Kiedy pierścień skończony jest ciałem?

Marcin Ból

Politechnika Krakowska
ul. Warszawska 24, Kraków

28 listopada 2021

Ładne twierdzenia

Definicja

Dziedziną całkowitości nazywamy niezerowy pierścień przemienny z jedynką bez dzielników zera.

Ładne twierdzenia

Definicja

Dziedziną całkowitości nazywamy niezerowy pierścień przemienny z jedynką bez dzielników zera.

Definicja

Pierścieniem z dzieleniem nazywamy niezerowy pierścień z jedynką, w którym każdy niezerowy element jest odwracalny.

Ładne twierdzenia

Definicja

Dziedziną całkowitości nazywamy niezerowy pierścień przemienny z jedynką bez dzielników zera.

Definicja

Pierścieniem z dzieleniem nazywamy niezerowy pierścień z jedynką, w którym każdy niezerowy element jest odwracalny.

Twierdzenie

Każda skończona dziedzina całkowitości jest ciałem.

Ładne twierdzenia

Definicja

Dziedziną całkowitości nazywamy niezerowy pierścień przemienny z jedynką bez dzielników zera.

Definicja

Pierścieniem z dzieleniem nazywamy niezerowy pierścień z jedynką, w którym każdy niezerowy element jest odwracalny.

Twierdzenie

Każda skończona dziedzina całkowitości jest ciałem.

Małe twierdzenie Wedderburna

Każdy skończony pierścień z dzieleniem jest ciałem.

Ładne twierdzenia

Definicja

Dziedziną całkowitości nazywamy niezerowy pierścień przemienny z jedynką bez dzielników zera.

Definicja

Pierścieniem z dzieleniem nazywamy niezerowy pierścień z jedynką, w którym każdy niezerowy element jest odwracalny.

Twierdzenie

Każda skończona dziedzina całkowitości jest ciałem.

Małe twierdzenie Wedderburna

Każdy skończony pierścień z dzieleniem jest ciałem.

Pierwsze z powyższych twierdzeń ma krótki i prosty, a drugie dosyć skomplikowany dowód.

Szybki dowód

Twierdzenie

Każda skończona dziedzina całkowitości jest ciałem.

Szybki dowód

Twierdzenie

Każda skończona dziedzina całkowitości jest ciałem.

Dowód

Niech A będzie skończoną dziedziną całkowitości oraz niech $0 \neq x \in A$. Jedyną rzeczą, którą należy wykazać jest istnienie elementu odwrotnego do x.

Szybki dowód

Twierdzenie

Każda skończona dziedzina całkowitości jest ciałem.

Dowód

Niech A będzie skończoną dziedziną całkowitości oraz niech $0 \neq x \in A$. Jedyną rzeczą, którą należy wykazać jest istnienie elementu odwrotnego do x. Rozważmy ciąg $x, x^2, x^3, \ldots$ Ponieważ dziedzina A jest skończona, to $x^m = x^n$ dla pewnych $m, n \in \mathbb{N}$, $m < n$.

Szybki dowód

Twierdzenie

Każda skończona dziedzina całkowitości jest ciałem.

Dowód

Niech A będzie skończoną dziedziną całkowitości oraz niech $0 \neq x \in A$. Jedyną rzeczą, którą należy wykazać jest istnienie elementu odwrotnego do x. Rozważmy ciąg $x, x^2, x^3, \ldots$ Ponieważ dziedzina A jest skończona, to $x^m = x^n$ dla pewnych $m, n \in \mathbb{N}$, $m < n$. Wtedy

$$0 = x^m - x^n = x^m(1 - x^{n-m}).$$

Szybki dowód

Twierdzenie

Każda skończona dziedzina całkowitości jest ciałem.

Dowód

Niech A będzie skończoną dziedziną całkowitości oraz niech $0 \neq x \in A$. Jedyną rzeczą, którą należy wykazać jest istnienie elementu odwrotnego do x. Rozważmy ciąg $x, x^2, x^3, \ldots$ Ponieważ dziedzina A jest skończona, to $x^m = x^n$ dla pewnych $m, n \in \mathbb{N}$, $m < n$. Wtedy

$$0 = x^m - x^n = x^m(1 - x^{n-m}).$$

Z braku dzielników zera mamy, że $x^m \neq 0$, a zatem $x^{n-m} = 1$, czyli $xx^{n-m-1} = 1$, a stąd wynika, że $x^{n-m-1} = x^{-1}$. $\square$

Piękne uogólnienie

Oba wcześniej wspomniane twierdzenia są szczególnymi przypadkami twierdzenie ogólniejszego, udowodnionego przez irlandzkiego matematyka Desmonda MacHale'a.

Twierdzenie 1

Niech R będzie niezerowym pierścieniem skończonym takim, że dla dowolnych $a, b \in R$

$$ab = 0 \implies a = 0 \vee b = 0.$$

Wtedy R jest ciałem.

