = \{x \in \mathbb{Q}^+ \mid \forall p \in \mathbb{P}, v_p(x) \geq m_p\}.$$

Таким образом, имеется континуум классов изоморфизма аддитивных подгрупп в $\mathbb{Q}^+$.
2. Непрерывные автоморфизмы $\mathbb{R}^+$. Вопрос о существовании у группы $\mathbb{R}^+$ автоморфизма, не являющегося гомотетией, поставленный в начале XIX века Коши, решил лишь Г. Гамель в 1905 году. Гамель построил много таких автоморфизмов. Его подход основан на том, что как аддитивные группы $\mathbb{R}$ и $\mathbb{R}^n$ изоморфны, а у $\mathbb{R}^n$ при $n \geq 2$ море автоморфизмов. Разумеется, построение изоморфизма между $\mathbb{R}$ и $\mathbb{R}^n$ зависит от аксиомы выбора, кроме того, такой изоморфизм заведомо не может быть непрерывным.

Теорема 13 (Коши). *Гомотетии $\theta_c : \mathbb{R}^+ \longrightarrow \mathbb{R}^+$, $x \mapsto cx$, где $c \in \mathbb{R}$, являются единственными **непрерывными** эндоморфизмами $\mathbb{R}^+$.*

Так как группа $\mathbb{R}_{>0}$ изоморфна $\mathbb{R}^+$, причем взаимно обратные изоморфизмы задаются отображениями $x \mapsto \ln(x)$ и $x \mapsto e^x$, соответственно, то эту теорему можно сформулировать еще любым из трех следующих **эквивалентных** образов. Эти результаты, собственно, и объясняют, почему в школьном курсе принято рассматривать степенные, показательные и логарифмические функции — никакие другие гомоморфизмы между аддитивными и мультипликативными структурами на $\mathbb{R}$ невозможно построить элементарными средствами.

Следствие 14. *Отображения $\mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0}$, $x \mapsto x^c$, где $c \in \mathbb{R}$, являются единственными **непрерывными** эндоморфизмами $\mathbb{R}_{>0}$.*

Следствие 15. *Отображения $\mathbb{R}^+ \longrightarrow \mathbb{R}^*$, $x \mapsto c^x$, где $c \in \mathbb{R}_{>0}$, являются единственными* ***непрерывными*** *гомоморфизмами $\mathbb{R}^+$ в $\mathbb{R}^*$.*

Следствие 16. *Отображения $\mathbb{R}_{>0} \longrightarrow \mathbb{R}^+$, $x \mapsto \log_c(x)$, где $c \in \mathbb{R}_{>0}$, $c \neq 1$, являются единственными* ***непрерывными*** *гомоморфизмами $\mathbb{R}_{>0}$ в $\mathbb{R}^+$.*

В книжке Фихтенгольца все эти четыре утверждения трактуются как независимые теоремы, с четырьмя разными (не слишком короткими) доказательствами! Применяя эти результаты к фактор-группе $\mathbb{T} \cong \mathbb{R}/\mathbb{Z}$, мы получаем еще такие следствия. Разумеется, как обычно, операция в $\mathbb{T}$ записывается мультипликативно.

Следствие 17. *Отображения $\mathbb{R}^+ \longrightarrow \mathbb{T}$, $x \mapsto e^{icx}$, где $c \in \mathbb{R}$, являются единственными* ***непрерывными*** *гомоморфизмами $\mathbb{R}^+$ в $\mathbb{T}$.*

Следствие 18. *Отображения $\mathbb{T} \longrightarrow \mathbb{T}$, $x \mapsto x^n$, где $n \in \mathbb{Z}$, являются единственными* ***непрерывными*** *эндоморфизмами $\mathbb{T}$.*

А что Вы можете сказать о гомоморфизмах $\mathbb{T}$ в $\mathbb{R}^+$?

