Алгебра

Сидоров Дмитрий

Группа БПМИ 219

June 11, 2022

№1

Реализуем поле $\mathbb{F}_9$ в виде $\mathbb{Z}_3[x]/(x^2+x+2)$. Перечислите в этой реализации все элементы данного поля, являющиеся порождающими циклической группы $F_9^\times$.

Решение:

Заметим, что мультипликативная группа $\mathbb{F}_9$ содержит 8 элементов, тк $\mathbb{F}_9^\times = F_9\backslash\{0\}$, а значит множество порождающих элементов $\mathbb{F}_9^\times$ совпадает с множеством элементов порядка 8. Таким образом, чтобы найти порождающие элементов группы $\mathbb{F}_9^\times$ нужно рассмотреть все элементы порядка 8, тк всякая циклическая группа, порождаемая элементом x, содержит $\mathrm{ord}(x)$ элементов. Тк $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+x+2)$, то $\mathbb{F}_9 = \{0, 1, 2, \overline{x}, \overline{x}+1, \overline{x}+2, 2\overline{x}, 2\overline{x}+1, 2\overline{x}+2\}$ (все многочлены над $\mathbb{Z}_3$, степень которых меньше 2). Значит $\mathbb{F}_9^\times = \{1, 2, \overline{x}, \overline{x}+1, \overline{x}+2, 2\overline{x}, 2\overline{x}+1, 2\overline{x}+2\}$ ($\mathbb{F}_9$ без 0). Заметим, что выполняется $\overline{x}^2+\overline{x}+2=0 \Rightarrow \overline{x}^2 = -\overline{x}-2 = 2\overline{x}+1$ и $3=0$, тк характеристика поля равна 3. Выберем среди $\{1, 2, \overline{x}, \overline{x}+1, \overline{x}+2, 2\overline{x}, 2\overline{x}+1, 2\overline{x}+2\}$ те элементы, порядок которых равен 8. Для этого найдём порядок каждого элемента.

$1 = 1 \Rightarrow \mathrm{ord}(1) = 1$

$2 \to 2^2 = 1 \Rightarrow \mathrm{ord}(2) = 1$

$\overline{x} \to \overline{x}^2 = 2\overline{x}+1 \to 2\overline{x}^2+\overline{x} = 2\overline{x}+2 \to 2\overline{x}^2+2\overline{x} = 2 \to 2\overline{x} \to 2\overline{x}^2 = \overline{x}+2 \to \overline{x}^2+2\overline{x} = \overline{x}+1 \to \overline{x}^2+\overline{x} = 1 \Rightarrow \mathrm{ord}(\overline{x}) = 8$

$\overline{x}+1 \to \overline{x}^2+2\overline{x}+1 = \overline{x}+2 \to \overline{x}^2+2 = 2\overline{x} \to 2\overline{x}^2+2\overline{x} = 2 \to 2\overline{x}+2 \to 2\overline{x}^2+\overline{x}+2 = 2\overline{x}+1 \to 2\overline{x}^2+1 = \overline{x} \to \overline{x}^2+\overline{x} = 1 \Rightarrow \mathrm{ord}(\overline{x}+1) = 8$

$\overline{x}+2 \to \overline{x}^2+\overline{x}+1 = 2 \to 2\overline{x}+1 \to 2\overline{x}^2+2\overline{x}+2 = 1 \Rightarrow \mathrm{ord}(\overline{x}+2) = 4$

$2\overline{x} \to 4\overline{x}^2 = 2\overline{x}+1 \to \overline{x}^2+2\overline{x} = \overline{x}+1 \to 2\overline{x}^2+2\overline{x} = 2 \to \overline{x} \to 2\overline{x}^2 = \overline{x}+2 \to 2\overline{x}^2+\overline{x} = 2\overline{x}+2 \to \overline{x}^2+\overline{x} = 1 \Rightarrow \mathrm{ord}(2\overline{x}) = 8$

$2\overline{x}+1 \to \overline{x}^2+\overline{x}+1 = 2 \to \overline{x}+2 \to 2\overline{x}^2+2\overline{x}+2 = 1 \Rightarrow \mathrm{ord}(2\overline{x}+1) = 4$

