

## 2. Делимость в ЕВКл. КоавыАХ.

Опр 1 Тусь  $A$  - ченосное коавыо. Элемент в коавыа  $A$  **делит** элемент  $a \in A$ , если  $\exists q \in A$ :  $a = qb$  (обозн:  $b \mid a$  или  $a : b$  „ $a$  делится на  $b$ “).

Э-ть  $a$  и  $b$  коавыа  $A$  **ассоцировька**, если  $a \mid b$  и  $b \mid a$  (обозн:  $a \sim b$ )

Прел 1 (св-ва делимости) Если  $A$  - ченосное коавыо, то 1)  $c \mid a$  и  $c \mid b \Rightarrow c \mid a+b$ ;

2)  $\forall a \in A \quad c \mid b \Rightarrow c \mid (ab)$

3)  $a$  и  $b$  ассоцировька  $\Leftrightarrow \exists c \in A^* : a = cb$  мн-во обр. э-ть

Упр 1 Д-ть прел 1, исходя из опр 1.

Опр 2 Число называется нормой  $A$  наз-ся **евклидовой**,  
если сущ-т ф-ция  $N: A \setminus \{0\} \rightarrow \mathbb{N}_0$

(называемая **нормой**), удовл. след. условиям:

- 1)  $N(ab) \geq N(a)$  и рав-во имеет место  $\Leftrightarrow b \in A^*$ ,
- 2)  $\forall a, b \in A, b \neq 0, \exists q, r \in A: a = qb + r$   
и мб  $r = 0$ , мб  $N(r) < N(b)$ .

Зам. В 2) не требуется единств.  $q$  и  $r$ . В 1) второе  
можно вывести из ост. условий

Примеры 1.  $A = \mathbb{Z}, N(a) = |a|$   
2.  $A = F[x], N(f) = \deg f$  } о сн. пример

Упр 2  $\Delta \rightarrow \Pi$ , что  $\mathbb{Z}[i] = \{a+bi \mid i \in \mathbb{Z}\}$  — кольцо **гел-х**  
**гауссовых чисел** евклидова норма  $N(\mathbb{Z}) = a^2 + b^2$ .

Опр 3 Наибольшим общим делителем  $a$  и  $b$

чисел  $a$  и  $b$  называется  $d \in A$  :

1)  $d | a$  и  $d | b$  ( $d$  — общий делитель  $a$  и  $b$ );

2) если  $d' \in A$  :  $d' | a$  и  $d' | b$ , то  $d' | d$ .

Обозн.  $d = (f, g)$ .

Т. 1 Если  $A$  — евкл. кольцо. Тогда для любых  $a, b \in A$

существует наиб. общий делитель  $d = (a, b)$  и  
найдутся  $u, v \in A$  :  $d = au + bv$ .

Д-во: Если  $b = 0$ , то  $(a, 0) = a = a \cdot 1 + b \cdot 0$   
и  $g$ -ть н.к.ч. Можно считать, что  $b \neq 0$ .

Лемма Если  $r$  — остаток от деления  $a$  на  $b$ , то  
н.к.ч.  $a$  и  $b$  и н.к.ч.  $b$  и  $r$

Общих делителей  $b$  и  $r$  совпадают. В частности,  
 $(a, b) = (b, r)$  (если они существуют).

$\Delta$ -во: Пусть  $a = bq + r$ . Если  $h \mid a$  и  $h \mid b$ , то  
 $h \mid r = a - bq$ . Аналогично, если  $h \mid b$  и  $h \mid r$ , то  
 $h \mid a = bq + r$ .  $\square$

$\Delta$ -во теорема: См  $\Delta$ -во т. 1.1 из [ВУН]  
и т. 1.1 из [ВМ],

Опр 4 Элементы  $a$  и  $b$  в  $R$  называются взаимно простыми, если  $(a, b) = 1$ .

Следствие (критерий взаимной простоты)

$$(a, b) = 1 \Leftrightarrow \exists u, v \in R : au + bv = 1.$$

Далее см. § 3.5 из [ВУН], начинаем с определения 4

Простой  $n$ -т конв.  $F[x]$   $n$ -ног аз. конв.  $F$   
наз-ся **неРАЗЛОЖИМЫМ**.

Средство 2 (из т-ма 2) Т.е.  $F$ -поле,  $f \in F[x]$ .

Тогда найдутся  $a \in F$  и  $p_1, \dots, p_r \in F[x]$ :

$\forall i=1, \dots, r$  и  $p_i$  — неРАЗЛОЖИМЫЙ  $n$ -т  
со старшим коэф-том 1 такие, что

$f = a p_1 \dots p_r$  и это разложение единств.  
с точностью до перестановки сомножителей.

Препр 2 Пусть  $A'$  - левка. Конъюн,  $a, b, c \in A$ .

Тогда 1)  $(a, b) = 1$  и  $(a, c) = 1 \Rightarrow (a, bc) = 1$

2)  $(a, b) = 1$  и  $a \mid (bc) \Rightarrow a \mid c$

3)  $(a, b) = 1$ ,  $a \mid c$  и  $b \mid c \Rightarrow (ab) \mid c$ .

$\Delta$ -во : см. следствие 1 (т.е. следствие из Т-мн 2 в § 3.5 из [ВУН]).

Альтернативный путь - аномальное только критичный взаимосвязи аномаль (следствие из 1),

см.  $\Delta$ -во препр. 5-2.2 из [ВМ] ■

Упр Докажите в  $\mathbb{Z}[i]$  числа 3 и 5 не простые элементы.