1 Задание со 2 занятия

Задача 1.1. Перечислите все (с точностью до изоморфизма) кольца из 4 элементов.

Доказательство. Каждое из следующих колец состоит из четырех элементов:

$$R_1 = \mathbb{Z}/4, R_2 = \mathbb{F}_2 \times \mathbb{F}_2 = \mathbb{F}_2[x]/\left(x^2+x\right), R_3 = \mathbb{F}_4 = \mathbb{F}_2[x]/\left(x^2+x+1\right), R_4 = \mathbb{F}_2[x]/\left(x^2\right)$$

Они неизоморфны, поскольку только R_3 является полем, только R_1 имеет характеристику $\neq 2$, R_2, R_3 приведены.

Обратно, пусть R — кольцо из четырёх элементов. Если $a \in R\backslash\{0,1\}$, то централизатор a является подгруппой $(R,+)$ с не менее чем тремя элементами $0, 1, a$, поэтому по Лагранжу также четвертый элемент должен коммутировать с a. Таким образом, R коммутативен. Если R приведено, то оно является конечным произведением локальных артиновых приведенных колец, т.е. полей, так что $R \cong R_2$ или $R \cong R_3$. Если R не приводится, то существует $a \in R\backslash\{0\}$ такой, что $a^2 = 0$. Поскольку $0, 1, a, a+1$ попарно различны, то это элементы R. Если $2 = 0$, то мы получаем инъективный гомоморфизм $\mathbb{F}_2[x]/\left(x^2\right) \to R, x \mapsto a$. Поскольку обе стороны имеют по четыре элемента, это изоморфизм. Если $2 \neq 0$, то характеристика должна быть равна 4, т.е. мы получаем вложение $\mathbb{Z}/4 \to R$, которое снова должно быть изоморфизмом. □

Задача 1.2. Докажите, что если простое число $p > 2$, то в группе обратимых элементов кольца $(\mathbb{Z}/p^n)^*$ есть элемент порядка $\varphi(p^n) = p^n - p^{n-1}$.

Доказательство. Заметим что $\varphi(p^n) = p^n - p^{n-1}$ - число обратимых элементов, они образуют подгруппу $\mathbb{Z}/p^n$ и эта группа циклическая, а следовательно есть элемент порядка $p^n - p^{n-1}$. □

Задача 1.3. Докажите, что если $n > 2$, то в группе обратимых элементов кольца $(\mathbb{Z}/2^n)^*$ нет элемента порядка $\varphi(2^n) = 2^{n-1}$, но есть элемент порядка 2^{n-2}.

Доказательство.

Докажем по индукции что $x^{2^{n-2}} = 1 \pmod{2^n}$

База $n = 3$ $x^{2^{3-2}} = 1 \pmod{2^3}$:

$$(2n+1)^2 = 4n^2 + 4n + 1 = 1 \pmod{2^3}$$
$$4n(n+1) = 8 \pmod{2^3}$$

Переход

$$x^{2^{k+1-2}} - 1 = x^{2^{k-2}-1} - 1 = (x^{2^{k-2}} - 1)(x^{2^{k-2}} + 1)$$

$(x^{2^{k-2}} - 1)$ кратно 2^k по предположению, $(x^{2^{k-2}} + 1)$ кратно 2 в силу нечетности x

Так как все обратимые элементы нечетные в рассматриваемой группе, то в степени 2^{n-2} они все будут давать 1, а следовательно обратимых элементов большего порядка нет. □

Задача 1.4. Докажите, что если линейный оператор f в конечномерном векторном пространстве V над некоторым полем $\mathbb{K}$ идемпотентен (т.е. $f^2 = f$ и $f \neq 0$ и $f \neq \mathrm{Id}_V$), то он является проектированием на некоторое подпространство (т.е. существует такое разложение V в прямую сумму подпространств $V = U \oplus W$, так что любой вектор $v \in V$ однозначно представляется в виде $v = u + w, u \in U, w \in W$, и тогда действие оператора состоит в том, что $f(v) = u$).

Доказательство. Распишем вектор x в виде: $x = x + F(x) - F(x)$, где $x - F(x) \in \ker(F)$ и $F(x) \in \mathrm{im}(F)$. Первое включение верно, так как при применении к нему F: $F(x-F(x)) = F(x)-F(F(x)) = F(x)-F^2(x) = F(x)-F(x) = 0$. Подпространства трансверсальны тогда и только тогда, когда все векторы $u+w = v \in U+W$ могут быть представлены единственным образом в виде $u \in U$ и $w \in W$, то есть подпространства не имеют никаких общих векторов, кроме нулевого. Пусть существует вектор, принадлежащий одновременно ядру и образу: $F(v) = 0,\ v \in F(v)$. Идемпотентный оператор действует тождественно на образ, следовательно пересечение возможно только по нулевому вектору, то есть трансверсальны. □

Задача 1.5. Верно ли утверждение предыдущей задачи без условия конечномерности V?

Доказательство. □