1 Кольца и поля

Определение 1.1 (Кольцо)**.** Кольцо - алгебра сигнатуры

$$(+^{(2)}, 0^{(0)}, -^{(1)}, \cdot^{(2)})$$

обладающее свойствами:

1. $(a+b)+c = a+(b+c)$
2. $a+0 = a$
3. $a+(-a) = 0$
4. $a+b = b+a$
5. $a(b+c) = ab+ac$

Определение 1.2 (Ассоциативное кольцо)**.** Кольцо с ассоциативностью умножения $(ab)c = a(bc)$

Определение 1.3 (Кольцо с единицей)**.** Кольцо, в котором существует элемент 1, такой что $a \cdot 1 = 1 \cdot a = a$

Определение 1.4 (Коммутативное кольцо)**.** Кольцо с коммутативностью умножения $ab = ba$

Определение 1.5 (Кольцо с делением)**.** Если для любого элемента кольца $a\,(a \neq 0))$ существует $b : ab = 1$, то такое кольцо называется кольцом с делением

Определение 1.6 (Тело)**.** Тело - ассоциативное, коммутативное кольцо с делением

Определение 1.7 (Поле)**.** Поле - ассоциативное, коммутативное кольцо с делением и единицей

Пример 1.1 (Примеры колец)**.**

Теорема 1.1. *Для любых элементов кольца a, b справедливы следующие утверждения:*

1. $a0 = 0a = 0$

2. $(-a)b = a(-b) = -(ab)$

Доказательство. □

Следствие 1.1. *В кольце с 1 ноль необратим.*

Определение 1.8 (Делитель нуля)**.** Пусть $a \cdot b = 0\, a, b \neq 0$, тогда a - левый делитель нуля, b - правый делитель нуля.

Пример 1.2 (Пример делителей нуля)**.**

Теорема 1.2. *Делители нуля необратимы*

Доказательство. □

Определение 1.9 (Идемпотент кольца)**.** Такие элементы кольца, для которых выполняется $a = a^2$

Теорема 1.3. *Идемпотенты - делители нуля*

Доказательство. □

Определение 1.10 (Целостное кольцо)**.** Ассоциативное, коммутативное кольцо с единицей без делителей нуля

Теорема 1.4. *Конечное целое кольцо ?????*

Доказательство. □

Теорема 1.5. *Каждое целостное кольцо может быть достроено до поля*

Доказательство. □

Определение 1.11 (Гомоморфизм колец)**.** $h : R \to S$ - гомоморфизм, определённый так: $a \equiv b \Leftrightarrow h(a) = h(b)$

Определение 1.12 (Ядро кольца)**.** $h : R \to S$ - гомоморфизм, тогда ядро кольца $\operatorname{Ker} h = \{a \in R : h(a) = 0\}$

Теорема 1.6. *Ядро кольца - подкольцо*

Определение 1.13 (Идеал)**.** R - кольцо, $\mathcal{I} \subseteq R$ - идеал (левый, правый, двусторонний), если

1. $\mathcal{I}$ - подкольцо

2. для любого $x \in R$ $x\mathcal{I} \subseteq \mathcal{I}$ (левый идеал), $\mathcal{I}x \subseteq \mathcal{I}$ (правый идеал)

Пример 1.3 (Пример идеалов)**.**

Теорема 1.7. *R - ассоциативное кольцо с единицей или R - тело или R тогда и только тогда когда в R Нет других идеалов, кроме $\{0\}$ и R*

Определение 1.14 (Булевое кольцо)**.**

Теорема 1.8. *Пусть I - двухсторонний идеал в R, тогда отношение $\equiv$: $x \equiv y \Leftrightarrow x - y \in I$ является конгруэнтностью*

Доказательство. $\square$

Следствие 1.2. *Существует фактор-алгебра ${}^{R}/_{\equiv}$, такая что ??????????????????*

Следствие 1.3. *$I = \operatorname{Ker} h$, где $h : R \to {}^{R}/_{\equiv}$*

Доказательство. $\square$

Определение 1.15 (Простой идеал)**.** Пусть R - ассоциативное, коммутативное кольцо с единицей, тогда I - простой идеал, если $ab \in I \Leftrightarrow a \in I$ или $b \in I$

Определение 1.16 (Максимальный идеал)**.** Пусть R - ассоциативное, коммутативное кольцо с единицей, тогда I - максимальный идеал, если для любого идеала $J : I \subseteq J, I \neq J$ выполняется $J = R$

Определение 1.17 (Главный идеал)**.** Пусть R - ассоциативное, коммутативное кольцо с единицей, тогда I - главный идеал, если для некоторого $a \in R$ $I = aR$

Пример 1.4 (??????)**.**

Лемма 1.1. *Если I и J - идеалы, то $I + J$ тоже идеал*

Доказательство. $\square$

Теорема 1.9. *Пусть R - ассоциативное, коммутативное кольцо с единицей, I - идеал, тогда*

1. *I - простой идеал $\Leftrightarrow$ ${}^{R}/_{I}$ - целостное*
2. *I - максимальный идеал $\Leftrightarrow$ ${}^{R}/_{I}$ - поле*

Доказательство. $\square$

Определение 1.18 (Евклидово кольцо)**.** R - ассоциативное, коммутативное кольцо с единицей, R - евклидово, если для каждого элемента a этого кольца существует его норма $\|a\|$.

Определение 1.19 (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 $\|r\| < \|a\|$