13. Ciała. Rozszerzenia ciał.

Z rozważań poprzedniego paragrafu wynika, że jeżeli wielomian f o współczynnikach w ciele K jest nierozkładalny, to pierścień ilorazowy $K[X]/(f)$ jest ciałem zawierającym ciało K. Przytoczmy ponownie szczególne przykłady tej konstrukcji.

13.1. Przykłady.

1. $\mathbb{Z}_2 \subseteq \mathbb{Z}_2[X]/(X^2+X+1)$ jest ciałem czteroelementowym zawierającym $\mathbb{Z}_2$.
2. Rozważmy homomorfizm $\Phi\colon \mathbb{Q}[X] \to \mathbb{R}$, $\Phi(X) = \sqrt{2}$, którego jądrem jest (X^2-2) zaś obrazem podciało ciała liczb rzeczywistych $\{a+b\sqrt{2}\colon a,b \in \mathbb{Q}\}$. Oznaczamy je symbolem $\mathbb{Q}(\sqrt{2})$. Mamy więc $\mathbb{Q} \subseteq \mathbb{Q}[X]/(x^2-2) \cong \mathbb{Q}(\sqrt{2})$. W ciele $\mathbb{Q}(\sqrt{2})$ wielomian X^2-2 jest iloczynem $(X-\sqrt{2})(X+\sqrt{2})$.
3. Rozważmy homomorfizm $\Phi\colon \mathbb{R}[X] \to \mathbb{C}$, $\Phi(X) = i$, którego jądrem jest (X^2+1) zaś obrazem ciało liczb zespolonych. Mamy więc $\mathbb{R} \subseteq \mathbb{R}[X]/(x^2+1) \cong \mathbb{C}$. W ciele $\mathbb{C}$ wielomian $X^2+1 = (X+i)(X-i)$.

Przypomnijmy i uzupełnijmy podstawowe definicje i fakty dotyczące ciał.

13.2. Definicja. *Charakterystyką ciała K nazywamy najmniejszą liczbę naturalną $n \in N$, dla której* $\underbrace{1+\cdots+1}_{n-\text{ razy}} = 0$.

Jeżeli taka liczba nie istnieje, to mówimy, że ciało ma charakterystykę 0. *Charakterystykę ciała K oznaczamy symbolem $\chi(K)$.*

Nietrudno sprawdzić, że charakterystyka ciała, o ile jest różna od zera, musi być liczbą pierwszą.

13.3. Przykłady. Ciałami charakterystyki p są $\mathbb{Z}_p$, $\mathbb{Z}_p[X]/(f)$, gdzie f jest wielomianem nierozkładalnym w $\mathbb{Z}_p[X]$, ciało funkcji wymiernych $Q(\mathbb{Z}_p[X]) = \mathbb{Z}_p(X)$.

Twierdzenie Bézout i grupa multyplikatywna ciała

Niech K będzie ciałem i niech $f \in K[X]$ będzie niezerowym wielomianem. Mówimy, że $a \in K$ jest pierwiastkiem wielomianu f, $f = a_0+a_1X+\cdots+a_nX^n$ jeżeli $f(a) = a_0 + a_1a + \cdots + a_na^n = 0$.

13.4. Twierdzenie Bézout. *Niech K będzie ciałem i niech $f \in K[X]$ i $f \neq 0$. Wówczas*

a) dla $a \in K$, $f(a) = 0$ wtedy i tylko wtedy gdy $(x-a) \mid f$ w $K[X]$;

b) liczba pierwiastków wielomianu f jest mniejsza równa od stopnia $\deg f$.

