Задача 2010–1

Централизатор подстановки — это множество подстановок, которые с ней коммутируют. Какое наименьшее число элементов может быть в централизаторе подстановки из группы $\mathbf{S}_n$? (*Предложил И. В. Аржанцев.*)

Ответ. n при $n = 1$, 2 и $n - 1$ при $n \geqslant 3$.

Решение. Разложим подстановку σ из группы $\mathbf{S}_n$ в произведение независимых циклов. Пусть m — число σ-неподвижных элементов из множества $\{1, \ldots, n\}$, а $n_1, \ldots, n_k$ — длины независимых циклов $\sigma_1, \ldots, \sigma_k$ длины $\geqslant 2$. Тогда $m + n_1 + \ldots + n_k = n$ и σ коммутирует с любой подстановкой вида $\sigma_0 \sigma_1^{s_1} \ldots \sigma_k^{s_k}$, где $\sigma_0 \in S_m$ — произвольная подстановка на σ-неподвижных элементах. Значит, в централизаторе σ содержится не менее $m! n_1 \ldots n_k$ подстановок.

Случай 1. $m \geqslant 2$. Тогда $m! n_1 \ldots n_k \geqslant (1+(m-1))(1+(n_1-1)) \ldots (1+(n_k-1))$. Последнее произведение равно сумме 2^{k+1} слагаемых, каждое из которых не меньше 1. Значит, все произведение не меньше чем

$$(m-1) + (n_1 - 1) + \ldots + (n_k - 1) + 2^{k+1} - (k+1) = n + 2^{k+1} - 2(k+1).$$

Заметим, что $2^{k+1} \geqslant 2(k+1)$, и тем самым централизатор подстановки σ содержит не менее n элементов.

Случай 2. $m = 0$. Как и в случае 1 доказывается, что $n_1 \ldots n_k \geqslant n_1 + \ldots + n_k = n$.

Случай 3. $m = 1$. Здесь $n_1 \ldots n_k \geqslant n_1 + \ldots + n_k = n - 1$.

Итак, централизатор подстановки σ содержит не менее $n - 1$ элемента. Пусть $n \geqslant 3$. Положим $\sigma = (12 \ldots n-1)$. Если $\tau\sigma = \sigma\tau$, то $\sigma(\tau(n)) = \tau(n)$, и значит $\tau(n) = n$. Наконец, если $\tau(1) = s$, $s < n$, то $\tau(2) = \sigma(s)$ и т.д., откуда $\tau = \sigma^s$, $0 \leqslant s \leqslant n - 1$. Это доказывает, что централизатор σ содержит ровно $n - 1$ элемент.

Упражнение. Решите аналогичную задачу для знакопеременной группы.

Задача 2010–2

Может ли подкольцо поля комплексных чисел (не обязательно содержащее единицу) иметь больше двух автоморфизмов, сохраняющих модуль? (*Предложили А. А. Клячко и А. А. Нечаев.*)

Ответ. Не может.

Решение. Задача легко сводится к случаю, когда кольцо содержит единицу (и даже является полем). Действительно, автоморфизм φ кольца $R \subseteq \mathbb{C}$ естественным образом продолжается до автоморфизма f поля частных $F = \{\frac{a}{b} \mid a \in R,\ b \in R \backslash \{0\}\} \subseteq \mathbb{C}$ по формуле $f(\frac{a}{b}) = \frac{\varphi(a)}{\varphi(b)}$. При этом автоморфизм f поля F также сохраняет модуль.

Поскольку единица переходит в единицу при любом автоморфизме, мы имеем равенства $|f(x)| = |x|$ и $|f(x) - 1| = |f(x-1)| = |x-1|$ для каждого $x \in F$. Эта система уравнений (относительно $f(x)$) имеет всего два решения: $f(x) = x$ и $f(x) = \overline{x}$.

Осталось показать, что если $f(x_0) = x_0$ для какого-то невещественного $x_0 \in F$, то $f(x) = x$ для всех $x \in F$. Предположив противное, мы получаем, что $f(x_0) = x_0$ и $f(x_1) = \overline{x_1}$ для некоторых невещественных $x_0, x_1 \in F$. Но тогда $|x_0 - x_1| = |f(x_0 - x_1)| = |x_0 - \overline{x_1}|$, что невозможно для невещественных чисел x_0 и x_1.

