Алгебра, листок 3 (крайний срок сдачи – 17 ноября)

Определение. Множество с парой операций, удовлетворяющих всем аксиомам поля, кроме существования обратного по умножению, называется коммутативным кольцом.
Примеры колец: поля, целые числа, многочлены с коэффициентами в данном кольце.

1. Пусть $\mathbb{Z}/p\mathbb{Z}$ – фактормножество $\mathbb{Z}$ по отношению эквивалентности

$$a \equiv b \mod p \Leftrightarrow p \text{ делит } a-b$$

с операциями $[a]+[b]=[a+b]$ и $[a]\cdot[b]=[ab]$ (через $[a]\in\mathbb{Z}/p\mathbb{Z}$ обозначается класс эквивалентности числа $a\in\mathbb{Z}$, называемый также его *вычетом* по модулю p).
a) Докажите, что операции определены корректно и определяют на $\mathbb{Z}/p\mathbb{Z}$ структуру кольца, но при непростом p это кольцо не является полем. **b)** Докажите, что при простом p и ненулевом $a\in\mathbb{Z}/p\mathbb{Z}$ отображение $f:\mathbb{Z}/p\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z}$, $f(x)=ax$, мономорфно. **c)** Выведите из этого, что $\mathbb{Z}/p\mathbb{Z}$ при простом p является полем (оно также обозначается $\mathbb{F}_p$). **d)** Докажите, что любое поле с простым количеством элементов p изоморфно $\mathbb{F}_p$. **e)** Докажите, что для любого конечного поля $\mathbb{K}$ существует простое p, такое что $\underbrace{a+\ldots+a}_{p}=0$ для любого $a\in\mathbb{K}$.

Определение. Число p из предыдущей задачи называется *характеристикой* поля $\mathbb{K}$.

2. **a)** Докажите, что для поля $\mathbb{K}$ характеристики p отображение $F:\mathbb{K}\to\mathbb{K}$, $F(x)=a^p$, является гомоморфизмом полей. **b)** Докажите, что при $\mathbb{K}=\mathbb{F}_p$ отображение F тождественно, то есть $x^p\equiv x \mod p$ для любого $x\in\mathbb{Z}$ (малая теорема Ферма).

Определение. Элемент кольца называется *обратимым*, если у него есть обратный, и *приводимым*, если представляется в виде произведения двух необратимых элементов.

3. Пусть $g\in R[x]$ – многочлен с коэффициентами в коммутативном кольце R. **a)** Докажите, что для любого многочлена $f\in R[x]$ с обратимым старшим коэффициентом существует пара многочленов r и $s\in R[x]$, $\deg r<\deg f$, такая что $g=sf+r$. **b)** Докажите, что для любого $a\in R$ существует $q\in R[x]$, такой что $g(x)=(x-a)q(x)+g(a)$.

4. **a)** Докажите, что каждая функция $\mathbb{F}_p\to\mathbb{F}_p$ представляется многочленом. **b)** Докажите, что $g(x)=x^p-x$ для простого p как функция на $\mathbb{F}_p$ тождественно нулевая, а как многочлен в $\mathbb{F}_p[x]$ разлагается на линейные множители. **c)** Докажите, что $g(x)$ и $g(x+1)$ равны как многочлены в $\mathbb{F}_p[x]$, а для любого $h\in\mathbb{F}_p[x]$ меньшей положительной степени $h(x)$ и $h(x+1)$ не равны даже как функции. **d)** Докажите, что многочлен x^p-x+1 неприводим над $\mathbb{F}_p$.

5. **a)** Редукция многочлена из $\mathbb{Z}[x]$ по модулю p – замена его коэффициентов на их вычеты по модулю p. Докажите, что неприводимость многочлена в $\mathbb{Z}[x]$ следует из неприводимости его редукции в $\mathbb{F}_p[x]$. **b)** Докажите критерий Эйзенштейна: многочлен из $\mathbb{Z}[x]$, у которого все коэффициенты кроме старшего делятся на простое число p, но при этом свободный член не делится на p^2, неприводим в кольце $\mathbb{Z}[x]$. **c)** Сделав замену $x\to x+1$, разложите на линейные множители многочлен $x^{p-1}+x^{p-2}+\ldots+x+1\in\mathbb{F}_p[x]$. **d)** Докажите, что многочлен $x^{k-1}+x^{k-2}+\ldots+x+1\in\mathbb{Z}[x]$ приводим в кольце $\mathbb{Z}[x]$ если и только если k не простое.

6. Пусть p – простое число. **a)** Решите уравнение $x^2\equiv 1 \mod p$. **b)** Докажите, что ровно половина ненулевых элементов в $\mathbb{F}_p$ являются квадратами.

7. **a)** Докажите, что уравнение $ax+by=1$ разрешимо в целых числах если и только если числа a и b взаимно просты. **b)** Докажите, что если m и n взаимно просты, то {числа, взаимно простые с mn} = {числа вида $xm+yn$, в которых x взаимно просто с n, а y – с m}.

8. Для каждого $n\in\mathbb{N}$ обозначим через $P_n\subset\mathbb{Z}/n\mathbb{Z}$ множество всех вычетов по модулю n, которые взаимно просты с n. Функция Эйлера $\varphi:\mathbb{N}\to\mathbb{N}$ – это число таких остатков: $\varphi(n)=|P_n|$. **a)** Докажите, что $\varphi(m)\varphi(n)=\varphi(mn)$ для взаимно простых m и n. **b)** Найдите $\varphi(p^a)$ для простого p. **c)** Найдите $\varphi(p_1^{a_1}\ldots p_k^{a_k})$ для простых $p_1,\ldots,p_k$.

9. **a)** Пусть $a\in\mathbb{Z}$ взаимно просто с n. Докажите, что отображение $P_n\to P_n$, сопоставляющее каждому $x\in P_n$ вычет ax по модулю n, является взаимно-однозначным. **b)** Докажите теорему Эйлера: $a^{\varphi(n)}\equiv 1 \mod n$ для любого a, взаимно простого с n.