

15. WYKŁAD 15: PODCIAŁA, PODCIAŁA GENEROWANE PRZEZ ZBIÓR, ROZSZERZENIA CIAŁ.
CHARAKTERYSTYKA PIERŚCIENIA I CIAŁA, CIAŁA PROSTE I KLASYFIKACJA CIAŁ PROSTYCH.

15.1. Podciała, podciała generowane przez zbiór, rozszerzenia ciał.

Definicja 15.1. Niech F będzie ciałem. Podzbiór $L \neq \emptyset$ zbioru F nazywamy **podciałem** ciała F (piszemy $L < F$), gdy $(L, +|_{L \times L}, \cdot|_{L \times L})$ jest ciałem.

Jeżeli $L < F$ to mówimy, że F jest **rozszerzeniem** ciała L .

Przykłady:

- (1) $\mathbb{Q} < \mathbb{R}$,
- (2) $\mathbb{R} < \mathbb{C}$.

Twierdzenie 15.1. Niech F będzie ciałem i niech $\emptyset \neq L \subset F$. Następujące warunki są równoważne:

- (1) $L < F$,
- (2) L ma następujące własności:
 - $1 \in L$,
 - $\forall x, y \in L (x - y \in L)$,
 - $\forall x, y \in L (x \cdot y^{-1} \in L)$.

Twierdzenie 15.2. Niech $\mathcal{R} = \{L_i : i \in I\}$ będzie rodziną podciał ciała F ;

- (1) $\bigcap_{i \in I} L_i$ jest podciałem ciała F ,
- (2) $\bigcup_{i \in I} L_i$ jest podciałem ciała F , o ile $\mathcal{R}$ jest łańcuchem.

Definicja 15.2. Niech F będzie ciałem oraz $A \subset F$ pewnym zbiorem. Niech ponadto $L < F$. Najmniejsze w sensie inkluzji podciało ciała F zawierające zbiór $L \cup A$ (tj. przekrój wszystkich podciał ciała F zawierających $L \cup A$) nazywamy **podciałem generowanym przez A nad L** (rozszerzeniem ciała L o zbiór A , rozszerzeniem ciała L o elementy zbioru A) i oznaczamy $L(A)$.

Jeżeli $A = \{a_1, \dots, a_n\}$, to ciało $L(\{a_1, \dots, a_n\})$ nazywamy **podciałem skończenie generowanym przez A nad L** (rozszerzeniem skończenie generowanym ciała L o zbiór A) i oznaczamy $L(a_1, \dots, a_n)$.

Jeżeli $A = \{a\}$ to skończenie generowane rozszerzenie $L(a)$ ciała L o element a nazywamy **rozszerzeniem prostym**.

Twierdzenie 15.3 (o postaci elementów rozszerzenia ciała o zbiór). Niech F będzie ciałem oraz $A \subset F$ pewnym zbiorem. Niech $L < F$. Wówczas

$$L(A) = \left\{ \frac{f(a_1, \dots, a_n)}{g(a_1, \dots, a_n)} : f, g \in L[x_1, \dots, x_n], g(a_1, \dots, a_n) \neq 0, a_1, \dots, a_n \in A, n \in \mathbb{N} \right\}.$$

Wniosek 15.1. (1) Niech F będzie ciałem oraz niech $a \in F$. Niech $L < F$. Wówczas

$$L(a) = \left\{ \frac{x_0 + x_1 a + \dots + x_n a^n}{y_0 + y_1 a + \dots + y_n a^n} : y_0 + y_1 a + \dots + y_n a^n \neq 0, n \in \mathbb{N} \cup \{0\}, x_i, y_i \in K \right\}.$$

(2) Niech F będzie ciałem oraz niech $\{a_1, \dots, a_n\} \subset F$. Niech $K < F$. Wówczas

$$L(a_1, \dots, a_n) = \left\{ \frac{f(a_1, \dots, a_n)}{g(a_1, \dots, a_n)} : f, g \in L[x_1, \dots, x_n], g(a_1, \dots, a_n) \neq 0 \right\}.$$

(to znaczy elementy rozszerzenia ciała o zbiór skończony są wartościami funkcji wymiernych o współczynnikach z danego ciała).