Упражнение 1. Покажите, что поле комплексных чисел имеет бесконечно много автоморфизмов[1], но только два из них

- — являются непрерывными[2];
- — переводят вещественные числа в вещественные[2];
- — коммутируют с сопряжением[2].

Упражнение 2. Покажите, что поле вещественных чисел, поле рациональных чисел и все поля вычетов не имеют нетождественных автоморфизмов.

Упражнение 3. Покажите, что группа автоморфизмов каждого конечного поля F является циклической и порождается *автоморфизмом Фробениуса*: $x \mapsto x^{\operatorname{char} F}$.

---

[1] Это трудная задача, она требует использования аксиомы выбора и знакомства с понятием базиса трансцендентности.

[2] А это простая задача.

Упражнение. Может ли подкольцо поля комплексных чисел, инвариантное относительно сопряжения, иметь больше двух автоморфизмов, коммутирующих с сопряжением?

Задача 2010–3

Докажите, что биномиальные коэффициенты C_2^2, C_3^2, C_4^2, C_5^2, C_6^2, ... дают все возможные остатки при делении на n тогда и только тогда, когда число n является степенью двойки. (*Предложил В. Т. Марков.*)

Решение. Предположим, что $n = 2^m$. Достаточно доказать, что числа $\frac{i(i+1)}{2}$ дают попарно разные остатки при делении на n при $0 \leqslant i \leqslant n-1$, или что разность

$$\frac{i(i+1)}{2} - \frac{j(j+1)}{2} = \frac{(i-j)(i+j+1)}{2} \text{при } 0 \leqslant j < i < n$$

не делится на n. Надо заметить, что из чисел $i-j$ и $i+j+1$ равно одно является четным, и после деления на 2 оно становится меньше n.

Пусть теперь n делится на нечетное простое число p. Если в нашей последовательности встречаются все остатки по модулю n, то это же верно и для модуля p, поэтому можно считать, что $n = p$. Деление на 2 есть умножение на элемент, обратимый по модулю p, поэтому его можно не учитывать. Тогда ненулевые остатки могут давать только члены 1×2, 2×3,...,$(p-2) \times (p-1)$ (далее последовательность периодически повторяется), но таковых только $p-2$ штуки.

Упражнение. Для каких натуральных n биномиальные коэффициенты C_3^3, C_4^3, C_5^3, C_6^3, C_7^3, ... дают все возможные остатки при делении на n?

Задача 2010–4

В аддитивной группе многочленов от одной переменной с рациональными коэффициентами степени не выше чем пять, принимающих целые значения в целых точках, есть замечательная подгруппа, состоящая из многочленов с целыми коэффициентами. Найдите ее индекс. (*Предложил А. А. Клячко*[3].)

Ответ. $5! \cdot 4! \cdot 3! \cdot 2! = 34560$.

Решение. Как устроены многочлены, принимающие целые значения в целых точках? Заметим, что знаменатели коэффициентов каждого такого многочлена делят факториал его степени. Это следует из интерполяционной формулы Лагранжа. Например, для многочлена f степени не выше чем пять мы имеем:

$$f(x) = f(0)\frac{(x-1)(x-2)(x-3)(x-4)(x-5)}{(0-1)(0-2)(0-3)(0-4)(0-5)} + \cdots + f(5)\frac{(x-0)(x-1)(x-2)(x-3)(x-4)}{(5-0)(5-1)(5-2)(5-3)(5-4)}.$$

С другой стороны, биномиальные коэффициенты

$$1,\ x,\ \frac{x(x-1)}{2},\ \frac{x(x-1)(x-2)}{3!},\ \frac{x(x-1)(x-2)(x-3)}{4!},\ \frac{x(x-1)(x-2)(x-3)(x-4)}{5!}$$

являются примерами многочленов степени k, принимающих целые значения в целых точках, со старшими коэффициентами $\frac{1}{k!}$. Из сказанного следует, что

> *каждый многочлен степени не выше n, принимающий целые значения в целых точках, единственным образом представляется в виде целочисленной линейной комбинации биномиальных коэффициентов C_x^0, C_x^1, ..., C_x^n.*

