Поля. 09 июля.

Определение. Множество $\mathbb{F}$ с операциями $+$ и $\times$ называется *полем*, если выполнены следующие аксиомы:

1) **(ассоциативность сложения)** $\forall a, b, c \in \mathbb{F} \quad (a+b)+c = a+(b+c)$;
2) **(коммутативность сложения)** $\forall a, b \in \mathbb{F} \quad a+b = b+a$;
3) **(существование нуля)** $\exists 0 \in \mathbb{F} : \forall a \in \mathbb{F} \quad a+0 = 0+a = a$;
4) **(существование обратного по сложению элемента)** $\forall a \in \mathbb{F}\ \exists b : a+b = b+a = 0$;
5) **(ассоциативность умножения)** $\forall a, b, c \in \mathbb{F} \quad (a \times b) \times c = a \times (b \times c)$;
6) **(коммутативность умножения)** $\forall a, b \in \mathbb{F} \quad a \times b = b \times a$;
7) **(существование единицы)** $\exists 1 : \forall b \quad b \times 1 = 1 \times b = b$;
8) **(существование обратного по умножению элемента)** $\forall b \neq 0 \quad \exists a : a \times b = b \times a = 1$;
9) **(дистрибутивность)** $\forall a, b, c \in \mathbb{F} \quad a \times (b+c) = a \times b + a \times c$;
10) в поле $1 \neq 0$.

1. Докажите, что в поле $0 \times a = a \times 0 = 0$.
2. Докажите, что нулевой элемент, единица, обратный по сложению и обратный по умножению единственны.

Аксиомы поля позволяют рассматривать многочлены, коэффициенты которых — это элементы поля. С такими многочленами можно выполнять все привычные операции и получать привычные итоги (деление с остатком, теорема Безу, наибольший общий делитель, главноидеальность, разложение на неприводимые множители).

3. Докажите, что любая функция на поле $\mathbb{F}_p$ со значениями в $\mathbb{F}_p$ представляется в виде многочлена.
4. а) Докажите, что у многочлена $(x+1)^{2^k}$ над $\mathbb{F}_2$ всего два ненулевых коффициента. б) Найдите количество ненулевых коэффициентов многочлена $(x+1)^{2013}$ над $\mathbb{F}_2$.
Определение. Даны два поля $\mathbb{F}_1$ и $\mathbb{F}_2$. Отображение $\varphi : \mathbb{F}_1 \longrightarrow \mathbb{F}_2$ называется *изоморфизмом*, если оно является биекцией, и для любых $x, y \in \mathbb{F}_1$ выполнено $\varphi(x+y) = \varphi(x)+\varphi(y)$ и $\varphi(xy) = \varphi(x)\varphi(y)$.
Определение. Поля называются *изоморфными*, если между ними существует изоморфизм.
Определение. Изоморфизм из поля в само себя называется автоморфизмом.
5. Докажите, что при любом изоморфизме ноль переходит в ноль, единица в единицу.
6. Докажите, что при любом изоморфизме разность переходит в разность, а частное – в частное.
7. Докажите, что изоморфность полей есть отношение эквивалентности.
8. Придумайте нетождественный автоморфизм поля $\mathbb{Q}[\sqrt{2}]$.
9. Докажите, что $\mathbb{Q}[\sqrt{2}]$ и $\mathbb{Q}[\sqrt{3}]$ не изоморфны.
10. Докажите, что у поля действительных чисел нет нетождественного автоморфизма.
11. Есть ли нетождественный автоморфизм у поля комплексных чисел?