Wykład 14
Ciała i ich własności

1 Charakterystyka ciała

Określenie ciała i własności działań w ciele były omówione na algebrze liniowej. Stosując terminologię z teorii pierścieni możemy powiedzieć, że **ciało jest to niezerowy pierścień, w którym każdy element niezerowy jest odwracalny**.

Niech $(K, +, \cdot, 0, 1)$ będzie ciałem. Jeżeli istnieje liczba naturalna n taka, że $n \cdot 1 = 0$ w ciele K, to najmniejszą taką liczbę naturalną n nazywamy *charakterystyką ciała* K. Jeżeli takiej liczby naturalnej nie ma, to mówimy, że ciało K ma charakterystykę 0. Charakterystykę ciała K oznaczamy przez $ch(K)$. Wobec tego, jeśli w grupie addytywnej K^+ ciała K, $o(1) = \infty$, to $ch(K) = 0$, a jeżeli $o(1) \in \mathbb{N}$, to $ch(K) = o(1)$.

Twierdzenie 14.1. *Jeżeli $n \in \mathbb{N}$ jest charakterystyką ciała K, to n jest liczbą pierwszą. W szczególności charakterystyka ciała skończonego też jest liczbą pierwszą.*

Dowód. Załóżmy, że n nie jest liczbą pierwszą. Ponieważ $0 \neq 1$ w K oraz $1 \cdot 1 = 1$, więc $n > 1$ i istnieją $k, l \in \mathbb{N}$ takie, że $1 < k, l < n$ oraz $n = k \cdot l$. Wtedy $0 = n \cdot 1 = (k \cdot l) \cdot 1 = (k \cdot 1) \cdot (l \cdot 1)$. Zatem z Wniosku 9.29, $k \cdot 1 = 0$ lub $l \cdot 1 = 0$. Ale $k, l < n$, więc mamy sprzeczność z minimalnością n. Wobec tego n jest liczbą pierwszą.

Jeśli K jest ciałem skończonym, to grupa K^+ jest skończona, więc $ch(K) = o(1) \in \mathbb{N}$ i na mocy pierwszej części dowodu, $ch(K)$ jest liczbą pierwszą. □

Przykład 14.2. Dla dowolnej liczby pierwszej p ciało $\mathbb{Z}_p$ ma charakterystykę p, bo $o(1) = p$ w grupie $\mathbb{Z}_p^+$. Natomiast ciało $\mathbb{Q}$ ma charakterystykę 0, bo dla $n \in \mathbb{N}$ jest $n \cdot 1 = n \neq 0$.

Twierdzenie 14.3. *Niech K będzie ciałem dodatniej charakterystyki p. Wówczas dla dowolnych $a, b \in K$ i dla dowolnego $n \in \mathbb{N}$:*

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}.$$

Dowód. Zastosujemy indukcję względem n. Dla $n = 1$ ze wzoru Newtona mamy

$$(a + b)^p = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} \cdot a^k \cdot b^{p-k}.$$

Ale z elementarnej teorii liczb $p \mid \binom{p}{k}$ dla $k = 1, \ldots, p-1$, więc $\binom{p}{k} = p \cdot l_k, \quad l_k \in \mathbb{N}$. Zatem $\binom{p}{k} \cdot 1 = (p \cdot l_k) \cdot 1 = l_k \cdot (p \cdot 1) = l_k \cdot 0 = 0$. Wobec tego $(a + b)^p = a^p + b^p$.

Załóżmy, że dla dowolnych $x, y \in K$ i dla pewnego $n \in \mathbb{N}$ jest $(x + y)^{p^n} = x^{p^n} + y^{p^n}$. Weźmy dowolne $a, b \in K$. Podstawiając $x = a^p$ i $y = b^p$ uzyskamy, że $(a^p + b^p)^{p^n} =$

$(a^p)^{p^n} + (b^p)^{p^n} = a^{p^{n+1}} + b^{p^{n+1}}$. Ale $a^p + b^p = (a+b)^p$, więc $(a^p + b^p)^{p^n} = [(a+b)^p]^{p^n} = (a+b)^{p^{n+1}}$ i ostatecznie $(a+b)^{p^{n+1}} = a^{p^{n+1}} + b^{p^{n+1}}$. □

Twierdzenie 14.4. *Każda skończona podgrupa grupy multiplikatywnej ciała K jest grupą cykliczną. W szczególności grupa multiplikatywna ciała skończonego jest cykliczna.*

Dowód. Niech A będzie skończoną podgrupą rzędu n w grupie K^* ciała K. Wtedy istnieje $a \in A$ takie, że $o(a) = s$ jest maksymalne w zbiorze $\{o(x) : x \in A\}$. Ponieważ z twierdzenia Lagrange'a $a^n = 1$, więc $s \leq n$. Ponadto z Lematu 3.20, $o(b)|s$ dla każdego $b \in A$. Zatem $b^s = 1$ dla $b \in A$. Stąd wielomian $f = x^s - 1 \in K[x]$ ma w ciele K co najmniej n pierwiastków. Zatem z Wniosku 12.10, $s \geq n$. Ale $s \leq n$, więc $n = s$. Ponadto $|\langle a \rangle| = o(a) = |A|$, więc $A = \langle a \rangle$, co kończy dowód. □