$2\overline{x}+2 \to \overline{x}^2+2\overline{x}+1 = \overline{x}+2 \to 2\overline{x}^2+1 = \overline{x} \to 2\overline{x}^2+2\overline{x} = 2 \to \overline{x}+1 \to 2\overline{x}^2+\overline{x}+2 = 2\overline{x}+1 \to \overline{x}^2+2 = 2\overline{x} \to \overline{x}^2+\overline{x} = 1 \Rightarrow \mathrm{ord}(2\overline{x}+2) = 8$

Значит $\overline{x},\ \overline{x}+1,\ 2\overline{x},\ 2\overline{x}+2$ являются порождающими в $\mathbb{F}_9^\times$. Тогда, тк из преобразований выше видно, что каждый элемент из $\mathbb{F}_9^\times$ может быть представлен как один из элементов $\overline{x},\ \overline{x}+1,\ 2\overline{x},\ 2\overline{x}+2$ в некоторой степени, то $\overline{x},\ \overline{x}+1,\ 2\overline{x},\ 2\overline{x}+2$ являются порождающими циклической группы $\mathbb{F}_9^\times$.

Ответ: $\overline{x},\ \overline{x}+1,\ 2\overline{x},\ 2\overline{x}+2$

№2

Проверьте, что многочлены x^2+3 и y^2+y+1 неприводимы над $\mathbb{Z}_5$, и установите явно изоморфизм между полями $\mathbb{Z}_5[x]/(x^2+3)$ и $\mathbb{Z}_5[y]/(y^2+y+1)$.

Решение:

Покажем, что многочлены x^2+3 и y^2+y+1 неприводимы над $\mathbb{Z}_5$. Известно, что многочлен степени 2 неприводим над полем $\mathbb{Z}_5$ тогда и только тогда, когда он не имеет корней в поле $\mathbb{Z}_5$. Покажем, что многочлены x^2+3 и y^2+y+1 не имеют корней в $\mathbb{Z}_5$, а значит они неприводимы в $\mathbb{Z}_5[x]$ и $\mathbb{Z}_5[y]$ соотв.

$(x^2+3)(0)=3,\ (x^2+3)(1)=4,\ (x^2+3)(2)=2,\ (x^2+3)(3)=2,\ (x^2+3)(4)=4 \Rightarrow x^2+3$ не имеет корней в $\mathbb{Z}_5$ (тк $x^2+3\neq 0$ при $0\leq x\leq 4$), а значит неприводим.

Аналогично y^2+y+1 неприводим, тк $(y^2+y+1)(0)=1,\ (y^2+y+1)(1)=3,\ (y^2+y+1)(2)=2,\ (y^2+y+1)(3)=3,\ (y^2+y+1)(4)=1$.

Таким образом, получили, что что многочлены x^2+3 и y^2+y+1 неприводимы над $\mathbb{Z}_5$, а значит $\mathbb{Z}_5[x]/(x^2+3)$ и $\mathbb{Z}_5[y]/(y^2+y+1)$ - это поля. Известно, что $\exists a\in\mathbb{Z}_5/(y^2+y+1):\ (x^2+3)(a)=0$, тогда рассмотрим гомоморфизм $\varphi:\ \mathbb{Z}_5[x]\to\mathbb{Z}_5[y]/(y^2+y+1),\ f\to f(a)$ (φ является гомоморфизмом, тк сохраняет сумму и произведение, тк является взятием значения многочлена в точке a).

Найдём $\mathrm{Ker}\varphi$. По определению ядро состоит из таких многочленов f, для которых $f(a)=0$. Тк ядро является главным идеалом в $\mathbb{Z}_5$, то $\exists g\in\mathbb{Z}_5:\ \mathrm{Ker}\varphi=(g)$. Тогда, тк $(x^2+3)(a)=0$, то (x^2+3) делится на g, но тк (x^2+3) неприводим над $\mathbb{Z}_5$, то либо g - константа, либо g пропорционален x^2+3. Заметим, что, если выполняется 1-ый случай, то φ переводит все многочлены в 0, что невозможно $\Rightarrow g$ пропорционален x^2+3, а значит $\mathrm{Ker}\varphi=(x^2+3)$. Тогда по теореме о гомоморфизме колец $\mathbb{Z}_5[x]/(x^2+3)\simeq\mathrm{Im}\varphi$. При этом размерности полей $\mathbb{Z}_5[x]/(x^2+3)$ и $\mathbb{Z}_5[y]/(y^2+y+1)$ совпадают (и равны 25), а значит, тк $\mathrm{Im}\varphi\subseteq\mathbb{Z}_5[y]/(y^2+y+1)$, $\mathbb{Z}_5[y]/(y^2+y+1)=\mathrm{Im}\varphi$, а значит сущесвует изоморфизм, который каждому многочлену $f\in\mathbb{Z}_5[x]/(x^2+3)$ сопоставляет многочлен
$f(a)\in\mathbb{Z}_5[y]/(y^2+y+1)$.