Dowód. Pierścień $K[X]$ jest dziedziną euklidesową, więc $f = g(X-a)+c$, gdzie $c \in K$ jest wielomianem stopnia 0. Jest jasne, że $f(a) = 0 \iff c = 0$, co dowodzi punktu a). Punkt b) łatwo dowodzimy przez indukcję korzystając z a). □

13.5. Wniosek. *Niech K będzie całem a K^* jego grupą multyplikatywną. Wówczas dowolna skończona podgrupa $G \leqslant K^*$ jest cykliczna.*

Dowód. Skorzystamy z charakteryzacji grup cyklicznych zawartej w Stwierdzeniu 3.4. Niech $k||G|$. Wówczas dla elementu $a \in G$, $o(a)|k$ wtedy i tylko wtedy, gdy $a^k = 1$, czyli wtedy i tylko wtedy, gdy a jest pierwiastkiem wielomianu X^k-1. Z twierdzenia Bézout wynika, że liczba tych pierwiastków jest nie większa od k, zatem G zawiera co najwyżej jedną podgrupę rzędu k, co dowodzi że G jest cykliczna. □

13.6. Wniosek. *Grupa $Aut(\mathbb{Z}_p)$ jest izomorficzna z $\mathbb{Z}_{p-1}$.*

Badanie homomorfizmów ciał zacznijmy od łatwej uwagi:
13.7. Uwaga Niech K będzie ciałem, a $\varphi : K \to L$ homomorfizmem pierścieni. Wówczas dla dowolnego $a \neq 0$, $a \in K$ mamy $\varphi(aa^{-1}) = \varphi(1) = 1 = \varphi(a)\varphi(a^{-1})$, więc $\varphi(a) \neq 0$ i φ jest monomorfizmem. Jeżeli L jest ciałem, to φ jest homomorfizmem ciał.
13.8. Przykład. Niech K będzie ciałem charakterystyki p. Wówczas przekształcenie zadane wzorem $\Phi(x) = x^p$ jest endomorfizmem tego ciała zwanym endomorfizmem Frobeniusa. Jeśli $|K| < \infty$ to endomorfizm Frobeniusa jest automorfizmem. Dla ciała $\mathbb{Z}_p$ jest on identycznością. Dla ciała czteroelementowego z Przykładu 13.1, 1) jest on nietrywialną inwolucją.

Rozszerzenia ciał.

Niech K będzie ciałem a R pierścieniem i niech $K \leqslant R$. Wówczas R ma strukturę przestrzeni liniowej nad K z dodawaniem wektorów i mnożeniem wektorów przez skalary z K zdefiniowanym przez mnożenie w pierścieniu R. Wymiar tej przestrzeni liniowej oznaczamy symbolem $|R : K|$.

13.9. Stwierdzenie. *Niech $f \in K[X]$ będzie wielomianem. Wówczas wymiar $|K[X]/(f) : K|$ pierścienia $K[X]/(f)$ jako przestrzeni liniowej nad K jest równy $deg f$.*

Dowód. Jest oczywiste, że warstwy $1 + (f)$, $X + (f)$, $\ldots$, $X^{n-1} + (f)$ są bazą $K[X]/(f)$ nad K. □

13.10. Stwierdzenie. *Niech K będzie ciałem zawartym w dziedzinie całkowitości R. Jeżeli $|R : K| < \infty$, to R jest ciałem.*

Dowód. Niech $a \in R$, $a \neq 0$. Przekształcenie $\phi_a : R \to R$, $\phi_a(r) = ar$ jest K liniowe i jest monomorfizmem, gdyż R jest dziedziną całkowitości. Jeżeli wymiar R nad K jest skończony to jest epimorfizmem i dla pewnego $r \in R$, $ar = 1$. □

13.11. Definicja. *Jeżeli $K \subseteq L$, gdzie K jest podciałem ciała L, to mówimy, że ciało L jest* **rozszerzeniem** *ciała K. Wymiar $|L : K|$ nazywamy* **stopniem rozszerzenia**.