2 Podciała i ciała proste

Definicja 14.5. Niech $(K, +, \cdot, 0, 1)$ będzie ciałem i niech $L \subseteq K$. Powiemy, że L *jest podciałem ciała* K, jeżeli L tworzy ciało ze względu na wszystkie działania określone w K, tzn. gdy $0, 1 \in L$ oraz dla dowolnych $a, b \in L$ mamy, że $-a \in L,\ a + b \in L,\ a \cdot b \in L$ i $\frac{1}{a} \in L$ dla $a \neq 0$. Mówimy też, że wówczas K jest *rozszerzeniem ciała* L.

Stwierdzenie 14.6. *Zbiór $L \subseteq K$ jest podciałem ciała K wtedy i tylko wtedy, gdy $1 \in L$ oraz dla dowolnych $a, b \in L$ jest $a - b \in L$ i dla dowolnych $a, b \in L$ takich, że $b \neq 0$ jest $\frac{a}{b} \in L$.*

Dowód. $\Rightarrow$. Załóżmy, że L jest podciałem ciała K. Wtedy $1 \in L$. Niech $a, b \in L$. Wtedy $-b \in L$, stąd $a - b = a + (-b) \in L$. Niech $a, b \in L,\ b \neq 0$. Wtedy $\frac{1}{b} \in L$, więc $\frac{a}{b} = a \cdot \frac{1}{b} \in L$.

$\Leftarrow$. Na odwrót, $1 \in L$, więc $0 = 1 - 1 \in L$. Niech $a, b \in L$. Wtedy $-b = 0 - b \in L$ oraz $a + b = a - (-b) \in L$. Ponadto dla $b = 0$ jest $a \cdot b = 0 \in L$, a dla $b \neq 0$, $\frac{1}{b} \in L$, bo $1 \in L$, więc $\frac{a}{\frac{1}{b}} = a \cdot b \in L$. Zatem na mocy Stwierdzenia 9.2, L jest podpierścieniem ciała K, czyli L jest pierścieniem. Ale $0 \neq 1$ w L oraz każdy niezerowy element z L jest odwracalny w L, więc L jest ciałem, czyli L jest podciałem ciała K. □

Uwaga 14.7. Niech L będzie podciałem ciała K. Z określenia charakterystyki ciała wynika od razu, że $ch(L) = ch(K)$. Ponadto, jeśli M jest podciałem ciała L, to na mocy Stwierdzenia 14.6, M jest podciałem ciała K.

Stwierdzenie 14.8. *Część wspólna dowolnej niepustej rodziny podciał ciała K jest podciałem ciała K.*

Dowód. Niech $\{K_t\}_{t \in T}$ będzie niepustą rodziną podciał ciała K. Wtedy $1 \in K_t$ dla każdego $t \in T$. Zatem $1 \in \bigcap_{t \in T} K_t$. Weźmy dowolne $a, b \in \bigcap_{t \in T} K_t$. Wtedy $a, b \in K_t$ dla każdego $t \in T$, więc ze Swierdzenia 14.6, $a - b \in K_t$ dla każdego $t \in T$, skąd

$a - b \in \bigcap_{t\in T} K_t$. Jeśli dodatkowo $b \neq 0$, to ze Stwierdzenia 14.6, $\frac{a}{b} \in K_t$ dla każdego $t \in T$. Zatem $\frac{a}{b} \in \bigcap_{t\in T} K_t$. Wobec tego na mocy Stwierdzenia 14.6, $\bigcap_{t\in T} K_t$ jest podciałem ciała K. $\square$

Uwaga 14.9. Niech ciało K będzie rozszerzeniem ciała L. Wówczas K jest przestrzenią liniową nad ciałem L, gdy dla $\alpha \in K,\ a \in L$ określimy

$$a \circ \alpha = a \cdot \alpha,$$

gdzie $\cdot$ oznacza mnożenie w ciele K. Moc dowolnej bazy K nad L oznaczamy przez $(K : L)$ i nazywamy *stopniem rozszerzenia* $L \subseteq K$. Jeżeli $(K : L)$ jest liczbą naturalną, to mówimy, że K jest *skończonym rozszerzeniem ciała* L.

Przykład 14.10. Zauważmy, że $(\mathbb{C} : \mathbb{R}) = 2$, bo $\{1,\ i\}$ jest bazą $\mathbb{C}$ nad ciałem $\mathbb{R}$. Natomiast $(\mathbb{R} : \mathbb{Q}) = |\mathbb{R}| \notin \mathbb{N}$, bo zbiór $\mathbb{R}$ jest nieprzeliczalny, a zbiór $\mathbb{Q}$ jest przeliczalny.

Definicja 14.11. Jeżeli ciało K nie posiada podciał różnych od K, to mówimy, że K jest *ciałem prostym*.