Przykłady:

(3) Niech $F = \mathbb{C}$, $\sqrt{2} \in \mathbb{C}$, $L = \mathbb{Q} < \mathbb{C}$. Wówczas:

$$\mathbb{Q}(\sqrt{2}) = \left\{ \frac{f(\sqrt{2})}{g(\sqrt{2})} : f, g \in \mathbb{Q}[x], g(\sqrt{2}) \neq 0 \right\}.$$

Definicja 15.3. Niech F będzie ciałem oraz niech $L_1 < F, L_2 < F, \dots, L_n < F$. Podciało generowane przez $L_2 \cup \dots \cup L_n$ nad L_1 nazywamy **kompozytem** (lub **iloczynem**) ciał $L_1, L_2, \dots, L_n$ i oznaczamy $L_1 \cdot L_2 \cdot \dots \cdot L_n$.

Uwaga 15.1. (1) Niech F będzie ciałem oraz niech $L_1 < F, L_2 < F$. Niech $\{a_1, \dots, a_n\} \subset F$ oraz $\{b_1, \dots, b_m\} \subset F$. Wówczas:

$$L_1(a_1, \dots, a_n) \cdot L_2(b_1, \dots, b_m) = L_1 \cdot L_2(a_1, \dots, a_n, b_1, \dots, b_m).$$

(2) Niech F będzie ciałem oraz niech $L < F$. Niech $\{a_1, \dots, a_n\} \subset F$ oraz $\{b_1, \dots, b_m\} \subset F$. Wówczas

$$L(a_1, \dots, a_n) \cdot L(b_1, \dots, b_m) = L(a_1, \dots, a_n, b_1, \dots, b_m).$$

(3) Niech F będzie ciałem oraz niech $L_1 < F, L_2 < F$. Niech $K_1 < L_1$ oraz niech $K_2 < L_2$. Wówczas

$$K_1 \cdot K_2 < L_1 \cdot L_2.$$

Uwaga 15.2. Niech F, L będą ciałami, niech $\phi : F \rightarrow L$ będzie homomorfizmem. Wówczas ϕ jest różnowartościowy.

Dowód. Ponieważ ϕ jest homomorfizmem, więc $\ker \phi < F$. Ponieważ jednak F jest ciałem, więc $\ker \phi \in \{\{0\}, F\}$. Gdyby $\ker \phi = F$, to w szczególności $\phi(1) = 0$, a więc ϕ nie byłby homomorfizmem. Zatem $\ker \phi = \{0\}$. $\square$

Definicja 15.4. Niech F będzie ciałem, niech $F < K$ i $F < L$ będą jego rozszerzeniami. Niech ponadto $\phi : K \rightarrow L$ będzie homomorfizmem. Jeśli $\phi|_F = \text{id}_F$, to ϕ nazywamy F -zanurzeniem.

Twierdzenie 15.4. Niech F, L będą ciałami, niech $F_1 < F, L_1 < L$, niech $\phi : F \rightarrow L$ będzie homomorfizmem. Wówczas:

- (1) $\phi(F_1) < L$,
- (2) $\phi^{-1}(L_1) < F$.

15.2. Charakterystyka pierścienia i ciała, ciała proste i klasyfikacja ciał prostych.

Definicja 15.5. Niech R będzie pierścieniem. Liczbę:

$$\text{char} R = \begin{cases} 0, & \text{gdy } r(1) = \infty \text{ w grupie addytywnej } (R, +), \\ n, & \text{gdy } r(1) = n \text{ w grupie addytywnej } (R, +), \end{cases}$$

nazywamy **charakterystyką** pierścienia R .

Przykłady:

- (1) $\text{char} \mathbb{Z} = 0, \text{char} \mathbb{Q} = 0$;
- (2) $\text{char} \mathbb{Z}_4 = 4, \text{char} \mathbb{Z}_7 = 7$;
- (3) $\text{char} \mathbb{R}[x] = 0$;
- (4) $\text{char} \mathbb{Z}_5[x] = 5$.

Uwaga 15.3. Niech R będzie pierścieniem. Odwzorowanie $\phi : \mathbb{Z} \rightarrow R$ dane wzorem

$$\phi(m) = m \cdot 1$$

jest homomorfizmem pierścieni. Jeśli $\text{char} R = 0$, to $\ker \phi = \{0\}$. Jeśli $\text{char} R = n$, to $\ker \phi = (n)$.