13.12. Uwaga Jeżeli $K \subseteq L$ jest rozszerzeniem, to $\chi(K) = \chi(L)$.
13.13. Przykład. Jeżeli $\chi(K) = p$, to K jest rozszerzeniem ciała $\mathbb{Z}_p$. Jeżeli $|K : \mathbb{Z}_p| = n$, to ciało K ma p^n elementów. Jeżeli $\chi(K) = 0$, to $\mathbb{Q} \subseteq K$. Ciała $\mathbb{Z}_p$ i $\mathbb{Q}$ nie mają podciał właściwych i nazywamy je ciałami prostymi.

13.14. Wniosek. *Niech $f \in K[X]$ będzie wielomianem nierozkładalnym. Rozszerzenie $K \subseteq K[X]/(f)$ jest stopnia $deg f$.*

13.15. Przykłady. Rozszerzenia $\mathbb{Z}_2 \subseteq \mathbb{Z}_2[X]/(X^2 + X + 1)$, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$, $\mathbb{R} \subseteq \mathbb{C}$ są rozszerzeniami stopnia 2. Rozszerzenia $\mathbb{Q} \subseteq \mathbb{R}$, $K \subseteq K(X)$ są rozszerzeniami nieskończonego stopnia.

13.16. Stwierdzenie. *Niech $K \subseteq L \subseteq M$ będzie ciągiem rozszerzeń. Rozszerzenie $K \subseteq M$ jest skończone wtedy i tylko wtedy, gdy rozszerzenia $K \subseteq L$ i $L \subseteq M$ są skończone. Wówczas*

$$|M : K| = |M : L| \cdot |L : K|.$$

Dowód. Jest oczywiste, że jeżeli $|M : K| < \infty$ to $|L : K| < \infty$ i $|M : L| < \infty$. Niech $|L : K| = n$ i $l_1, \ldots, l_n$ będzie bazą L nad K. Podobnie niech $|M : L| = r$ i $m_1, \ldots, m_r$ będzie bazą M nad L. Łatwo sprawdzić, że $\{l_i m_j\}_{0 \leq i \leq n, 0 \leq j \leq r}$ jest liniowo niezależnym zbiorem generatorów M jako przestrzeni liniowej nad K. □

13.17. Definicja. *Niech $K \subseteq L$ będzie rozszerzeniem. Element $a \in L$ nazywamy algebraicznym nad K wtedy i tylko wtedy, gdy istnieje wielomian $f \in K[X]$ taki, że $f(a) = 0$. Element $a \in L$, ktory nie jest algebraiczny nad K nazywamy elementem przestępnym nad K.*

Niech $K \subseteq L$ będzie rozszerzeniem. Dla elementu $a \in L$, zdefiniujmy

$$K[a] = \{f(a) \mid f \in K[X]\} \leqslant L,$$

$$K(a) = \{\frac{u}{v} \in L \mid u, v \in K[a], v \neq 0\} \leqslant L.$$

Jest jasne, że $K(a)$ jest ciałem ułamków $K[a]$ i najmniejszym podciałem L zawierającym $K \cup \{a\}$ – nazywamy je ciałem generowanym przez a nad K.

13.18. Lemat. *Niech $K \subseteq L$ będzie rozszerzeniem i niech $a \in L$.*
1. *Jeżeli a jest elementem przestępnym nad K, to $K[a] \cong K[X]$ oraz $K(a) \cong K(X)$.*
2. *Jeżeli a jest elementem algebraicznym nad K, to $|K[a] : K| \leq \deg f$, gdzie f jest dowolnym niezerowym wielomianem dla którego $f(a) = 0$.*

Dowód. Niech $\Theta : K[X] \to K[a]$ będzie zadane wzorem $\Theta(f) = f(a)$. Jest jasne, że

$$K[X]/\ker\Theta \cong K[a].$$

Jeżeli a jest elementem przestępnym, to $\ker\Theta = 0$, i $K[X] \cong K[a]$, co dowodzi punktu 1.
Jeżeli a jest elementem algebraicznym i $f(a) = 0$, to $(f) \leqslant \ker\Theta$ i mamy epimorfizm $\pi : K[X]/(f) \twoheadrightarrow K[X]/\ker\Theta \cong K[a]$ przestrzeni liniowych nad K. Zatem zbiór $\{1, a, \ldots, a^{n-1}\}$, $n = \deg f$, generuje przestrzeń $K[a]$ nad K gdyż jest obrazem bazy $1 + (f), X + (f), \ldots, X^{n-1} + (f)$ przestrzeni liniowej $K[X]/(f)$ nad K przy epimorfizmie π. □