Przykład 14.12. Zauważmy, że $\mathbb{Q}$ jest ciałem prostym. Rzeczywiście, niech $K \subseteq \mathbb{Q}$ będzie podciałem ciała $\mathbb{Q}$. Wówczas K jest podpierścieniem w $\mathbb{Q}$, więc na mocy Stwierdzenia 9.3, $\mathbb{Z} \subseteq K$. Weźmy dowolne $q \in \mathbb{Q}$. Wówczas istnieją $n \in \mathbb{Z}$ i $k \in \mathbb{N}$ takie, że $q = \frac{n}{k}$. Ale $n, k \in K$ i $k \neq 0$, więc $q \in K$. Stąd $\mathbb{Q} \subseteq K$, czyli $K = \mathbb{Q}$.

Przykład 14.13. Dla dowolnej liczby pierwszej p, $\mathbb{Z}_p$ jest ciałem prostym. Rzeczywiście, niech $K \subseteq \mathbb{Z}_p$ będzie podciałem ciała $\mathbb{Z}_p$. Wówczas $1 \in K$, stąd $\langle 1\rangle \subseteq K$. Ale $\langle 1\rangle = \mathbb{Z}_p$, więc $K = \mathbb{Z}_p$.

Uwaga 14.14. Niech K i L będą ciałami i niech $f\colon K \to L$ będzie homomorfizmem pierścieni. Wówczas $f(1) = 1 \neq 0$, skąd $1 \notin Ker(f)$. Ale $Ker(f) \lhd K$ i K jest ciałem, więc na mocy Stwierdzenia 10.4, $Ker(f) = \{0\}$. Wobec tego na mocy Stwierdzenia 10.27, f jest różnowartościowe. Zatem każdy homomorfizm pierścieni z ciała K w ciało L jest zanurzeniem. Zauważmy jeszcze, że dla $b \in K \setminus \{0\}$ istnieje $b^{-1} \in K$, więc $1 = f(1) = f(b \cdot b^{-1}) = f(b) \cdot f(b^{-1})$, a zatem $[f(b)]^{-1} = f(b^{-1})$. Wobec tego dla $a \in K$ i $b \in K \setminus \{0\}$ mamy, że $f(\frac{a}{b}) = f(a \cdot b^{-1}) = f(a) \cdot f(b^{-1}) = f(a) \cdot [f(b)]^{-1} = \frac{f(a)}{f(b)}$. Stąd i ze stwierdzeń 10.27 i 14.6 uzyskujemy, że $f(K)$ jest podciałem ciała L.

Jeśli dodatkowo homomorfizm pierścieni f jest "na", to mówimy, że f jest *izomorfizmem ciał*. Mówimy, że ciała K i L są *izomorficzne* i piszemy $K \cong L$, jeśli istnieje izomorfizm ciał $f\colon K \to L$. W algebrze utożsamiamy ciała izomorficzne.

Twierdzenie 14.15. *Każde ciało K posiada dokładnie jedno podciało proste F. Jeśli $ch(K) = 0$, to $F \cong \mathbb{Q}$ i $F = \{\frac{k\cdot 1}{n\cdot 1} \ :\ k, n \in \mathbb{Z},\ n > 0\}$, a jeśli $ch(K) = p > 0$, to*

$F \cong \mathbb{Z}_p$ *i* $F = \{k \cdot 1 \ : \ k = 0, 1, \ldots, p-1\}$. *W szczególności, jedynymi ciałami prostymi z dokładnością do izomorfizmu są:* $\mathbb{Q}$ *i* $\mathbb{Z}_p$ *dla* p *będących liczbami pierwszymi.*

Dowód. Rodzina $\mathcal{K}$ wszystkich podciał ciała K jest niepusta, bo $K \in \mathcal{K}$. Zatem na mocy Stwierdzenia 14.8, $\bigcap_{M \in \mathcal{K}} M$ jest podciałem ciała K zawartym w każdym podciele ciała K. Wobec tego $\bigcap_{M \in \mathcal{K}} M$ jest najmniejszym podciałem ciała K, a zatem na mocy Uwagi 14.7, $\bigcap_{M \in \mathcal{K}} M$ jest ciałem prostym. Jeśli F jest podciałem prostym ciała K, to $\bigcap_{M \in \mathcal{K}} M \subseteq F$, skąd $F = \bigcap_{M \in \mathcal{K}} M$. Wobec tego ciało K posiada dokładnie jedno podciało proste F, które jednocześnie jest najmniejszym podciałem ciała K.

Załóżmy, że $ch(K) = 0$. Bezpośrednie sprawdzenie pokazuje, że funkcja $f\colon \mathbb{Q} \to K$ dana wzorem $f(\frac{k}{n}) = \frac{k \cdot 1}{n \cdot 1}$ dla $k \in \mathbb{Z}$, $n \in \mathbb{N}$, jest dobrze określona i jest homomorfizmem pierścieni. Wobec tego na mocy Uwagi 14.14, $f(\mathbb{Q})$ jest podciałem ciała K izomorficznym z ciałem $\mathbb{Q}$. Ponadto $f(\mathbb{Q}) = \{\frac{k \cdot 1}{n \cdot 1} \ : \ k, n \in \mathbb{Z}, \ n > 0\}$. Jeśli M jest dowolnym podciałem ciała K, to na mocy Stwierdzenia 9.3, $l \cdot 1 \in M$ dla każdego $l \in \mathbb{Z}$. Stąd $f(\mathbb{Q}) \subseteq M$, a więc $f(\mathbb{Q}) = F$.

