Семинар 1. (06/09/2019) Коммутативные алгебраические структуры

Задача 1.1. Составьте таблицы умножения для колец $\mathbb{Z}/(m)$, для $4 \leqslant m \leqslant 8$. В каждом из них найдите все обратимые элементы, все квадраты, все делители нуля и все нильпотенты. Для обратимых элементов постройте таблицу обратных.

Задача 1.2. Разделите с остатком многочлен $f(x)$ на $g(x)$ над полем $\Bbbk$ и найдите обратный к $f(x)$ в кольце вычетов $\Bbbk[x]/(g(x))$, если таковой существует.
(а) $\Bbbk = \mathbb{Q}$, $f(x) = x^5 + x^6 + 1$, $g(x) = x + 2$;
(б) $\Bbbk = \mathbb{Q}$, $f(x) = x^3 + x^2 + 1$, $g(x) = x^2 + 1$;
(в) $\Bbbk = \mathbb{F}_2$, $f(x) = x^7 + 1$, $g(x) = x^2 + x + 1$;
(г) $\Bbbk = \mathbb{F}_4 := \mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1)$, $f(x) = x^3 + x + 1$, $g(x) = x^2 + 1$;
(д) $\Bbbk = \mathbb{F}_4 := \mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1)$, $f(x) = x^3 + x + 1$, $g(x) = x^2 + [\alpha]x + 1$.

Задача 1.3. Пусть $\mathbb{F}_4 \simeq \mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1)$ – поле из четырёх элементов, которые мы обозначим $\{0, 1, [\alpha], [\alpha + 1]\}$. Найдите все делители нуля и все обратимые элементы в кольцах вычетов
(а) $\mathbb{F}_4[x]/(x^2 + [\alpha]x + 1)$, **(б)** $\mathbb{F}_4[x]/(x^2 + [\alpha + 1]x + [\alpha])$.

Задача 1.4.
(а) Покажите, что кольцо вычетов $\mathbb{F}_8 := \mathbb{F}_2[\beta]/(\beta^3 + \beta + 1)$ – поле из 8-элементов.
(б) Верно ли, что многочлены x^3+x^2+1 и x^3+x+1 имеют по три различных корня в $\mathbb{F}_8$? Разложите оба многочлена в произведение линейных множителей в $\mathbb{F}_8$.

Задача 1.5. Пусть R – кольцо с конечным числом элементов, а $R^\times$ – множество обратимых элементов этого кольца. Числом $\varphi(R)$ назовём количество элементов в $R^\times$. Верно ли, что
(а) $R^\times$ – абелева группа относительно операции умножения,
(б) любой элемент или обратим или является делителем нуля: $\forall b \in (R \setminus R^\times)\ \exists c \in R\colon bc = 0$.
(в) $\forall a \in R^\times$ выполнено $a^{\varphi(R)} = 1$,

Задача 1.6. Пусть $\mathbb{F}_p := \mathbb{Z}/(p)$, где $p \in \mathbb{N}$ – простое.
(а) Покажите, что $\mathbb{F}_p$ – поле.
(б) Решите в $\mathbb{F}_p$ уравнение $x^2 = 1$.
(в) Вычислите произведение всех ненулевых элементов $\mathbb{F}_p$ и докажите теорему Вильсона: *Натуральное число $p > 2$ – просто $\Leftrightarrow$ $(p-1)! + 1$ делится на p.*
(г) Какие значения принимают многочлены $x^p - x$, x^{p-1} и $x^{\frac{p-1}{2}}$ на $\mathbb{F}_p$ и на квадратах из $\mathbb{F}_p$.
(д) Сколько в $\mathbb{F}_p$ ненулевых квадратов? Всегда ли в $\mathbb{F}_p$ разрешимо уравнение $x^2 + y^2 = -1$.
(е) Запишем элементы $\mathbb{F}_p$ в виде $-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, 0, 1, \ldots, \frac{p-1}{2}$.
Докажите (лемму Гаусса): число $a \in \mathbb{F}_p$ тогда и только тогда является квадратом, когда число «положительных» чисел этой записи, становящихся «отрицательными» при умножении на a, чётно.

Задача 1.7. При каких p уравнения **(а)** $x^2 = -1$, **(б)** $x^2 = 2$ разрешимы в $\mathbb{F}_p$.

Задача 1.8. Бывают ли среди факторколец гауссовых чисел $\mathbb{Z}[i]$ поля характеристики 2 и 3? Что можно сказать про характеристику полей, получаемых факторкольцами чисел Эйзенштейна $\mathbb{Z}[\exp \frac{2\pi i}{3}]$.

Задача 1.9*. Для каких простых p существует гомоморфизм колец $\mathbb{Z}[i] \to \mathbb{Z}/(p)$.