Кольца и поля

(памятка грядущим Властелинам Колец и Царицам Полей)

Коммутативное кольцо с единицей — это множество с двумя операциями: *сложением* $(a,b) \longmapsto a+b$ и *умножением* $(a,b) \longmapsto a \cdot b = ab$, которые подчиняюся следующим трём наборам аксиом.

1) Аксиомы сложения

   а) коммутативность (переместительный закон): $a+b=b+a \quad \forall a,b\,;$

   б) ассоциативность (сочетательный закон): $a+(b+c)=(a+b)+c \quad \forall a,b,c\,;$

   в) существование нейтрального элемента (нуля): $\exists\, 0 \ : \ a+0=a \quad \forall a\,;$

   г) существование противоположного: $\forall\, a \quad \exists\,(-a) \ : \ a+(-a)=0\,.$

2) Аксиомы умножения

   а) коммутативность: $ab=ba \quad \forall a,b$

   б) ассоциативность: $a(bc)=(ab)c \quad \forall a,b,c$

   в) существование единицы: $\exists\, 1 \ : \ a\cdot 1=a \quad \forall a$

3) Аксиома дистрибутивности (распределительный закон): $a(b+c)=ab+ac \quad \forall a,b,c$

Поле — это коммутативное кольцо с единицей, в котором $\forall\ a \neq 0 \quad \exists a^{-1} \ : \ a\cdot a^{-1}=1$ (аксиома существования обратного) и $0 \neq 1$ (аксиома нетривиальности). Вторая аксиома запрещает называть полем *тривиальное кольцо* $K=\{0\}$, а первая говорит, что всякий ненулевой элемент поля *обратим*. В произвольном кольце допускаются необратимые элементы и даже *делители нуля* — элементы $a \neq 0$, такие что $ab=0$ для некоторого $b \neq 0$.

М$26\frac{1}{2}\diamond$1. Может ли делитель нуля или сам нуль быть обратим в каком-либо кольце?

Примеры полей: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ (вычеты по *простому* модулю n).

Примеры колец: $\mathbb{Z}$; $\mathbb{Z}/n\mathbb{Z}$ (вычеты по модулю n); $C[0,1]$ (непрерывные функции на отрезке); $K[x]$ (многочлены с коэффициентами из любого коммутативного кольца K с единицей); $\mathbb{Q}[x]/f\mathbb{Q}[x]$ (вычеты по модулю $f \in \mathbb{Q}[x]$, называемые также *алгебраическими числами* вида $a_0\vartheta^m + a_1\vartheta^{m-1} + \cdots + a_{m-1}\vartheta + a_m$ с $f(\vartheta)=0$, $m<\deg f$, $a_i \in \mathbb{Q}$ и обозначаемое в таком контексте через $\mathbb{Q}[\vartheta]$ с $f(\vartheta)=0$; например, $\mathbb{Q}[\sqrt{2}] = \{\alpha+\beta\sqrt{2} \mid \alpha,\beta \in \mathbb{Q}\} = \mathbb{Q}[x]/(x^2-2)\mathbb{Q}[x]$ или $\mathbb{Q}[\sqrt[3]{5}] = \{\alpha+\beta\sqrt[3]{5}+\gamma\sqrt[3]{25} \mid \alpha,\beta,\gamma \in \mathbb{Q}\} = \mathbb{Q}[x]/(x^3-5)\mathbb{Q}[x]$).

М$26\frac{1}{2}\diamond$2. Верно ли, что кольцо вычетов $\mathbb{Z}/n\mathbb{Z}$ является полем тогда и только тогда, когда n просто?

М$26\frac{1}{2}\diamond$3. Верно ли, что кольцо алгебраических чисел $\mathbb{Q}[\vartheta]$ с $f(\vartheta)=0$ является полем тогда и только тогда, когда f неприводим над $\mathbb{Q}$?

М$26\frac{1}{2}\diamond$4. Верно ли, что в любом поле: **а)** нуль единственен; **б)** единица единственна; **в)** $(-a)$ однозначно определяется по a; **г)** a^{-1} однозначно определяется по a; **д)** $a\cdot 0=0\ \forall a$; **е)** $(-1)\cdot a=(-a)\ \forall a$; **ж)** $ab=ac$ и $a\neq 0 \Rightarrow b=c$?

М$26\frac{1}{2}\diamond$5. Какие свойства из зад. М$26\frac{1}{2}\diamond$4 выполнены **а)** в любом коммутативном кольце с 1? **б)** в кольце без делителей нуля?

Вычитание и деление. В любом кольце есть *вычитание*: $(a,b) \longmapsto a-b \overset{\text{def}}{=} a+(-b)$, а если b обратим, то и *деление*: $(a,b) \longmapsto a/b \overset{\text{def}}{=} ab^{-1}$.

М$26\frac{1}{2}\diamond$6. Можно ли определить $a-b$ как единственный элемент, дающий a в сумме с b?