Niech teraz $ch(K) = p$, gdzie p jest liczbą pierwszą. Ponieważ $o(1) = p$ w $\mathbb{Z}_p^+$ i $o(1) = p$ w grupie K^+, więc funkcja $g\colon \mathbb{Z}_p \to K$ dana wzorem $g(k \cdot 1) = k \cdot 1$ dla $k \in \mathbb{Z}$, jest dobrze określona. Bezpośrednie sprawdzenie pokazuje, że g jest homomorfizmem pierścieni. Wobec tego na mocy Uwagi 14.14, $g(\mathbb{Z}_p)$ jest podciałem ciała K izomorficznym z ciałem $\mathbb{Z}_p$. Ponadto $g(\mathbb{Z}_p) = \{k \cdot 1 \ : \ k = 0, 1, \ldots, p-1\}$. Jeśli M jest dowolnym podciałem ciała K, to na mocy Stwierdzenia 9.3, $l \cdot 1 \in M$ dla każdego $l \in \mathbb{Z}$. Stąd $g(\mathbb{Z}_p) \subseteq M$, a więc $g(\mathbb{Q}) = F$. $\square$

Twierdzenie 14.16. *Niech* K *będzie ciałem skończonym. Wówczas* $|K| = p^n$ *i* $ch(K) = p$ *dla pewnej liczby pierwszej* p *oraz dla pewnej liczby naturalnej* n. *Wszystimi różnymi podciałami ciała* K *są* $L_m = \{a \in K \ : \ a^{p^m} = a\}$, *gdzie* $m \in \mathbb{N}$ *i* $m|n$. *W szczególności liczba wszystkich podciał ciała* p^n*-elementowego jest równa liczbie wszystkich dzielników liczby* n.

Dowód. Z Twierdzenia 14.1, $ch(K) = p$ dla pewnej liczby pierwszej p. Niech L będzie podciałem ciała K. Wtedy K jest przestrzenią liniową nad ciałem L. Ale K jest skończone, więc istnieje skończona baza $\{\alpha_1, \ldots, \alpha_s\}$, K nad L. Każdy element należący do K może być zapisany jednoznacznie w postaci kombinacji liniowej elementów tej bazy. Zatem $|K| = |L^s| = |L|^s$.

Z Twierdzenia 14.15 istnieje podciało F ciała K takie, że $|F| = p$. Stąd $|K| = p^n$ dla pewnego $n \in \mathbb{N}$. Jeżeli L jest dowolnym podciałem ciała K, to $F \subseteq L$, więc na mocy pierwszej części dowodu, $|L| = p^m$ dla pewnego $m \in \mathbb{N}$. Ale $p^n = |K| = |L|^s = p^{ms}$ dla pewnego $s \in \mathbb{N}$, więc $n = ms$ i $m \mid n$. Ponadto grupa L^* ma rząd równy $p^m - 1$, więc na moc twierdzenia Lagrange'a, $a^{p^m - 1} = 1$ dla każdego $a \in L \setminus \{0\}$. Stąd $a^{p^m} = a$ dla każdego $a \in L$. Zatem $L \subseteq L_m$. Ale z Wniosku 12.10, $|L_m| \leq p^m$, więc $L = L_m$.

Niech teraz $m \in \mathbb{N}$ i $m|n$. Ponieważ $1^{p^m} = 1$, więc $1 \in L_m$. Weźmy dowolne $a, b \in L_m$. Wtedy $a^{p^m} = a$ i $b^{p^m} = b$ oraz $(-1)^{p^m} = -1$. Zatem z Twierdzenia 14.3, $(a-b)^{p^m} =$

$a^{p^m}+(-1)^{p^m}\cdot b^{p^m}=a-b$, więc $a-b\in L_m$. Ponadto, gdy $b\neq 0$, to $(\frac{a}{b})^{p^m}=\frac{a^{p^m}}{b^{p^m}}=\frac{a}{b}$, więc $\frac{a}{b}\in L_m$. Zatem ze Stwierdzenia 14.6, L_m jest podciałem ciała K. Dalej, z Twierdzenia 14.4 istnieje $c\in K^*$ takie, że $o(c)=p^n-1$ w grupie K^*. Ale $m|n$, więc, $p^m-1|p^n-1$. Wobec tego w grupie cyklicznej K^* element $u=c^{\frac{p^n-1}{p^m-1}}$ ma rząd p^m-1. Zatem elementy $1,u,u^2,\ldots,u^{p^m-2}$ są parami różne i jest ich dokładnie p^m-1. Ponadto $u^{p^m-1}=1$, więc $u^{p^m}=u$, skąd $u\in L_m$. Zatem $\{0,1,u,\ldots,u^{p^m-2}\}$ jest p^m-elementowym podzbiorem podciała L_m, skąd $|L_m|\geq p^m$. Ale każdy element z L jest pierwiastkiem wielomianu $x^{p^m}-x\in K[x]$, więc na mocy Wniosku 12.10, $p^m\geq|L_m|$. Wobec tego $|L_m|=p^m$ i $L_m=\{0,1,u,\ldots,u^{p^m-2}\}$. Zatem L_m jest podciałem p^m-elementowym ciała K. $\square$