Отступление: полиномиальные автоморфизмы K^+. Над произвольным полем K нельзя говорить о непрерывности, но можно спросить себя, каковы **полиномиальные** гомоморфизмы $K^+ \longrightarrow K^+$ и $K^* \longrightarrow K^*$? Иными словами, предлагается найти все **многочлены** $f \in K[x]$ такие, что $f(x+y) = f(x) + f(y)$ или, соответственно, $f(xy) = f(x)f(y)$. В этом утверждении содержится некоторая двусмысленность: как следует понимать равенство $f(xy) = f(x)f(y)$ — **функционально**, т. е. как совпадение значений $f(ab) = f(a)f(b)$ для любых $a, b \in K$ или **формально**, как равенство многочленов в $K[x, y]$? Впрочем, если поле K бесконечно, этого вопроса не возникает, так как ненулевой многочлен конечной степени не может иметь бесконечно много корней (теорема о формальном и функциональном равенстве многочленов, принцип несущественности алгебраических неравенств).

Упражнение 11. Докажите, что если K бесконечное поле, а $f \in K[x]$ — многочлен такой, что $f(ab) = f(a)f(b)$ для любых $a, b \in K$, то $f = x^n$.

Решение. По только что помянутому принципу несущественности алгебраических неравенств многочлены $f(xy)$ и $f(x)f(y)$ совпадают как элементы $K[x, y]$. Пусть $f = a_n x^n + \ldots + a_1 x + a_0$. Сравнивая коэффициенты при $x^n y^n$ мы видим, что $a_n = 1$, а сравнивая коэффициенты при $x^n y^i$, $i = 0, \ldots, n-1$, получаем $a_n a_i = 0$.
Как показывает пример $x^3 + x^2 + x \in \mathbb{F}_2[x]$, для конечного поля это утверждение не имеет места.

Дополнение 2: Группа автоморфизмов неабелевой простой группы

1. Группа автоморфизмов неабелевой простой группы. Следующий цикл задач взят со с. 131 книги Н. Бурбаки, Алгебра, том I.

Упражнение 12. Пусть G — неабелева простая группа. Покажите, что $\mathrm{Inn}(G)$ — характеристическая подгруппа в $\mathrm{Aut}(G)$.

Решение. Пусть $\varphi \in \mathrm{Aut}(\mathrm{Aut}(G))$. Тогда $\mathrm{Inn}(G) \cap \varphi(\mathrm{Inn}(G)) \trianglelefteq \mathrm{Aut}(G)$. Так как $\mathrm{Inn}(G) \cong G$ простая, то либо $\mathrm{Inn}(G) \cap \varphi(\mathrm{Inn}(G)) = \mathrm{Inn}(G)$, в этом случае доказательство закончено, либо $\mathrm{Inn}(G) \cap \varphi(\mathrm{Inn}(G)) = 1$. Во втором случае $\mathrm{Aut}(G)$ содержит прямое произведение $\mathrm{Inn}(G) \times \varphi(\mathrm{Inn}(G))$. Но ведь G группа без центра и, значит, по предыдущей задаче $C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) = 1$.

Упражнение 13. Пусть G — группа без центра и $\varphi \in \mathrm{Aut}(\mathrm{Aut}(G))$. Показать, что если $\varphi(I_g) = I_g$ для всех $I_g \in \mathrm{Inn}(G)$, то $\varphi = \mathrm{id}$.

Решение. По условию для любого $g \in G$ имеем $\varphi(I_g) = I_g$ и, тем самым,

$$\varphi(\pi) I_g \varphi(\pi)^{-1} = \varphi(\pi I_g \pi^{-1}) = \varphi(I_{\pi(g)}) = I_{\pi(g)} = \pi I_g \pi^{-1}$$

для любого $\pi \in \mathrm{Aut}(G)$. Это равенство можно переписать в виде $\pi^{-1}\varphi(\pi) I_g = I_g \pi^{-1}\varphi(\pi)$. По первой задаче автоморфизм $\pi^{-1}\varphi(\pi)$, центральный, но так как G группа без центра, то $\pi^{-1}\varphi(\pi)(g) = g$ для всех $g \in G$. Но это и значит, что $\varphi(\pi)(g) = \pi(g)$ так что действительно $\varphi(\pi) = \pi$, как и утверждалось.

