1 Евклидовы кольца, кольца главных идеалов, факториальные кольца

Определение 1.1 (Евклидово кольцо)**.** R - ассоциативное, коммутативное кольцо с единицей, R - евклидово, если для каждого элемента a этого кольца существует его норма $\|a\|$.

Определение 1.2 (Евклидова норма)**.** Это некоторая функция элемента кольца, такая что

1. $\|a\| \in \omega$
2. если $a, b \neq 0$, то $\|ab\| \geq \max(\|a\|, \|b\|)$
3. если $a \neq 0$, то для любого b существуют d и r такие что $b = da + r$ и $\|r\| < \|a\|$ или $r = 0$

Определение 1.3 (Кольцо главных идеалов)**.** Кольцо главных идеалов - кольцо, в котором все идеалы главные

Теорема 1.4. *Каждое евклидово кольцо - кольцо главных идеалов*

Доказательство. □

Теорема 1.5. *В кольце главных идеалов R не существует бесконечно возрастающей цепи идеалов*

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq ...$$

Доказательство. Пусть $I_0 \subseteq I_1 \subseteq I_2 \subseteq ...$ - возрастающая цепь идеалов и $I = \cup_{i=0}^{\infty} I_i$, докажем что I - идеал

1. докажем что I - подкольцо по теореме **??**

   (a) I замкнут по сложению и умножению, покажем на элементах $a, b \in I$. В таком случае в цепи есть идеалы I_j и I_k, такие что $a \in I_j$ и $b \in I_k$. Если $m \geq \max(j, k)$ то оба элемента a и b принадлежат I_m, поэтому принадлежат и $a + b$ и ab. Поэтому $a + b \in I$ и $ab \in I$

   (b) $0 \in I$ потому что $0 \in I_i$ для всякого i

   (c) Пусть $a \in I$. Тогда $a \in I_j$ Для какого-то j, в этом случае $-a \in I_j$, следовательно $-a \in I$

следовательно I - подкольцо

2. Пусть $a \in I$. Тогда $a \in I_j$ Для какого-то j. Пусть r - любой элемент R, тогда $ra \in I_j$, следовательно $ra \in I$. Следовательно $rI \subseteq I$

по определению **??** I - идеал.

Так как R - КГИ и I - идеал, то существует $a \in R$, такое что $I = aR$. Так как $a \in I$ существует n такой что $a \in I_n$. Следовательно $aR \subseteq I_n$. По определению I $I_n \subset I = aR$. I_n и I входят друг в друга следовательно $I = I_n$. Если брать любое $m \geq n$ то должно выполнятся условие $I \subseteq I_m$. Это возможно только если $I_m = I$.

Следовательно после некоторого конечного элемента n цепь идеалов перестаёт возрастать □

Определение 1.6 (Простой элемент)**.** Пусть R - ассоциативное, коммутативное кольцо с единицей, тогда a - простой, если из $a = bc$ следует что b или c обратимы

Определение 1.7 (Факториальное кольцо)**.** Пусть R - ассоциативное, коммутативное кольцо с единицей, тогда R - факториальное кольцо, если для каждого элемента $a \in R$

1. существует простые $b_1, ..., b_n$, такие что $a = b_1...b_n$

2. если $a = c_1...c_m$, где $c_1, ..., c_m$ - простые, то $m = n$, существует перестановка σ, Такая что $c_i = e_i b_{\sigma(i)}$ Для обратимого e_i

Теорема 1.8. *Существует нефакториальное кольцо*

Теорема 1.9. *R - целостное кольцо и $a \neq 0$, Тогда следующие условия эквивалентны*

1. *a - необратимый*

2. *$aR \neq R$*

3. *Для любого $b \neq 0$ $abr \neq bR$*

4. *для некоторого $b \neq 0$ $abr \neq bR$*

Доказательство. $1 \Rightarrow 2$

$ab \neq 1$ для любого b, соответствено $aR \not\ni 1$, следовательно $aR \neq R$

$2 \Rightarrow 3$

Пусть $b \neq 0$. Допустим $abR = br \ni b$. Пусть для некоторого $r \in R$ верно $abr = b$, следовательно

$$arb - b = 0 \Rightarrow (ar-1)b = 0 \Rightarrow ar - 1 = 0 \Rightarrow ar = 1$$

то есть $1 \in aR$, следовательно $aR = R$, Противоречие.