Это доказывается очевидной индукцией по степени. Столь же очевидно, что

> *каждый многочлен степени не выше n с целыми коэффициентами единственным образом представляется в виде целочисленной линейной комбинации многочленов $0!C_x^0$, $1!C_x^1$, ..., $n!C_x^n$.*

Таким образом, мы нашли согласованные базисы интересующей нас свободной абелевой группы и ее подгруппы. Отсюда понятно, что индекс есть произведение факториалов $0! \cdot 1! \cdot \cdots \cdot n!$, а соответствующая факторгруппа представляет собой прямую сумму циклических групп $\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \cdots \oplus \mathbb{Z}_{n!}$.

Упражнение 1. Решите аналогичную задачу о многочленах от двух переменных.

Упражнение 2. Верно ли, что многочлен от одной переменной степени не выше чем сто, принимающий целые значения в точках 0, 1, ..., 100, принимает целые значения во всех целых точках?

---

[3]Эту задачу мы позаимствовали из книжки [Клячко Александр А. Теория Галуа: Уч. пособие. — Куйбышев: КГУ, 1982].

Задача 2010–5

В таблице 2010×2010 расставлены элементы поля $\mathbb{Z}_3$. Известно, что разность любых двух столбцов есть столбец, содержащий поровну элементов 0, 1 и 2. Докажите, что разность любых двух строк является строкой, содержащей поровну элементов 0, 1 и 2. (*Автор неизвестен. Задача предлагалась на олимпиаде мех-мата МГУ в 1980 году.*)

Решение. Матрице $A = (a_{ij})$ над $\mathbb{Z}_3$ сопоставим комплексную матрицу B с элементами $b_{ij} = \varepsilon^{a_{ij}}$, где ε — первообразный кубический корень из единицы, то есть на места нулей напишем единицы, на места единиц напишем $\frac{-1+\sqrt{3}i}{2}$, а на места двоек напишем $\frac{-1-\sqrt{3}i}{2}$. В матрице B любые два столбца ортогональны в эрмитовом смысле, то есть матрица $\frac{1}{\sqrt{2010}}B$ является унитарной. Следовательно, у нее любые две строки ортогональны, то есть для любых двух строк $(x_1, \ldots, x_{2010})$ и $(y_1, \ldots, y_{2010})$ матрицы B мы имеем $x_1\overline{y_1} + \cdots + x_{2010}\overline{y_{2010}} = 0$. Но каждое слагаемое в этой сумме является одним из кубических корней из единицы, поэтому сумма может быть нулевой только в случае, когда каждый из корней встречается в сумме одинаковое число раз. Другими словами, разность любых двух строк матрицы A содержит поровну нулей, единиц и двоек, что и требовалось.

Упражнение. Для каких колец вычетов $\mathbb{Z}_n$ верно аналогичное утверждение? Для каких конечных полей верно аналогичное утверждение?

Задача 2010–6

Найдите все билинейные формы на пространстве $\mathbb{R}^n$, характеристический многочлен матрицы которых не зависит от выбора базиса в $\mathbb{R}^n$, в котором эта матрица записана. (*Предложил В. В. Батырев.*)

Ответ. Только нулевая.

Решение. Пусть $b(\cdot,\cdot)$ — данная билинейная форма и $B = (b_{ij})$ — ее матрица в базисе $e_1, \ldots, e_n$. Тогда характеристический многочлен

$$\det(B - tE) = (-1)^n t^n + a_1 t^{n-1} + \ldots + a_n$$

в базисе $\lambda e_1, \ldots, \lambda e_n$, где $\lambda \in \mathbb{R} \setminus \{0\}$, имеет вид

$$(-1)^n t^n + \lambda^2 a_1 t^{n-1} + \ldots + \lambda^{2n} a_n.$$

Поскольку указанные многочлены совпадают для всех ненулевых значений λ, мы заключаем, что $a_1 = \ldots = a_n = 0$. В частности, след матрицы B равен нулю. Любой ненулевой вектор $v \in \mathbb{R}^n$ можно дополнить до базиса $v_1 = v, v_2, \ldots, v_n$ в $\mathbb{R}^n$. Заменяя v на λv и приравнивая след соответствующей матрицы к нулю, мы получаем