Упражнение 14. Пусть G — неабелева простая группа. Показать, что каждый автоморфизм группы $\mathrm{Aut}(G)$ внутренний.

Решение. Сопоставим автоморфизму $\varphi \in \mathrm{Aut}(\mathrm{Aut}(G))$ автоморфизм π группы G следующим образом: $I_{\pi(g)} = \varphi(I_g)$. По первой задаче этого пункта $\mathrm{Inn}(G) \cong G$ характеристическая подгруппа в $\mathrm{Aut}(G)$. Утверждается, что тогда $\varphi(\psi) = \pi\psi\pi^{-1}$ для любого $\psi \in \mathrm{Aut}(G)$. Это равносильно тому, что автоморфизм $\psi \mapsto \pi^{-1}\varphi(\psi)\pi$ группы $\mathrm{Aut}(G)$ тождественный. В силу второй задачи для этого достаточно показать, что он оставляет на месте все внутренние автоморфизмы. В самом деле,

$$\pi^{-1}\varphi(I_g)\pi(x) = \pi^{-1}I_{\pi(g)}\pi(x) = \pi^{-1}(\pi(g)\pi(x)\pi(g)^{-1}) = gxg^{-1} = I_g(x),$$

что и требовалось.
Таким образом, резюмируя содержание этих задач, мы доказали следующий результат.

Теорема 19. *Если G неабелева простая группа, то* $\mathrm{Aut}(G) \cong \mathrm{Aut}(\mathrm{Aut}(G))$.

2. Теорема Виландта. В действительности в 1939 году Х. Виландт доказал следующий результат. Положим $\mathrm{Aut}_0(G) = G$, $\mathrm{Aut}_1(G) = \mathrm{Aut}(G)$, $\mathrm{Aut}_2(G) = \mathrm{Aut}(\mathrm{Aut}(G))$, и далее $\mathrm{Aut}_n(G) = \mathrm{Aut}(\mathrm{Aut}_{n-1}(G))$. Каждая группа без центра вкладывается в свою группу автоморфизмов, и мы отождествим G с подгруппой в $\mathrm{Aut}(G)$. В свою очередь, группа автоморфизмов группы без центра — тоже группа без центра, так что мы получаем башню $G \le \mathrm{Aut}(G) \le \mathrm{Aut}_2(G) \le \ldots$. Как мы только что показали, для неабелевых простых групп эта башня стабилизируется уже на первом шаге. Это утверждение допускает очень широкое обобщение.

Теорема 20 (Виландт)**.** *Если G — конечная группа без центра, то существует n такое, что* $\mathrm{Aut}_n(G) = \mathrm{Aut}_{n+1}(G) = \ldots$.

Для бесконечных групп аналогичная стабилизация тоже происходит, но на бесконечном ординале (S. Thomas, 1985).
3. Гипотеза Шрайера. Одно из самых важных наблюдений, относящихся к строению группы $\mathrm{Aut}(G)$ для неабелевой конечной простой группы G, состоит в следующем.

Теорема 21 (Гипотеза Шрайера)**.** *Группа* $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ *внешних автоморфизмов конечной простой группы G разрешима.*

В течение многих десятилетий эта гипотеза играла совершенно исключительную роль в теории конечных групп, как в силу своей важности — многие факты теории конечных групп легко проверяются по модулю гипотезы Шрайера, — так и в силу своей неприступности. В настоящее время справедливость гипотезы Шрайера *проверена* для всех конечных простых групп, но только при помощи классификации конечных простых групп, т.е. фактически перебором. Никакого **прямого** доказательства этой теоремы, не опирающегося на классификацию, в настоящее время нет.