$3 \Rightarrow 4$

Если для любого $b \neq 0$ верно $abr \neq bR$, то верно и для некоторого

$4 \Rightarrow 1$

Допустим a - обратимый, то есть существует $r \in R$, такой что $ar = 1$, получается

$$abR = baR \subseteq bR$$

и

$$bR = 1 \cdot bR = arbR = abrR \subseteq abR$$

следовательно $bR = abR$, что противоречит 4, следовательно a необратим

□

Теорема 1.10. *Если R - КГИ, то каждый необратимый элемент отличный от нуля раскладывается в конечное произведение простых элементов*

Доказательство. Пусть $a \in R$, $a \neq 0$, и a - необратимый

1. Сначала покажем что a имеет в разложении простой множитель. Если a простой, то разложение завершено. Если нет, то $a = a_1 b_1$, где ни a_1 ни b_1 необратимые. Тогда $a \in a_1 R$ и $aR \subset a_1 R$. Включение строгое, потому что если $aR = a_1 R$, то для некоторого $r \in R$ было бы $a_1 = ar$ и $a = arb_1$. Так как R - целостное и $rb_1 = 1$, то b_1 - обратимый, что противоречит разложению $a = a_1 b_1$, где ни a_1 ни b_1 необратимые.

   Если a_1 не простой, то можно сказать $a_1 = a_2 b_2$, где ни a_2 ни b_2 необратимые. Получается

   $$aR \subset a_1 R \subset a_2 R$$

   где каждое включение строгое. Если a_2 не простое то можно продолжить цепь, но по теореме 1.5 цепь нельзя продолжать бесконечно и после конечного числа шагов она закончится идеалом $a_r R$, где a_r - простое число. Следовательно в разложении a есть некоторый простой элемент a_r

2. Теперь покажем что a раскладывается в произведение простых элементов R. Если a не простое, то по пункту 1 можно сказать $a = p_1 c_1$, где p_1 - простое число и c_1 необратимое. Поэтому aR строго вкладывается в $c_1 R$. Если c_1 не простой, то $c_1 = p_2 c_2$ где p_2 - простое число и c_2 необратимое. Можно построить строго возрастающую цепь идеалов
$$aR \subset c_1 R \subset c_2 R$$
Эта цепь должна остановиться после конечного числа шагов на идеале $c_r R$, где c_r - простой. Тогда
$$a = p_1 p_2 ... p_r c_r$$
разложение на конечное число простых множителей

□

Лемма 1.11. *Пусть I - идеал КГИ R. Тогда I является максимальным тогда и только тогда когда $I = pR$, где p - простой*

Доказательство. □

Теорема 1.12. *пусть R - целостное кольцо главных идеалов, тогда R - факториальное*

Доказательство. Для того чтобы показать что R - факториальное, надо показать что оно удовлетворяет условиям из 1.7:

1. по теореме 1.11

2. Надо показать что если $a = c_1 ... c_m = b_1, ..., b_n$, где $c_1, ..., c_m, b_1, ..., b_n$ - простые, то $m = n$, существует перестановка σ, Такая что $c_i = e_i b_{\sigma(i)}$ Для обратимого e_i

   Предположим что $n \geq m$. Так как $c_1 | a$, то $c_1 | b_1, ..., b_n$, то есть $c_1 | b_j$ для какого-то j. Можно переставить местами так что $c_1 | b_1$. Тогда $b_1 = c_1 e_1$ для какого-то обратимого $e_1 \in R$. Следовательно
$$c_1 c_2 ... c_m = e_1 c_1 b_2 ... b_n$$
   и
$$c_2 ... c_m = e_1 b_2 ... b_n$$
   Продолжая процесс получается
$$1 = e_1 e_1 ... e_m b_{m+1} b_n$$

Так как ни один из b_i необратим, получается $m = n$ и $c_i = e_i b_{\sigma(i)}$. Покажем что существует такая $\sigma : \{1, ..., m\} \to \{1, ..., m\}$ что σ - биекция. Определим $\sigma(i) =$ минимальный j, такой что $b_j | c_i$ и $j \notin \{\sigma(1), ..., \sigma(i-1)\}$. Нужно доказать что такой j всегда найдётся, что σ инъективна и сюръективна.

$\square$