Dowód. Bez trudu pokazujemy, że ϕ jest homomorfizmem. Załóżmy, że $\text{char} R = 0$. Pokażemy, że $\ker \phi = \{0\}$. Ustalmy $m \in \ker \phi$. Wówczas

$$m \in \ker \phi \Leftrightarrow m \cdot 1 = 0 \Leftrightarrow m = 0.$$

Załóżmy, że $\text{char} R = n$. Pokażemy, że $\ker \phi = (n)$. Ustalmy $m \in \ker \phi$. Wówczas

$$m \in \ker \phi \Leftrightarrow m \cdot 1 = 0 \Leftrightarrow n|m \Leftrightarrow m \in (n).$$

□

Wniosek 15.2. Niech R będzie pierścieniem.

- (1) Jeśli $\text{char} R = 0$, to R zawiera podpierścień izomorficzny z $\mathbb{Z}$.
- (2) Jeśli $\text{char} R = n$, to R zawiera podpierścień izomorficzny z $\mathbb{Z}_n$.

Dowód. (1) Zdefiniujmy odwzorowanie $\phi : \mathbb{Z} \rightarrow R$ wzorem

$$\phi(m) = m \cdot 1.$$

Oznaczmy $R_1 = \text{im} \phi$. Wobec twierdzenia o izomorfizmie

$$\mathbb{Z} / \ker \phi \cong R_1.$$

Ponieważ $\ker \phi = \{0\}$, więc $R \cong \mathbb{Z} / \{0\} \cong \mathbb{Z}$.

- (2) Analogicznie.

□

Wniosek 15.3. Niech R będzie pierścieniem.

- (1) Jeśli R jest pierścieniem całkowitym, to $\text{char} R = 0$ lub $\text{char} R = p$ dla pewnej liczby pierwszej p .
- (2) Jeśli R jest ciałem, to $\text{char} R = 0$ lub $\text{char} R = p$ dla pewnej liczby pierwszej p .

Dowód. (1) Przypuśćmy, że $\text{char} R = pq$, dla pewnych liczb pierwszych p, q . Wówczas R zawiera pierścień izomorficzny z $\mathbb{Z}_{pq}$, a więc $p, q \in \mathcal{D}(\mathbb{Z}_{pq}) \subset \mathcal{D}(R)$, co daje sprzeczność.

- (2) Oczywiście.

□

Przykłady:

- (5) $\text{char} \mathbb{R} = 0$;
- (6) $\text{char} \mathbb{Z}_p = p$, gdzie p jest dowolną liczbą pierwszą.

Uwaga 15.4. Niech R będzie pierścieniem i niech $R_1 < R$. Wówczas $\text{char} R_1 = \text{char} R$.

Uwaga 15.5. Niech R będzie pierścieniem i niech $\text{char} R = p$. Wówczas

- (1) $\forall a, b \in R (a + b)^p = a^p + b^p$;
- (2) $\forall a, b \in R (a + b)^{p^n} = a^{p^n} + b^{p^n}$.

Dowód. (1) Ponieważ

$$(a+b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k}$$

oraz

$$\forall k \in \{1, \dots, p-1\} p \mid \binom{p}{k}$$

więc

$$\forall k \in \{1, \dots, p-1\} \binom{p}{k} a^k b^{p-k} = 0.$$

(2) Indukcja. □

Definicja i Uwaga 15.1. Niech F będzie ciałem i niech $\text{char} F = p$. Wówczas odwzorowanie $\phi : F \rightarrow F$ dane wzorem

$$\phi(a) = a^p$$

jest homomorfizmem ciał. Obraz $\text{im} \phi$ oznaczamy przez F^p i nazywamy **p -potęgą ciała F** .

Definicja 15.6. Ciało F nazywamy **ciałem prostym** gdy nie zawiera podciała właściwych.

Twierdzenie 15.5. Niech F będzie ciałem. Wówczas F zawiera podciało proste.

Dowód. Zdefiniujmy

$$K = \bigcap \{L : L < F\}.$$

Wówczas K jest podciałem ciała F . Pokażemy, że K jest ciałem prostym. Ustalmy $M < K$. Wówczas $M < F$, więc $K \subset M$ i tym samym $K = M$. □

Twierdzenie 15.6 (o klasyfikacji ciał prostych). Niech F będzie ciałem prostym. Wówczas

- (1) Jeśli $\text{char} F = 0$, to $F \cong \mathbb{Q}$.
- (2) Jeśli $\text{char} F = n$, to $F \cong \mathbb{Z}_p$.