Найдём этот изоморфизм явно. Для этого найдём описанный выше a. Тк $a\in\mathbb{Z}_5/(y^2+y+1)$, то a можно представить в виде многочлена степени не выше 2 (тк каждый элемент $\mathbb{Z}_5/(y^2+y+1)$ представляется в виде многочлена степени не выше $2=\deg(y^2+y+1)$), а значит $a=by+c,\ b,c\in\mathbb{Z}_5$. Тогда, тк $(x^2+3)(a)=0$, а также выполняется $\overline{y}^2=-\overline{y}-1=4\overline{y}+4$, то $a^2+3=(b\overline{y}+c)^2+3=b^2\overline{y}^2+2bc\overline{y}+c^2+3=b^2(4\overline{y}+4)+2bc\overline{y}+c^2+3=4b^2\overline{y}+4b^2+2bc\overline{y}+c^2+3=\overline{y}(4b^2+2bc)+3+4b^2+c^2=0$, а тк равенство выполняется, например, при $b=2,\ c=1$ (тк тогда $4b^2+2bc=16+4=20\ \vdots\ 5$ и $3+4b^2+c^2=20\ \vdots\ 5$), то $a=by+c=2x+1$.

Таким образом, получили изоморфизм $\mathbb{Z}_5[x]/(x^2+3)\xrightarrow{\sim}\mathbb{Z}_5[y]/(y^2+y+1)$, который задаётся как
$b\overline{x}+c\to b(2\overline{y}+1)+c$.

Ответ: $\mathbb{Z}_5[x]/(x^2+3)\xrightarrow{\sim}\mathbb{Z}_5[y]/(y^2+y+1)$, $b\overline{x}+c\to b(2\overline{y}+1)+c$

№3

Перечислите все подполя поля $\mathbb{F}_{262144}$, в которых многочлен x^3+x^2+1 имеет корень.

Решение:

Заметим, что $262144=2^{18}$, а тк $18=2\cdot 9=2\cdot 3^2$, то подполя $\mathbb{F}_{262144}$ это $\mathbb{F}_2,\ \mathbb{F}_{2^2},\ \mathbb{F}_{2^3},\ \mathbb{F}_{2^6},\ \mathbb{F}_{2^9},\ \mathbb{F}_{2^{18}}$. Заметим, что $(x^3+x^2+1)(0)=1,\ (x^3+x^2+1)(1)=1$ в $\mathbb{Z}_2\Rightarrow x^3+x^2+1$ не имеет корней в $\mathbb{Z}_2[x]$, а значит этот многочлен неприводим в $\mathbb{Z}_2[x]$, и тогда, тк $\deg(x^3+x^2+1)=3$ и $2^3=8$, то можно реализовать поле $\mathbb{F}_{2^3}$ в виде $\mathbb{Z}_2[x]/(x^3+x^2+1)$. Тогда, тк при $\overline{x}^3+\overline{x}^2+1=0$ выполняется $\overline{x}^3=-\overline{x}^2-1=\overline{x}^2+1$, то $\overline{x}^3+\overline{x}^2+1=2\overline{x}^2+2=0$, а значит в поле $\mathbb{F}_{2^3}$ x^3+x^2+1 имеет корень (тк $\overline{x}$ - это элемент поля $\mathbb{Z}_2[x]/(x^3+x^2+1)$). Заметим, что, тк 3 делит 6, 9, 18, то в $\mathbb{F}_{2^6},\ \mathbb{F}_{2^9},\ \mathbb{F}_{2^{18}}$ x^3+x^2+1 тоже имеет корень, тк эти поля являются расширением поля $\mathbb{F}_{2^3}$, а значит они содержат элемент, который является корнем многочлена x^3+x^2+1.