$$\lambda^2 b(v, v) + b(v_2, v_2) + \ldots + b(v_n, v_n) = 0.$$

Значит, $b(v, v) = 0$ и форма $b(\cdot,\cdot)$ кососимметрична. Если

$$a = b(v_1, v_2) \neq 0,$$

то ограничение формы b на подпространство $U = \langle v_1, v_2\rangle$ невырождено, поэтому $\mathbb{R}^n = U \oplus U^{\perp}$. Это разложение определяет разложение характеристического многочлена матрицы B в произведение $f_1(t)f_2(t)$, где $f_1(t) = t^2 + a^2$. Если заменить вектор v_1 на λv_1 и не изменять другие базисные векторы, первый сомножитель будет равен $t^2 + \lambda^2 a$, откуда следует, что $a = 0$, противоречие. Значит, форма $b(\cdot,\cdot)$ является нулевой.

Замечание. Приведенное доказательство проходит над любым полем которое содержит более трех элементов и характеристика которого не равна двум.

Упражнение. Решите аналогичную задачу над полем из трех элементов.

Задача 2010–7

Назовем элемент группы *стойким*, если он остается на месте под действием всех автоморфизмов. Опишите все конечные группы, в которых стойких элементов не меньше половины. (*Предложил А. А. Клячко.*)

Ответ. Циклические группы порядков один, два и четыре.

Решение. Заметим, что все стойкие элементы являются центральными, так как они должны оставаться на месте при сопряжении любым элементом группы. Значит, центр интересующей нас группы имеет индекс не больше двух. Но факторгруппа по центру, как известно, не может быть циклической и, следовательно, не может иметь порядок два. Значит, центр совпадает со всей группой, то есть группа является абелевой.

Поскольку в абелевой группе (записанной аддитивно) отображение $x \mapsto -x$ является автоморфизмом, все ненулевые стойкие элементы должны быть порядка два. Это означает, что в группе имеется подгруппа индекса не больше чем два, изоморфная $\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$, а сама группа, стало быть, изоморфна либо $\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$, либо $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$. Нетрудно убедиться, что в группе $\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$ ненулевых стойких элементов нет, если число слагаемых больше одного (поскольку, например, элемент, у которого вторая координата ненулевая, сдвигается автоморфизмом $(x, y, z, t, \dots) \mapsto (x+y, y, z, t, \dots)$); а в группе $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$ есть единственный стойкий ненулевой элемент: $(2, 0, 0, \dots, 0)$ (докажите!). Отсюда все следует.

Упражнение. В каких группах стойких элементов не меньше трети?

Задача 2010–8

Назовем ассоциативное кольцо с единицей *антителом*, если оно не содержит неединичных обратимых элементов. Докажите следующую «антитеорему Веддерберна»: все конечные антитела коммутативны. (*Предложил А. А. Клячко.*)

Решение 1. Заметим, что так как -1 — всегда обратимый элемент кольца, то $-1 = 1$.

В кольце R нет ненулевых нильпотентных элементов, так как если $r^n = 0$, то элемент $1 + r$ обратим (докажите это).

Рассмотрим произвольный элемент $a \in R$ и мультипликативную подполугруппу G, им порожденную (то есть все элементы вида a^k, $k \in \mathbb{N}$). Заметим, что если мы рассмотрим на полугруппе G отображение $x \mapsto x^2$, то оно будет взаимно однозначным, так как из $x^2 = y^2$ следует (при условии $1 + 1 = 0$), что $0 = x^2 - y^2 = (x - y)(x + y) = (x - y)^2$. Так как в кольце R нет ненулевых нильпотентных элементов, то $x = y$. Значит, возведение в квадрат осуществляет некоторую перестановку элементов (конечной) полугруппы G. Из этого очевидно следует существование такого ненулевого m, что $a^{2^m} = a$.

Обозначим a^{2^m-1} через e. Заметим, что элемент $e \in R$ является идемпотентом (то есть $e^2 = e$), так как

$$e^2 = (a^{2^m-1})^2 = a^{2^{m+1}-2} = a^{2^m} a^{2^m-2} = a \cdot a^{2^m-2} = a^{2^m-1} = e.$$

Кроме того, как легко заметить, $ae = a$.

