Wykład 6 (teoria pierścieni)

DEF. **Pierścień** $R = (R, +, \cdot)$ ring

1. $(R, +)$ grupa przemienna
2. $(R, \cdot)$ łączność (półgrupa)
3. rozdzielności: $(x+y)\cdot z = x\cdot z + y\cdot z$, $z\cdot(x+y) = z\cdot x + z\cdot y$

pierścień przemienny, $x\cdot y = y\cdot x$ z jedynką, $\exists 1$ $x\cdot 1 = 1\cdot x = x$

dzielniki zera jeśli $x\cdot y = 0$ i $x, y \neq 0$, to x, y – dzielniki zera

(R z 1): elementy odwracalne, $U(R)$ – grupa jednostek a – odwracalny, jeśli $\exists b$: $a\cdot b = b\cdot a = 1$ piszemy $b = a^{-1}$

pierścień z dzieleniem – $U(R) = R\setminus\{0\}$ $\frac{a}{b} = ab^{-1}$

ciało – z dzieleniem, przemienny $F = (F, +, \cdot)$ | dwie grupy $(F, +)$ przemienne $(F\setminus\{0\}, \cdot)$ połączone rozdzielnością

Podpierścień – $S \subseteq R$ – zamkn. na dział. $+, \cdot, -$

$x, y \in S \Rightarrow x - y \in S \wedge x\cdot y \in S$

podgrupa

PRZYKŁADY:

1. $(\mathbb{Z}, +, \cdot)$, ciała: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
2. pierścień bez jedynki $2\mathbb{Z}$ - parzyste
3. $(\mathbb{Z}_m, +_m, \cdot_m)$, dzielniki zera jeśli m złożona, $m = p\cdot q$, to $p, q \in \mathbb{Z}_m$ $p, q > 1$ $p \cdot_m q = 0$
4. $\mathbb{Z}_p$ – ciało, p - liczba pierwsza (dowód – dalej)
5. $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\} \leqslant \mathbb{C}$, (dla $d \in \mathbb{Z}$, $\sqrt{d} \notin \mathbb{Z}$) podpierścień $\mathbb{Z}[\sqrt{d}] \leq \mathbb{C}$

$(a+b\sqrt{d}) - (c+f\sqrt{d}) = (a-c) + (b-f)\sqrt{d}$

$(a+b\sqrt{d})(c+f\sqrt{d}) = (ac+bfd) + (cb+af)\sqrt{d}$

$\mathbb{Z}[\sqrt{-1}] = \{a + bi : a, b \in \mathbb{Z}\}$ pierścień liczb całkowitych Gaussa

Elementarne własności:

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$
4. $(-1) \cdot a = -a$, jeśli $1 \in R$
5. $(a+b)^2 = a^2 + b^2 + ab + ba$

$(\forall a \in R)$ → d-d

$a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$

$a \cdot 0 = a \cdot 0 + a \cdot 0 \quad | -a \cdot 0$

$0 = a \cdot 0$

$a \cdot (-b)$ jest el. przeciwnym do $a \cdot b$

spr. $a \cdot (-b) + a \cdot b = a(-b+b) = a \cdot 0 = 0$ ☒

TWIERDZENIE. R przemienny z 1 jest ciałem $\iff$ nie ma dzielników zera.

skończony

Dowód: „$\Rightarrow$" Zał. że są dziel. zera $a \cdot b = 0$, $a, b \neq 0$

$a^{-1} \cdot a \cdot b = a^{-1} \cdot 0$, $b = 0$ ↯.

$\Leftarrow$ każdy el. $a \in R$ ma el. odwrotny ??

$f: R \setminus 0 \to R \setminus 0 \; / \; x \to a \cdot x$

$a \cdot 1, a \cdot 2, \ldots, a \cdot m \, 1$

$a \cdot r \equiv a \cdot s$

$a(r-c) \equiv 0$

$\exists r \; a \cdot r \equiv 1$

→ skończony

WNIOSEK 1: $\mathbb{Z}_p$ jest ciałem

(wtedy i tylko wtedy gdy p jest liczbą pierwszą)

$(\mathbb{Z}_p \setminus \{0\}, \cdot)$ grupa rzędu $p-1$

WNIOSEK 2: Małe Twierdzenie Fermata: $x^{p-1} \equiv 1 \pmod{p}$

Homomorfizm pierścieni

DEF. $f : R \to S$ homomorfizm jeśli

(i) $f(x+y) = f(x) + f(y)$ dla wszystkich $x, y \in R$

(ii) $f(x \cdot y) = f(x) \cdot f(y)$ dla wszystkich $x, y \in R$

DEF. $\mathrm{Ker} f = \{r \in R : f(r) = 0\}$ jądro

TWIERDZENIE:

(i) $\mathrm{Ker} f$ jest podgrupą $(R, +)$

(ii) $r \cdot \mathrm{Ker} f$, $\mathrm{Ker} f \cdot r \subseteq \mathrm{Ker} f$ (dla każdego $r \in R$)

$x \in \mathrm{Ker} f$.
$f(r \cdot x) = f(r) \cdot \underbrace{f(x)}_{0} = f(r) \cdot 0 = 0$
$\Rightarrow r \cdot x \in \mathrm{Ker} f$.

$\forall r \in R \; \forall x \in \mathrm{Ker} f \;\; r \cdot x \in \mathrm{Ker} f$.

Cd. (WIELOMIANY). R_{21}

wpr. oznaczenia: $x = (0,1,0,0,0,\dots)$, wtedy $x^2 = (0,0,1,0,0,\dots)$, $x^3 = (0,0,0,1,\dots)$

$(a_0, a_1, \dots, a_m, 0, 0, \dots) = a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m$, gdzie $a_i = (a_i, 0, 0, \dots)$

EX $\mathbb{Z}_2[x]$ — wielk.

pierśc. funkcji wielomianów mod $\mathbb{Z}_2$

$a_0 + a_1 x$ mod $\mathbb{Z}_2$

$0, 1$
$x, 1+x$

$x^2 = x$
$0 \cdot 0 = 0$
$1 \cdot 1 = 1$

DEF. Podzbiór $I \subseteq R$ nazywamy **ideałem**, jeśli spełnia

(i) I jest podgrupą $(R, +)$

(ii) $rI, Ir \subseteq I$ dla każdego $r \in R$

(w szczególności I jest podpierścieniem!) — szczególny podpierścień

Piszemy: $I \lhd R$

Pierścień ilorazowy R/I (dla $I \lhd R$):

$R/I = \{r+I : r \in R\}$ zbiór warstw $(R,+)$ – grupa addytywna $\quad (r+I)+(s+I) = (r+s)+I$

definiujemy mnożenie: $(r+I)\cdot(s+I) \stackrel{\text{def}}{=} (rs)+I$

TWIERDZENIE: Definicja nie zależy od wyboru reprezentantów.

Dowód: $r_1 = r+i_1$, $s_1 = s+i_2$, $i_1, i_2 \in I$ $\quad$ (wtedy $r+I = r_1+I$, $s+I = s_1+I$)

$r_1 s_1 = (r+i_1)(s+i_2) = rs + \underbrace{ri_2 + i_1 s + i_1 i_2}_{\in I}$ $\quad r_1 s_1 \in (rs)+I$

$r_1 s_1 + I = rs + I$ ☑

☑ $(R/I, +, \cdot)$ – jest pierścieniem (zwanym ilorazowym)

① ↑

② $(r+I)\cdot((s+I)\cdot(t+I)) = ((r+I)\cdot(s+I))\cdot(t+I)$

$\Vert \quad (rst)+I$

③ $(r+I)((s+I)+(t+I)) = (r+I)((s+t)+I) = (r(s+t))+I =$

$= (rs+rt)+I = (rs)+I + (rt)+I = (r+I)(s+I)+(r+I)(t+I)$

KONSTRUKCJE PIERŚCIENI

① Pierścień macierzy $n\times n$ $M_n(R)$ – dod, mnoż – niepremienny, z 1 $\begin{bmatrix}1 & & \\ & \ddots & \\ & & 1\end{bmatrix}$

② Pierścień wielomianów $R[x]$ dla R z 1.

wielomian { a) funkcja postaci $w(x) = a_0 + a_1 x + \ldots + a_m x^m$, $a_i \in R$
b) formalne wyrażenie $a_0 + a_1 x + \ldots + a_m x^m$, dodaw., mnoże. $= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots$

FORMALNIE: ciągi wiesk. postaci $w = (a_0, a_1, \ldots, a_m, 0, 0, \ldots) = (a_i)$, $m = \deg w$ – stopień wielomianu

dodaw: $(a_i)+(b_i) = (a_i+b_i)$, $(a_i)\cdot(b_i) = (c_i)$ $\quad c_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_i b_0$