Piękne uogólnienie

Oba wcześniej wspomniane twierdzenia są szczególnymi przypadkami twierdzenie ogólniejszego, udowodnionego przez irlandzkiego matematyka Desmonda MacHale'a.

Twierdzenie 1

Niech R będzie niezerowym pierścieniem skończonym takim, że dla dowolnych $a, b \in R$

$$ab = 0 \implies a = 0 \vee b = 0.$$

Wtedy R jest ciałem.

Zauważmy, że powyższe twierdzenie nie zakłada ani przemienności pierścienia R, ani istnienia jedynki w tym pierścieniu.

Dowód

Ponieważ $R \neq \{0\}$ możemy ustalić niezerowy element $a \in R$. Niech $R = \{r_1, \ldots, r_n\}$. Definiujemy funkcję $\alpha : R \to R$ wzorem

$$\alpha(r_i) = r_i a$$

dla każdego i.

Dowód

Ponieważ $R \neq \{0\}$ możemy ustalić niezerowy element $a \in R$. Niech $R = \{r_1, \ldots, r_n\}$. Definiujemy funkcję $\alpha : R \to R$ wzorem

$$\alpha(r_i) = r_i a$$

dla każdego i. Jeżeli $\alpha(r_i) = \alpha(r_j)$, wtedy $r_i a = r_j a$, a zatem $(r_i - r_j)a = 0$. Ponieważ $a \neq 0$, otrzymujemy że $r_i = r_j$, a zatem α jest iniekcją, a ponieważ R jest skończony, to również bijekcją.

Dowód

Ponieważ $R \neq \{0\}$ możemy ustalić niezerowy element $a \in R$. Niech $R = \{r_1, \ldots, r_n\}$. Definiujemy funkcję $\alpha : R \to R$ wzorem

$$\alpha(r_i) = r_i a$$

dla każdego i. Jeżeli $\alpha(r_i) = \alpha(r_j)$, wtedy $r_i a = r_j a$, a zatem $(r_i - r_j)a = 0$. Ponieważ $a \neq 0$, otrzymujemy że $r_i = r_j$, a zatem α jest iniekcją, a ponieważ R jest skończony, to również bijekcją. W takim razie istnieją takie $t, t^* \in R$, że

$$\alpha(t) = a \quad \text{oraz} \quad \alpha(t^*) = t,$$

czyli

$$ta = a \quad \text{oraz} \quad t^* a = t.$$

Dowód

Zdefiniujmy teraz funkcję $\beta : R \longrightarrow R$ wzorem

$$\beta(r_i) = ar_i$$

dla każdego i. Na mocy tego samego rozumowania co wcześniej β jest bijekcją

Dowód

Zdefiniujmy teraz funkcję $\beta : R \longrightarrow R$ wzorem

$$\beta(r_i) = ar_i$$

dla każdego i. Na mocy tego samego rozumowania co wcześniej β jest bijekcją, a stąd istnieją takie $s, s^* \in R$, że

$$\beta(s) = a \quad \text{oraz} \quad \beta(s^*) = s,$$

czyli

$$as = a \quad \text{oraz} \quad as^* = s.$$

Dowód

$$ta = a, \quad t^*a = t, \quad as = a, \quad as^* = s$$

Niech teraz x będzie dowolnym elementem pierścienia R.

Dowód

$$ta = a, \quad t^*a = t, \quad as = a, \quad as^* = s$$

Niech teraz x będzie dowolnym elementem pierścienia R. Ponieważ α, β są bijekcjami, to istnieją elementy b oraz c w R takie, że

$$x = ba = ac.$$

Dowód

$$ta = a, \quad t^* a = t, \quad as = a, \quad as^* = s$$

Niech teraz x będzie dowolnym elementem pierścienia R. Ponieważ α, β są bijekcjami, to istnieją elementy b oraz c w R takie, że

$$x = ba = ac.$$

Mamy zatem, że

$$tx = t(ac) = (ta)c = ac = x,$$

Dowód

$$ta = a, \quad t^*a = t, \quad as = a, \quad as^* = s$$

Niech teraz x będzie dowolnym elementem pierścienia R. Ponieważ α, β są bijekcjami, to istnieją elementy b oraz c w R takie, że

$$x = ba = ac.$$

Mamy zatem, że

$$tx = t(ac) = (ta)c = ac = x,$$

a zatem t jest lewą jedynką pierścienia R. Podobnie,

Dowód

$$ta = a, \quad t^* a = t, \quad as = a, \quad as^* = s$$

Niech teraz x będzie dowolnym elementem pierścienia R. Ponieważ α, β są bijekcjami, to istnieją elementy b oraz c w R takie, że

$$x = ba = ac.$$

Mamy zatem, że

$$tx = t(ac) = (ta)c = ac = x,$$

a zatem t jest lewą jedynką pierścienia R. Podobnie,

$$xs = (ba)s = b(as) = ba = x,$$

Dowód

$$ta = a, \quad t^*a = t, \quad as = a, \quad as^* = s$$

Niech teraz x będzie dowolnym elementem pierścienia R. Ponieważ α, β są bijekcjami, to istnieją elementy b oraz c w R takie, że

$$x = ba = ac.$$

Mamy zatem, że

$$tx = t(ac) = (ta)c = ac = x,$$

a zatem t jest lewą jedynką pierścienia R. Podobnie,

$$xs = (ba)s = b(as) = ba = x,$$

a zatem s jest prawą jedynką R. A więc $t = ts = s = 1$.