13.19. Stwierdzenie. *Niech $K \subseteq L$ będzie rozszerzeniem i niech $a \in L$. Następujące warunki są równoważne:*
1. *a jest elementem algebraicznym;*
2. *$|K[a] : K| < \infty$;*
3. *$K[a] = K(a)$.*

Dowód. Implikacja 1. $\implies$ 2. wynika z poprzedniego stwierdzenia.
2. $\implies$ 3. Pierścień $K[a]$ jako podpierścień ciała jest oczywiście dziedziną całkowitości więc ze Stwierdzenia 13.10 wynika, że $K[a]$ jest ciałem, a zatem jest równy swojemu ciału ułamków $K(a)$.
3. $\implies$ 1. Gdyby a było elementem przestępnym, to ze Stwierdzenia 13.18 zachodziłoby $K[a] \cong K[X]$, ale $K[X]$ nie jest ciałem, więc $K[a]$ byłoby różne od swojego ciała ułamków. □

13.20. Definicja. *Niech $K \subseteq L$ będzie rozszerzeniem i niech $a \in L$ będzie elementem algebraicznym nad K. Stpień rozszerzenia $|K(a) : K|$ nazywamy* **stopniem elementu** *a nad K.*

Przyjrzymy się teraz czemu jest równy stopień elementu algebraicznego.

13.21. Stwierdzenie. *Niech $K \subseteq L$ będzie rozszerzeniem i niech $a \in L$ będzie elementem algebraicznym nad K. Następujące liczby naturalne są równe:*
1. *stopień elementu a nad K;*
2. *stopień nierozkładalnego wielomianu $f \in K[X]$ dla którego $f(a) = 0$;*
3. *najmniejszy stopień takiego niezerowego wielomianu $f \in K[X]$, że $f(a) = 0$.*

Dowód. Jak wiemy $K[a] \cong K[X]/\ker\Theta$, gdzie $\Theta : K[X] \to K[a]$ jest epimorfizmem zadanym wzorem $\Theta(f) = f(a)$. Z poprzedniego stwierdzenia, jeżeli a jest elementem algebraicznym to $K(a) = K[a]$ i stopień elementu a jest równy $|K[a] : K|$. Pierścień $K[X]$ jest dziedziną euklidesową z waluacją będącą stopniem wielomianu. Niech $(f) = \ker\Theta \lhd K[X]$. Wielomian f jest wyznaczony jednoznacznie z dokładnością do stowarzyszenia i jest on wielomianem minimalnego stopnia spośród należących do $\ker\Theta$. Ponieważ $K[X]/\ker\Theta \cong K[a] = K(a)$ jest ciałem, to (f) jest maksymalny. Zatem f jest elementem pierwszym, a więc nierozkładalnym, Jest to jedyny z dokładnością do stowarzyszenia wielomian nierozkładalny w ideale (f), gdyż każdy inny jest postaci $f \cdot g$ dla pewego $g \in K[X]$. Z wniosku 13.14 wynika, że $|K[X]/(f) : K| = \deg f$.

□

13.22. Definicja. *Niech $K \subseteq L$ będzie rozszerzeniem i niech $a \in L$ będzie elementem algebraicznym nad K. Nierozkładalny w $K[X]$ wielomian f, taki że $f(a) = 0$ nazywamy* **wielomianem minimalnym elementu** *a.*

13.23. Definicja. *Mówimy, że rozszerzenie $K \subseteq L$ jest algebraiczne jeżeli każdy element ciała L jest algebraiczny nad K.*

Ze Stwierdzenia 13.19 wynika następujący

13.24. Wniosek. *Rozszerzenie skończonego stopnia jest algebraiczne.*

Stwierdzenie odwrotne nie jest prawdziwe.