Uwaga 14.17. Pokażemy jak można skonstruować ciało p^n -elementowe dla liczb pierwszych p oraz $n\in\mathbb{N}$. Najpierw znajdujemy w pierścieniu $\mathbb{Z}_p[x]$ wielomian unormowany f stopnia n, który jest nierozkładalny w tym pierścieniu. Niech $I=(f)$. Wtedy z Wniosku 13.16 pierścień ilorazowy $\mathbb{Z}_p[x]/I$ jest ciałem. Ponadto z Twierdzenia 12.13 każdy element pierścienia $\mathbb{Z}_p[x]/I$ można zapisać jednoznacznie w postaci $a_0+a_1x+\ldots+a_{n-1}x^{n-1}+I$ dla pewnych $a_0,a_1,\ldots,a_{n-1}\in\mathbb{Z}_p$. Ale $|\mathbb{Z}_p|=p$, więc $|\mathbb{Z}_p[x]/I|=p^n$, czyli $\mathbb{Z}_p[x]/I$ jest ciałem p^n-elementowym.

Jeśli $n=2$ lub $n=3$, to ze Stwierdzenia 12.32 wystarczy aby f nie miał pierwiastka w ciele $\mathbb{Z}_p$. Stąd dla $p=2$ i $n=2$ wystarczy wziąć $f=x^2+x+1$ i otrzymujemy ciało 4-elementowe $\mathbb{Z}_2[x]/(x^2+x+1)$.

Jeśli $n=2$ i $p>2$, to $C=\{c^2:c\in\mathbb{Z}_p\}=\{0^2,1^2,\ldots,(\frac{p-1}{2})^2\}$ jest zbiorem $1+\frac{p-1}{2}=\frac{p+1}{2}$-elementowym. Ale $p>2$, więc $\frac{p+1}{2}<p$ i istnieje $a\in\mathbb{Z}_p\setminus C$. Wtedy wielomian $f=x^2-a$ nie ma pierwiastka w $\mathbb{Z}_p$, więc $\mathbb{Z}_p[x]/(x^2-a)$ jest ciałem p^2-elementowym.

Jeśli $n=3$, to mamy dokładnie $p^2(p-1)$ wielomianów postaci $f=x^3+ax^2+bx+c\in\mathbb{Z}_p[x]$ takich, że $c\neq 0$. Natomiast rozkładalne wielomiany unormowane stopnia 3 z niezerowym wyrazem wolnym na mocy Twierdzenia 13.5 są postaci $(x+k)(x^2+lx+t)$ dla pewnych $k,l,t\in\mathbb{Z}_p$, $k,t\neq 0$. Zatem takich wielomianów jest co najwyżej $p(p-1)^2$. Ale $p(p-1)^2<p^2(p-1)$, więc istnieje f, które nie ma pierwiastka w $\mathbb{Z}_p$ i wobec tego $\mathbb{Z}_p[x]/(f)$ jest ciałem p^3-elementowym.

Można udowodnić, że dla każdej liczby pierwszej p i dla każdego $n\in\mathbb{N}$ istnieje wielomian nierozkładalny $f\in\mathbb{Z}_p[x]$ stopnia n, a więc wtedy $\mathbb{Z}_p[x]/(f)$ jest ciałem p^n-elementowym.

3 Ciało ułamków

Każdy podpierścień ciała jest dziedziną całkowitości. Okazuje się, że także każda dziedzina całkowitości jest podpierścieniem pewnego ciała.

Definicja 14.18. Powiemy, że ciało K jest *ciałem ułamków* dziedziny całkowitości P, jeżeli

(i) P jest podpierścieniem K oraz

(ii) każdy element ciała K można zapisać w postaci $\frac{a}{b}$ dla pewnych $a, b \in P$, $b \neq 0$.

Przykład 14.19. Niech P będzie dowolnym podpierścieniem ciała $\mathbb{Q}$. Wtedy ze Stwierdzenia 9.3 mamy, że $\mathbb{Z} \subseteq P$. Wobec tego każdy element z $\mathbb{Q}$ można zapisać w postaci $\frac{a}{b}$ dla pewnych $a, b \in P$, $b \neq 0$. Zatem z Definicji 14.18 mamy, że $\mathbb{Q}$ jest ciałem ułamków dla P. Wobec tego $\mathbb{Q}$ **jest ciałem ułamków każdego swego podpierścienia**.

