WYKŁAD 5

5. Konstrukcja ciał p^n-elementowych

Def. 1: Niech $(R,+,\cdot)$ będzie pierścieniem. Podzbiór $I \subset R$ nazywamy ideałem pierścienia R, ~~jeśli~~ i oznaczamy $I \triangleleft R$, jeśli:

(1) $\forall a,b \in I \quad a-b \in I$

(2) $\forall a \in I \ \forall b \in R \quad ba \in I$

Przykład: (1) $\{n : 5|n\}$ jest ideałem w $(\mathbb{Z},+,\cdot)$.

(2) $\{f : X|f\}$ jest ideałem w $(\mathbb{R}[x],+,\cdot)$.

Def. 2: Niech $(R,+,\cdot)$ będzie pierścieniem, a $A \subset R$ pewnym zbiorem. Najmniejszy ideał pierścienia R zawierający zbiór A nazywamy ideałem generowanym przez A i oznaczamy (A). Każdy zbiór A o tej własności, że $(A) = I$ nazywamy zbiorem generatorów ideału I. Jeśli $A = \{a_1,\dots,a_n\}$ to oznaczamy

$$(a_1,\dots,a_n) := (A)$$

Mówimy, że ideał jest skończenie generowany, gdy istnieją takie elementy $a_1,\dots,a_n \in R$, że:

$$I = (a_1,\dots,a_n).$$

Mówimy, że ideał jest główny, gdy istnieje element $a \in R$ taki, że:

$$I = (a).$$

Mówimy, że pierścień R jest pierścieniem ideałów głównych gdy każdy jego ideał jest ideałem głównym.

Tw. 1 (o postaci elementów ideału generowanego przez zbiór): Niech $(R,+,\cdot)$ będzie pierścieniem oraz niech $A \subset R$. Wówczas:

$$(A) = \{a_1b_1+\dots+a_nb_n : n \in \mathbb{N},\ a_1,\dots,a_n \in A,\ b_1,\dots,b_n \in R\}.$$

Dowód: Oznaczmy

$$A_1 = \{a_1b_1+\dots+a_nb_n : n \in \mathbb{N},\ a_1,\dots,a_n \in A,\ b_1,\dots,b_n \in R\}.$$

Pokażmy, że $A_1 \triangleleft R$.

Istotnie, jeśli $a_1b_1+\dots+a_nb_n,\ a_1'b_1'+\dots+a_m'b_m' \in A_1$, to $a_1b_1+\dots+a_nb_n+a_1'(-b_1')+\dots+a_m'(-b_m') \in A_1$

Ponadto dla $b \in R$ $\quad b(a_1b_1+\dots+a_nb_n) = a_1bb_1+\dots+a_nbb_n \in A_1$

Pokażemy, że $A_1 = (A)$.

Inkluzja $(\supset)$ jest oczywista, pozostaje wykazać $(\subset)$.

Dowód prowadzimy indukcyjnie względem n.

Dla $n=1$ niech $a_1 \in A$. Wówczas a_1b_1 należy do każdego ideału zawierającego a, w szczególności do (A).

Dla $n>1$ ustalmy $a_1,\dots,a_n \in A$, $b_1,\dots,b_n \in R$ i załóżmy, że

$$a_1b_1+\dots+a_nb_n \in (A)$$

Ustalmy $a_{n+1} \in A$, $b_{n+1} \in R$. Wówczas

$$\underbrace{\underbrace{a_1b_1+\dots+a_nb_n}_{\in (A)} + \underbrace{a_{n+1}b_{n+1}}_{\in (A)}}_{\in (A)} \in (A)$$

$\square$

Przykłady: (1) W pierścieniu $\mathbb{Z}$:

$$(5) = \{k5 : k \in \mathbb{Z}\}$$
$$(4,6) = \{k4 + l6 : k, l \in \mathbb{Z}\}$$

(2) W pierścieniu $\mathbb{R}[X]$:

$$(X) = \{f \cdot X : f \in \mathbb{R}[X]\}$$

Tw. 2: Niech $(F,+,\cdot)$ będzie ciałem. Wówczas $(F[X],+,\cdot)$ jest pierścieniem ideałów głównych.

Dowód: Ustalmy $I \triangleleft F[X]$. Jeśli $I = \{0\}$, to $I = (0)$ jest ideałem głównym. Jeśli $I \neq \{0\}$ to istnieje niezerowy element $f \in I$. W szczególności możemy zdefiniować

$h :=$ wielomian z I możliwie najmniejszego stopnia $\neq 0$

Pokażemy, że $I = (h)$.

Inkluzja $(\supset)$ jest oczywista, pozostaje wykazać $(\subset)$. Ustalmy $g \in I$. Dzieląc z resztą g przez h otrzymujemy

$$g = qh + r, \quad q, r \in F[X], 0 \leqslant \deg r < \deg h.$$

W szczególności $r = g - qh \in I$. Skoro $\deg r < \deg h$, więc z wyboru h $r = 0$. Zatem $g = qh$ i $g \in (h)$ □

Def. 3: Niech $(R,+,\cdot)$ będzie pierścieniem i niech $I \triangleleft R$. **Warstwą** elementu $a \in R$ względem ideału I nazywamy zbiór

$$a + I := \{a + i : i \in I\}$$

Zbiór wszystkich warstw oznaczamy przez R/I.