Dowód. (1) Odwzorowanie $\phi : \mathbb{Z} \rightarrow F$ dane wzorem

$$\phi(m) = m \cdot 1$$

jest różnowartościowym homomorfizmem. Wobec własności uniwersalnej ciała ułamków, istnieje dokładnie jeden homomorfizm różnowartościowy $\psi : (\mathbb{Z}) \rightarrow F$ taki, że

$$\psi \circ \lambda = \phi,$$

gdzie $\lambda : \mathbb{Z} \rightarrow (\mathbb{Z})$ jest homomorfizmem kanonicznym. Ponadto $\text{im} \psi < F$ i skoro F jest proste, więc $\text{im} \psi = F$. Wobec tego $\mathbb{Q} \cong (\mathbb{Z}) \cong F$.

(2) Odwzorowanie $\phi : \mathbb{Z} \rightarrow F$ dane wzorem

$$\phi(m) = m \cdot 1$$

jest homomorfizmem takim, że $\ker \phi = (p)$. Wobec twierdzenia o homomorfizmie istnieje dokładnie jeden homomorfizm $\psi : \mathbb{Z}/(p) \rightarrow F$ taki, że

$$\psi \circ \kappa = \phi,$$

gdzie $\kappa : \mathbb{Z} \rightarrow \mathbb{Z}/(p)$ jest epimorfizmem kanonicznym. Ponadto $\mathbb{Z}/(p)$ jest ciałem, więc ψ jest różnowartościowy. Ponadto $\text{im} \psi < F$ i skoro F jest ciałem prostym, to $\text{im} \psi = F$. Wobec tego $\mathbb{Z}_p \cong F$.

□

Wniosek 15.4. *Niech F będzie ciałem. Wówczas*

- (1) *Jeśli $\text{char} F = 0$, to F zawiera podciało izomorficzne z $\mathbb{Q}$.*
- (2) *Jeśli $\text{char} F = p$, to F zawiera podciało izomorficzne z $\mathbb{Z}_p$.*

Wniosek 15.5. *Niech F będzie ciałem o p elementach, gdzie p jest liczbą pierwszą. Wówczas $F \cong \mathbb{Z}_p$.*

Dowód. Charakterystyka ciała F jest różna od 0, a zatem równa pewnej liczbie pierwszej q . Tym samym F zawiera podciało izomorficzne z $\mathbb{Z}_q$. W szczególności grupa addytywna $(F, +)$ ciała F zawiera jako podgrupę grupę izomorficzną z grupą addytywną $(\mathbb{Z}_q, +)$ ciała $\mathbb{Z}_q$. Stąd, wobec twierdzenia Lagrange'a, $q|p$ i w konsekwencji $q = p$. □

Definicja 15.7. *Niech F będzie ciałem. Pierścieniem prostym zawartym w ciele F nazywamy*

- $\mathbb{Z}$, jeżeli $\text{char} F = 0$,
- $\mathbb{Z}_p$, jeżeli $\text{char} F = p$, dla pewnej liczby pierwszej p .

Uwaga 15.6. *Niech F będzie ciałem prostym, niech $F < K$ i $F < L$ będą jego rozszerzeniami. Niech ponadto $\phi: K \rightarrow L$ będzie homomorfizmem. Wówczas ϕ jest F -zanurzeniem.*

Dowód. Z definicji $\phi(1) = 1$ i skoro ϕ jest homomorfizmem, to

$$\phi\left(\underbrace{1 + \dots + 1}_m\right) = \underbrace{1 + \dots + 1}_m.$$

Jeśli $\text{char} F = p$, to dowód jest zakończony. Jeśli $\text{char} F = 0$, to, dalej z definicji homomorfizmu, mamy:

$$\phi\left(\frac{\underbrace{1 + \dots + 1}_m}{\underbrace{1 + \dots + 1}_n}\right) = \frac{\phi\left(\underbrace{1 + \dots + 1}_m\right)}{\phi\left(\underbrace{1 + \dots + 1}_n\right)} = \frac{\underbrace{1 + \dots + 1}_m}{\underbrace{1 + \dots + 1}_n}.$$

□