Przedstawimy teraz konstrukcję ciała ułamków dowolnej dziedziny całkowitości P. Niech $S = P \times (P \setminus \{0\})$. W zbiorze S określamy relację $\sim$ przyjmując, że dla dowolnych $(a_1, b_1), (a_2, b_2) \in S$:

$$(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 \cdot b_2 = a_2 \cdot b_1.$$

Pokażemy, że $\sim$ jest relacją równoważności w S:

1° Jeżeli $(a, b) \in S$, to $a \cdot b = a \cdot b$, więc $(a, b) \sim (a, b)$.

2° Jeżeli $(a, b),\ (c, d) \in S$ oraz $(a, b) \sim (c, d)$, to $a \cdot d = c \cdot b$. Stąd $c \cdot b = a \cdot d$, czyli $(c, d) \sim (a, b)$.

3° Jeżeli $(a_1, b_1),\ (a_2, b_2),\ (a_3, b_3) \in S$ są takie, że $(a_1, b_1) \sim (a_2, b_2)$ oraz $(a_2, b_2) \sim (a_3, b_3)$, to $a_1 \cdot b_2 = a_2 \cdot b_1$ i $a_2 \cdot b_3 = a_3 \cdot b_2$, stąd $a_1 \cdot b_2 \cdot b_3 = a_2 \cdot b_1 \cdot b_3$ i $a_2 \cdot b_3 \cdot b_1 = a_3 \cdot b_2 \cdot b_1$, więc $a_1 \cdot b_2 \cdot b_3 = a_3 \cdot b_2 \cdot b_1$. Ale $b_2 \neq 0$ i P jest dziedziną całkowitości, więc $a_1 \cdot b_3 = a_3 \cdot b_1$, stąd $(a_1, b_1) \sim (a_3, b_3)$.

Klasę abstrakcji o reprezentancie $(a, b) \in S$ będziemy oznaczali przez $\frac{a}{b}$. Zbiór wszystkich klas abstrakcji relacji $\sim$ będziemy oznaczali przez P_0.

Zauważmy najpierw, że dla $(a, b) \in S$ i $0 \neq d \in P$ jest

$$\frac{a}{b} = \frac{a \cdot d}{b \cdot d}.$$

Rzeczywiście, $a \cdot (b \cdot d) = (a \cdot d) \cdot b$, stąd $(a, b) \sim (a \cdot d, b \cdot d)$, więc $\frac{a}{b} = \frac{a \cdot d}{b \cdot d}$.

Dla $(a, b) \in S$ mamy też, że $\frac{a}{b} = \frac{0}{1} \Leftrightarrow a = 0$. Rzeczywiście, dla $a = 0$ jest $a \cdot 1 = 0 = 0 \cdot b$, więc $(a, b) \sim (0, 1)$, stąd $\frac{a}{b} = \frac{0}{1}$. Jeżeli zaś $\frac{a}{b} = \frac{0}{1}$, to $(a, b) \sim (0, 1)$, skąd $a \cdot 1 = 0 \cdot b$, czyli $a = 0$.

Niech $1 = \frac{1}{1}$ i $0 = \frac{0}{1}$. Ponieważ $0 \neq 1$ w P, więc z naszych rozważań wynika, że $0 \neq 1$ w P_0.

Określamy teraz w P_0 dodawanie i mnożenie przy pomocy wzorów:

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 \cdot b_2 + a_2 \cdot b_1}{b_1 \cdot b_2}, \tag{1}$$

$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 \cdot a_2}{b_1 \cdot b_2}. \tag{2}$$

Sprawdzimy, że te określenia nie zależą od wyboru reprezentantów klas abstrakcji. Niech $(a_1, b_1), (x_1, y_1), (a_2, b_2), (x_2, y_2) \in S$ oraz $(a_1, b_1) \sim (x_1, y_1), (a_2, b_2) \sim (x_2, y_2)$. Wtedy $a_1 \cdot y_1 = x_1 \cdot b_1$ i $a_2 \cdot y_2 = x_2 \cdot b_2$. Musimy udowodnić, że wówczas $(a_1 \cdot b_2 + a_2 \cdot b_1, b_1 \cdot b_2) \sim (x_1 \cdot y_2 + x_2 \cdot y_1, y_1 \cdot y_2)$ i $(a_1 \cdot a_2, b_1 \cdot b_2) \sim (x_1 \cdot x_2, y_1 \cdot y_2)$, czyli że $(a_1 \cdot b_2 + a_2 \cdot b_1) \cdot y_1 y_2 = (x_1 y_2 + x_2 y_1) \cdot b_1 \cdot b_2$ i $a_1 \cdot a_2 \cdot y_1 \cdot y_2 = x_1 \cdot x_2 \cdot b_1 \cdot b_2$. Ale $a_1 \cdot a_2 \cdot y_1 \cdot y_2 = (a_1 \cdot y_1) \cdot (a_2 \cdot y_2) = x_1 \cdot b_1 \cdot x_2 \cdot b_2 = x_1 \cdot x_2 \cdot b_1 \cdot b_2$ oraz $(a_1 \cdot b_2 + a_2 \cdot b_1) \cdot y_1 y_2 = (a_1 y_1) \cdot b_2 y_2 + (a_2 y_2) \cdot b_1 y_1 = x_1 \cdot b_1 \cdot b_2 \cdot y_2 + x_2 \cdot b_2 \cdot b_1 \cdot y_1 = (x_1 \cdot y_2 + x_2 \cdot y_1) \cdot b_1 \cdot b_2$, więc wzory (1) i (2) są dobrze określone.