Теперь рассмотрим, оставшиеся поля, те $\mathbb{F}_2,\ \mathbb{F}_{2^2}$. Для $\mathbb{F}_2$ заметим, что это поле содержит 2 элемента, а тк каждое поле содержит 0 и 1, то $\mathbb{F}_2$ содержит только 0 и 1. При этом, как было показано выше, 0 и 1 не являются корнями x^3+x^2+1, а значит x^3+x^2+1 не имеет корень в $\mathbb{F}_2$.

Аналогично с $\mathbb{F}_{2^3}$ реализуем поле $\mathbb{F}_{2^2}$ в виде $\mathbb{Z}_2[x]/(x^2+x+1)$ (тк $(x^2+x+1)(0)=1,\ (x^2+x+1)(1)=1 \Rightarrow x^2+x+1$ неприводим в $\mathbb{Z}_2[x]$), и при этом элементы этого поля являются многочленами степени меньше 2, те это поле состоит из элементов $\{0,\ 1,\ \overline{x},\ \overline{x}+1\}$. Тогда при $\overline{x}^2+\overline{x}+1=0$ выполняется $\overline{x}^2=\overline{x}+1$. $(x^3+x^2+1)(0)=1,\ (x^3+x^2+1)(1)=1,\ (x^3+x^2+1)(\overline{x})=\overline{x}^2+\overline{x}+\overline{x}^2+1=\overline{x}+1,\ (x^3+x^2+1)(\overline{x}+1)=(\overline{x}+1)^3+(\overline{x}+1)^2+1=(\overline{x}+1)(\overline{x}^2+1)+(\overline{x}^2+1)+1=(\overline{x}+1)\overline{x}+\overline{x}+1=\overline{x}+1+\overline{x}+\overline{x}+1=\overline{x}$. Таким образом, значения x^3+x^2+1 от всех элементов поля $\mathbb{Z}_2[x]/(x^2+x+1)$ не равно 0, а значит x^3+x^2+1 не имеет корней в $\mathbb{F}_{2^2}$.

Итого, многочлен x^3+x^2+1 имеет корень в подполях $\mathbb{F}_{2^3},\ \mathbb{F}_{2^6},\ \mathbb{F}_{2^9},\ \mathbb{F}_{2^{18}}$.

Ответ: $\mathbb{F}_{2^3},\ \mathbb{F}_{2^6},\ \mathbb{F}_{2^9},\ \mathbb{F}_{2^{18}}$

№4

Пусть p - простое число, $q=p^n$ и $\alpha \in \mathbb{F}_q$. Докажите, что если многочлен $x^p-x-\alpha \in \mathbb{F}_q[x]$ имеет корень, то он разлагается на линейные множители.

Доказательство:

Рассмотрим поле $\mathbb{F}_p$. Заметим, что тк $q=p^n$, те q делится на p (причём единственный способом), то $\mathbb{F}_p \subseteq \mathbb{F}_q$. При этом $\forall a,b \in \mathbb{F}_q$ выполняется $(a+b)^p=a^p+b^p$, тк $\mathrm{char}\mathbb{F}_q=p$. Рассмотрим произвольный элемент $y \in \mathbb{F}_p$. Заметим, что порядок $\mathbb{F}_q^\times$ равен $p-1$, те выполняется $y^{p-1}\cdot y=e\cdot y=y \Rightarrow y^p=y$. По условию $x^p-x-\alpha$ имеет корень. Обозначим его как x_0. Тогда $x_0^p-x_0-\alpha=0$. Рассмотрим $(x^p-x-\alpha)(x_0-y)$ (значение многочлена при $x=x_0-y$) : $(x^p-x-\alpha)(x_0-y)=(x_0-y)^p-(x_0-y)-\alpha=x_0^p-y^p-x_0+y-\alpha=x_0^p-y-x_0+y-\alpha=x_0^p-x_0-\alpha=0$. Таким образом, x_0 и y образуют корень многочлена $x^p-x-\alpha$. Заметим, что в $\mathbb{F}_p$ p элементов, а тк мы брали произвольный y, то многочлен $x^p-x-\alpha$ имеет p корней, но тк его степень тоже равна p, он разлагается на линейные множители. ■