Пусть $m > 1$. Рассмотрим элементы кольца R $b = a + (1 - e)$ и $c = a^{2^m-2} + (1 - e)$. Перемножим их:

$$bc = a^{2^m-1} + a(1-e) + (1-e)a^{2^m-2} + (1-e)^2 = e + ae(1-e) + (1-e)e \cdot a^{2^m-2} + (1-e) = e + (1-e) = 1.$$

Таким образом, элемент b обратим, то есть $b = 1 = e + (1 - e)$. Значит, $a = e$. Если $m = 1$, то $a = e$ по построению. Следовательно, любой произвольно взятый элемент кольца является идемпотентом.

Теперь рассмотрим произвольные два элемента кольца R — x и y:

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + y + xy + yx.$$

Значит, $xy + yx = 0$, что равносильно $xy = yx$, так как $-1 = 1$.

Решение 2. Минус единица всегда является обратимым элементом, поэтому в антителе $-1 = 1$, то есть всякое антитело A имеет характеристику два и, следовательно, является алгеброй над $\mathbb{Z}_2$.

Рассмотрим произвольный элемент $a \in A \setminus \{0, 1\}$. Минимальный многочлен $f \in \mathbb{Z}_2[x]$ этого элемента (то есть ненулевой многочлен над $\mathbb{Z}_2$ минимальной степени, аннулирующий элемент a) делится на x (поскольку иначе равенство $0 = f(a) = 1 + a(\dots)$ свидетельствовало бы об обратимости элемента a). По аналогичным причинам многочлен f обязан делиться на $x + 1$ (иначе $a + 1$ был бы неединичным обратимым элементом). Таким образом, $f(x) = (x^2 + x)g(x)$. При этом многочлен $g(x)$ не делится на x,

поскольку иначе элемент $1+(a+1)g(a)$ был бы неединичным обратимым элементом: $(1+(a+1)g(a))^2 = 1+((a+1)g(a))^2 = 1+f(a)(\dots) = 1$. По аналогичным причинам многочлен g не делится на $x+1$.

Заметим теперь, что многочлен $h(x) = (x^2+x)+g(x)$ взаимно прост с $f(x)$, так как он не делится ни на x, ни на $x+1$, ни на какой делитель многочлена g. Это означает, что $1 = u(x)h(x)+v(x)f(x)$ для некоторых многочленов u и v. Подставляя в это равенство $x = a$, мы получаем обратимость элемента $h(a)$. Поскольку A — антитело, $h(a) = 1$. Значит, степень многочлена $h(x)+1 = (x^2+x)+g(x)+1$ не меньше степени многочлена $f(x) = (x^2+x)g(x)$ (в силу минимальности f). Следовательно, многочлен g есть единица и $a^2 = a$ для всех $a \in A$.

В частности, для любых $a, b \in A$ мы имеем $a+b = (a+b)^2 = a^2+ab+ba+b^2 = a+ab+ba+b$, то есть $ab = ba$, что и требовалось.

Упражнение 1. Где в этом решении использовалась конечность антитела?

Упражнение 2. Настоящая *теорема Веддерберна* говорит, что *всякое конечное тело* (то есть ассоциативное кольцо с единицей, в котором каждый ненулевой элемент обратим) *коммутативно.* Попробуйте доказать эту гораздо более трудную (но вполне доступную второкурсникам) теорему или прочитайте в какой-нибудь книжке, как она доказывается.

Упражнение 3. Приведите примеры некоммутативых (бесконечных) тел и антител.

Упражнение 4. Покажите, что для конечномерной алгебры A с единицей над полем F следующие условия равносильны:

1. A — тело;
2. в A нет делителей нуля;
3. минимальный многочлен (над F) каждого элемента неприводим (над F);

и следующие условия тоже равносильны:

1′. алгебра A изоморфна прямой сумме тел;
2′. в A нет ненулевых нильпотентных элементов;
3′. минимальный многочлен (над F) каждого элемента свободен от квадратов, то есть не делится на квадрат никакого многочлена (над F), отличного от константы.

Упражнение 5. Докажите, что каждая конечная полугруппа содержит идемпотент (то есть, элемент, равный своему квадрату).