Teraz udowodnimy, że $(P_0, +, \cdot, 0, 1)$ jest ciałem. W tym celu sprawdzamy spełnienie aksjomatów ciała:

1. Niech $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in S$. Wtedy $(\frac{a_1}{b_1} + \frac{a_2}{b_2}) + \frac{a_3}{b_3} = \frac{a_1 \cdot b_2 + a_2 \cdot b_1}{b_1 \cdot b_2} + \frac{a_3}{b_3} = \frac{a_1 \cdot b_2 \cdot b_3 + a_2 \cdot b_1 \cdot b_3}{b_1 \cdot b_2 \cdot b_3} + \frac{a_3 \cdot b_1 \cdot b_2}{b_1 \cdot b_2 \cdot b_3} = \frac{a_1 \cdot b_2 \cdot b_3 + a_2 \cdot b_1 \cdot b_3 + a_3 \cdot b_1 \cdot b_2}{b_1 \cdot b_2 \cdot b_3}$, bo $\frac{a_1}{b} + \frac{a_2}{b} = \frac{a_1 + a_2}{b}$, gdyż $\frac{a_1}{b} + \frac{a_2}{b} = \frac{a_1 \cdot b + a_2 \cdot b}{b^2} = \frac{(a_1 + a_2) \cdot b}{b \cdot b} = \frac{a_1 + a_2}{b}$. Ponadto:
   $\frac{a_1}{b_1} + (\frac{a_2}{b_2} + \frac{a_3}{b_3}) = \frac{a_1}{b_1} + \frac{a_2 \cdot b_3 + a_3 \cdot b_2}{b_2 \cdot b_3} = \frac{a_1 \cdot b_2 \cdot b_3}{b_1 \cdot b_2 \cdot b_3} + \frac{a_2 \cdot b_3 \cdot b_1 + a_3 \cdot b_2 \cdot b_1}{b_1 \cdot b_2 \cdot b_3} = \frac{a_1 \cdot b_2 \cdot b_3 + a_2 \cdot b_3 \cdot b_1 + a_3 \cdot b_2 \cdot b_1}{b_1 \cdot b_2 \cdot b_3}$, więc dodawanie jest łączne.

2. Niech $(a_1, b_1), (a_2, b_2) \in S$. Wtedy $\frac{a_2}{b_2} + \frac{a_1}{b_1} = \frac{a_2 \cdot b_1 + a_1 \cdot b_2}{b_2 \cdot b_1} = \frac{a_1 \cdot b_2 + a_2 \cdot b_1}{b_1 \cdot b_2} = \frac{a_1}{b_1} + \frac{a_2}{b_2}$, więc dodawanie jest przemienne.

3. Niech $(a, b) \in S$. Wtedy $0 = \frac{0}{b}$ oraz $\frac{a}{b} + 0 = \frac{a}{b} + \frac{0}{b} = \frac{a+0}{b} = \frac{a}{b}$, więc 0 jest elementem neutralnym dodawania.

4. Niech $(a, b) \in S$. Wtedy $(-a, b) \in S$ oraz $\frac{a}{b} + \frac{-a}{b} = \frac{a+(-a)}{b} = \frac{0}{b} = 0$. Zatem $-(\frac{a}{b}) = \frac{(-a)}{b}$.

5. Niech $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in S$. Wtedy $(\frac{a_1}{b_1} \cdot \frac{a_2}{b_2}) \cdot \frac{a_3}{b_3} = \frac{a_1 \cdot a_2}{b_1 \cdot b_2} \cdot \frac{a_3}{b_3} = \frac{a_1 \cdot a_2 \cdot a_3}{b_1 \cdot b_2 \cdot b_3}$ i $\frac{a_1}{b_1} \cdot (\frac{a_2}{b_2} \cdot \frac{a_3}{b_3}) = \frac{a_1}{b_1} \frac{a_2 \cdot a_3}{b_2 \cdot b_3} = \frac{a_1 \cdot a_2 \cdot a_3}{b_1 \cdot b_2 \cdot b_3}$, więc mnożenie jest łączne.

6. Niech $(a_1, b_1), (a_2, b_2) \in S$. Wtedy $\frac{a_2}{b_2} \cdot \frac{a_1}{b_1} = \frac{a_2 \cdot a_1}{b_2 \cdot b_1} = \frac{a_1 \cdot a_2}{b_1 \cdot b_2} = \frac{a_1}{b_1} \cdot \frac{a_2}{b_2}$, więc mnożenie jest przemienne.

7. Niech $(a, b) \in S$. Wtedy $\frac{a}{b} \cdot 1 = \frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b}$, czyli 1 jest elementem neutralnym mnożenia.