Przykłady: (1) W pierścieniu $\mathbb{Z}_6$ ideał główny generowany przez element $2 \in \mathbb{Z}_6$ ma postać

$$(2) = \{0, 2, 4\}$$

Warstwy tego ideału to:

$$0 + (2) = \{0+0, 0+2, 0+4\} = (2)$$
$$1 + (2) = \{1, 3, 5\} = W$$
$$2 + (2) = \{0, 2, 4\} = (2)$$
$$3 + (2) = \{1, 3, 5\} = W$$
$$4 + (2) = (2)$$
$$5 + (2) = W$$

Zatem $\mathbb{Z}_6/(2) = \{(2), W\}$.

(2) W pierścieniu $\mathbb{Z}$ ideał główny generowany przez element (3) ma postać

$$(3) = \{0, 3, 6, 9, \dots, -3, -6, -9, \dots\}$$

Warstwy tego ideału to

$$0 + (3) = (3)$$
$$1 + (3) = \{1, 4, 7, 10, \dots, -2, -5, -8, \dots\} = W_1$$
$$2 + (3) = \{2, 5, 8, 11, \dots, -1, -4, -7, \dots\} = W_2$$
$$3 + (3) = (3)$$

Zatem $\mathbb{Z}/(3) = \{(3), W_1, W_2\}$ i $\mathbb{Z}/(3)$ można utożsamić z $\mathbb{Z}_3$

(3) Kluczowa konstrukcja tego wykładu to przeniesienie pomysłu z przykładu (2) na pierścień wielomianów nad ciałem skończonym.

W pierścieniu $\mathbb{Z}_2[X]$ ~~wielomian~~ ideał główny generowany przez X^2+X+1 ma postać

$$(X^2+X+1) = \{X^2+X+1,\ X^3+X^2+X,\ X^3+X^2+X+X^2+X+1, \dots, f(X)\cdot(X^2+X+1)\}$$

Warstwy tego ideału to

$$0+(X^2+X+1) = (X^2+X+1)$$
$$1+(X^2+X+1) = W_1$$
$$X+(X^2+X+1) = W_2$$
$$X+1+(X^2+X+1) = W_3$$

Dowolna inna warstwa będzie równa $(X^2+X+1), W_1, W_2, W_3$:
ustalmy warstwę $f+(X^2+X+1)$ i niech $g \in f+(X^2+X+1)$.
Wówczas $g = f + q_h(X^2+X+1)$. Dzieląc f z resztą przez X^2+X+1 mamy

$$f = q_1(X^2+X+1)+r_1 \quad \text{oraz } 0 \le \deg r_1 < \deg(X^2+X+1) = 2$$

Jedyne możliwe wybory dla r_1 to

$$0,\ 1,\ X,\ X+1$$

a zatem jeżeli np. $r_1 = X+1$ to

$$g = f+q_h(X^2+X+1) = q_1(X^2+X+1)+(X+1)+q_h(X^2+X+1) =$$
$$=(X+1)+(q_1+q_h)(X^2+X+1) \in W_3$$

Zatem $\mathbb{Z}_2[X]/(X^2+X+1) = \{(X^2+X+1), W_1, W_2, W_3\}$ i
$\mathbb{Z}_2[X]/(X^2+X+1)$ można utożsamić z możliwymi resztami z dzielenia przez wielomian X^2+X+1.

Tw.3: Niech $(F,+,\cdot)$ będzie ciałem, niech $p \in F[X]$ będzie wielomianem nierozkładalnym tj. takim, że jeśli

$$p = f \cdot g, \quad f, g \in F[X]$$

to $\deg f = 0$ lub $\deg g = 0$. W zbiorze warstw $F[X]/(p)$ wprowadzamy dodawanie:

$$(f+(p)) + (g+(p)) = (f+g)+(p)$$

oraz mnożenie

$$(f+(p)) \cdot (g+(p)) = f \cdot g + (p)$$

Wówczas $F[X]/(p)$ jest ciałem.

Dowód: Pokażemy dla przykładu, że dowolny element $\neq (p)$ jest odwracalny.
Ustalmy $f+(p) \in F[X]/(p)$. Ponieważ $f+(p) \neq (p)$, więc $f \notin (p)$ i tym samym $p \nmid f$. Ponadto p jest nierozkładalny, a więc $NWD(f,p)=1$.
Wobec algorytmu Euklidesa istnieją $a, b \in F[X]$ takie, że:

$$af + bp = 1$$

Wówczas $af = 1 - bp \in 1+(p)$, a więc $(a+(p))\cdot(f+(p)) = 1+(p)$ □

Uwaga: Niech $F[X]/(p)$ będzie ciałem zdefiniowanym przez wielomian nierozkładalny p. Oznaczamy:

$$a_n a_{n-1} \dots a_1 a_0 := a_n X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0 + (p)$$

Przykład: $10 = X + (X^2+X+1)$ w $\mathbb{Z}_2[X]$.