13.25. Stwierdzenie. *Niech $K \subseteq L$ będzie rozszerzeniem. Wówczas zbiór A wszystkich elementów L algebraicznych nad K jest podciałem L.*

Dowód. Niech $a, b \in A$. Rozpatrzmy rozszerzenie $K \subseteq K(a)$ – jest ono skończone. Jeżeli $b \in L$ jest algebraiczne nad K, to jest algebraiczne nad $K(a)$, więc rozszerzenie $K(a) \subseteq K(a)(b) = K(a, b)$ też jest skończone. Mamy ciąg rozszerzeń:

$$K \subseteq K(a) \subseteq K(a, b).$$

Wynika z tego, że rozszerzenie $K \subseteq K(a, b)$ jest skończone a więc algebraiczne. Zatem elementy $a + b$, $a - b$, $a - b$, a^{-1} jako należące do $K(a, b)$ są algebraiczne.

□

13.26. Przykład. Rozważmy rozszerzenie $\mathbb{Q} \subseteq \mathbb{C}$ i niech A oznacza liczby $\mathbb{C}$ algebraiczne nad $\mathbb{Q}$ – nazywamy je liczbami algebraicznymi. Rozszerzenie algebraiczne $\mathbb{Q} \subseteq A$ jest nieskończonego stopnia. Niech $p \in \mathbb{N}$ będzie liczbą pierwszą. Wielomian $X^n - p$ jest nierozkładalny w $\mathbb{Q}[X]$ z kryterium Eisensteina i jest wielomianem minimalnym dla $\sqrt[n]{p} \in A$. Zatem $|A : \mathbb{Q}| \geq n$ dla każdego $n \in \mathbb{N}$ i $|A : \mathbb{Q}| = \infty$.

Na koniec przyjrzyjmy się ponownie rozszerzeniu $K \subseteq K[X]/(f) = L$, gdzie $f \in K[X]$ jest wielomianem nierozkładalnym. Niech $a = X + (f)$. Wielomian f jako wielomian $L[X]$ jest już rozkładalny, bo a jest jego pierwiastkiem. Tak więc możemy uważać, że L powstało z K przez dodanie pierwiastka a.

13.27. Definicja. *Ciało K nazywa się* **algebraicznie domknięte** *jeżeli każdy wielomian dodatniego stopnia ma w ciele K co najmniej jeden pierwiastek.*

Nietrudno zauważyć,że ciało K jest algebraicznie domknięte jeżeli każdy wielomian o współczynnikach z K dodatniego stopnia jest iloczynem wielomianów stopnia 1. Podstawowe twierdzenie algebry mówi, że ciało liczb zespolonych $\mathbb{C}$ jest algebraicznie domknięte.

Możemy mając dane ciało K próbować skonstruować ciało algebraicznie domknięte dołączając kolejno pierwiastki wielomianów.

13.28. Definicja. *Rozszerzenie $K \subseteq L$ nazywamy algebraicznym domknięciem ciała K wtedy i tylko wtedy, gdy rozszerzenie to jest algebraiczne i L jest ciałem algebraicznie domkniętym.*

13.29. Przykłady.1. $\mathbb{Q} \subseteq A$ jest algebraicznym domknięciem ciała liczb wymiernych.

2. $\mathbb{R} \subseteq \mathbb{C}$ jest algebraicznym domknięciem ciała liczb rzeczywistych.

13.30. Twierdzenie. *Dla każdego ciała K istnieje algebraiczne domknięcie $K \subseteq L$ i jest ono wyznaczone jednoznacznie z dokładnością do izomorfizmu.*

KONIEC