8. Dla $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in S$: $\frac{a_1}{b_1} \cdot (\frac{a_2}{b_2} + \frac{a_3}{b_3}) = \frac{a_1}{b_1} \cdot \frac{a_2 \cdot b_3 + a_3 \cdot b_2}{b_2 \cdot b_3} = \frac{a_1 \cdot a_2 \cdot b_3 + a_1 \cdot a_3 \cdot b_2}{b_1 \cdot b_2 \cdot b_3}$ oraz $\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} + \frac{a_1}{b_1} \cdot \frac{a_3}{b_3} = \frac{a_1 \cdot a_2}{b_1 \cdot b_2} + \frac{a_1 \cdot a_3}{b_1 \cdot b_3} = \frac{a_1 \cdot a_2 \cdot b_3}{b_1 \cdot b_2 \cdot b_3} + \frac{a_1 \cdot a_3 \cdot b_2}{b_1 \cdot b_2 \cdot b_3} = \frac{a_1 \cdot a_2 \cdot b_3 + a_1 \cdot a_3 \cdot b_2}{b_1 \cdot b_2 \cdot b_3}$, więc mnożenie jest rozdzielne względem dodawania.

9. Niech $(a, b) \in S$ będzie takie, że $\frac{a}{b} \neq 0$. Wtedy, jak wiemy $a \neq 0$, więc $(b, a) \in S$ oraz $\frac{a}{b} \cdot \frac{b}{a} = \frac{a \cdot b}{b \cdot a} = \frac{1}{1} = 1$, bo $a, b \neq 0$. Stąd $(\frac{a}{b})^{-1} = \frac{b}{a}$.

Z 1–9 wynika zatem, że $(P_0, +, \cdot, 0, 1)$ jest ciałem.

Niech $f\colon P \to P_0$ będzie funkcją daną wzorem $f(a) = \frac{a}{1}$ dla $a \in P$. Wtedy dla $a, b \in P$: $f(a) = f(b) \Leftrightarrow \frac{a}{1} = \frac{b}{1} \Leftrightarrow (a, 1) \sim (b, 1) \Leftrightarrow a \cdot 1 = b \cdot 1 \Leftrightarrow a = b$. Zatem f jest różnowartościowe. Ponadto $f(1) = \frac{1}{1} = 1$ oraz dla $a, b \in P$:

$$f(a + b) = \frac{a + b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b)$$

i

$$f(a \cdot b) = \frac{a \cdot b}{1} = \frac{a \cdot b}{1 \cdot 1} = \frac{a}{1} \cdot \frac{b}{1} = f(a) \cdot f(b).$$

Zatem f jest zanurzeniem pierścieni. Stąd dla $a \in P$ można dokonać utożsamienia:

$$a \equiv \frac{a}{1}.$$

Przy tym utożsamieniu P jest podpierścieniem ciała P_0. Dla $0 \neq b \in P$ mamy, że $\frac{1}{b} = (\frac{b}{1})^{-1} = b^{-1}$, więc dla $a \in P$ jest $\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = a \cdot b^{-1}$, stąd $P_0 = \{a \cdot b^{-1} : a, b \in P, b \neq 0\}$, czyli P_0 jest ciałem ułamków dla P. Ponadto dla $(a_1, b_1), (a_2, b_2) \in S$ mamy, że $\frac{a_1}{b_1} = \frac{a_2}{b_2} \Leftrightarrow a_1 \cdot b_2 = a_2 \cdot b_1$, bo $\frac{a_1}{b_1} = \frac{a_2}{b_2} \Leftrightarrow (a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 \cdot b_2 = a_2 \cdot b_1$.

Jeżeli L jest ciałem, to ciało ułamków pierścienia $L[x]$ oznaczamy przez $L(x)$ i nazywamy *ciałem funkcji wymiernych zmiennej x nad ciałem L*. Wówczas L jest podciałem ciała $L(x)$, skąd $ch(L(x)) = ch(L)$. Ponieważ $1, x, x^2, \ldots$ są liniowo niezależne nad L i należą do $L(x)$, więc $(L(x) : L) = \infty$. Podstawiając $L = \mathbb{Z}_p$ uzyskamy stąd, że **istnieją ciała nieskończone dowolnej dodatniej charakterystyki** (np. ciała $\mathbb{Z}_p(x)$).

Zagadka 1. Skonstruuj ciało 8-elementowe.

Zagadka 2. Skonstruuj ciało 27-elementowe.

Zagadka 3. Skonstruuj ciało 125-elementowe.

Zagadka 4. Skonstruuj ciało 7^3-elementowe.

Zadanie 5. Skonstruuj ciało 16-elementowe.

Zagadka 6. Ile podciał ma ciało 2^{2010}-elementowe?

Zagadka 7. Niech d będzie liczbą całkowitą, która nie jest kwadratem liczby całkowitej. Udowodnij, że $\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} : x, y \in \mathbb{Q}\}$ jest ciałem ułamków pierścienia liczbowego $\mathbb{Z}[\sqrt{d}]$.