Dowód

$ta = a, \quad t^*a = t, \quad as = a, \quad as^* = s, \quad s = t = 1$

Teraz ponieważ

$$as^* = s = 1 = t = t^*a,$$

Dowód

$ta = a, \quad t^*a = t, \quad as = a, \quad as^* = s, \quad s = t = 1$

Teraz ponieważ

$$as^* = s = 1 = t = t^*a,$$

wnioskujemy, że a posiada prawą odwrotność s^* i lewą odwrotność t^*.

Dowód

$ta = a, \quad t^*a = t, \quad as = a, \quad as^* = s, \quad s = t = 1$

Teraz ponieważ

$$as^* = s = 1 = t = t^*a,$$

wnioskujemy, że a posiada prawą odwrotność s^* i lewą odwrotność t^*. Stąd

$$s^* = 1s^* = (t^*a)s^* = t^*(as^*) = t^*1 = t^*,$$

Dowód

$ta = a, \quad t^*a = t, \quad as = a, \quad as^* = s, \quad s = t = 1$

Teraz ponieważ

$$as^* = s = 1 = t = t^*a,$$

wnioskujemy, że a posiada prawą odwrotność s^* i lewą odwrotność t^*. Stąd

$$s^* = 1s^* = (t^*a)s^* = t^*(as^*) = t^*1 = t^*,$$

zatem $s^* = t^* = a^{-1}$ i stąd każdy niezerowy element $a \in R$ jest odwracalny w R.

Dowód

$ta = a, \quad t^*a = t, \quad as = a, \quad as^* = s, \quad s = t = 1$

Teraz ponieważ

$$as^* = s = 1 = t = t^*a,$$

wnioskujemy, że a posiada prawą odwrotność s^* i lewą odwrotność t^*. Stąd

$$s^* = 1s^* = (t^*a)s^* = t^*(as^*) = t^*1 = t^*,$$

zatem $s^* = t^* = a^{-1}$ i stąd każdy niezerowy element $a \in R$ jest odwracalny w R. Widzimy zatem, że R jest skończonym pierścieniem z dzieleniem, a z małego twierdzenia Wedderburna R jest ciałem, co kończy dowód. $\square$

Kolejne ładne twierdzenie

Zajmiemy się teraz drugim uogólnieniem małego twierdzenia Wedderburna.

Twierdzenie 2

Niech R będzie pierścieniem skończonym z jedynką i niech T będzie zbiorem elementów odwracalnych pierścienia R. Jeśli $|T| > |R| - \sqrt{|R|}$, to R jest ciałem.

Kolejne ładne twierdzenie

Zajmiemy się teraz drugim uogólnieniem małego twierdzenia Wedderburna.

Twierdzenie 2

Niech R będzie pierścieniem skończonym z jedynką i niech T będzie zbiorem elementów odwracalnych pierścienia R. Jeśli $|T| > |R| - \sqrt{|R|}$, to R jest ciałem.

Zauważmy, że w założeniach małego twierdzenia Wedderburna występuje warunek $|T| = |R| - 1$. Powyższe twierdzenie mówi o tym, że wystarczy, aby zachodził warunek $|T| > |R| - \sqrt{|R|}$ by otrzymać ten sam wniosek.

Kolejne ładne twierdzenie

Zajmiemy się teraz drugim uogólnieniem małego twierdzenia Wedderburna.

Twierdzenie 2

Niech R będzie pierścieniem skończonym z jedynką i niech T będzie zbiorem elementów odwracalnych pierścienia R. Jeśli $|T| > |R| - \sqrt{|R|}$, to R jest ciałem.

Zauważmy, że w założeniach małego twierdzenia Wedderburna występuje warunek $|T| = |R| - 1$. Powyższe twierdzenie mówi o tym, że wystarczy, aby zachodził warunek $|T| > |R| - \sqrt{|R|}$ by otrzymać ten sam wniosek.

Co więcej, tego wyniku nie da się już poprawić, gdyż pierścień $\mathbb{Z}_{p^2}$, $p \in \mathbb{P}$, posiada dokładnie $p^2 - p$ elementów odwracalnych oraz nie jest ciałem.

Do dowodu tego twierdzenia będziemy potrzebować kilku prostych lematów. Od tej pory R jest pierścieniem skończonym z jedynką $1 \neq 0$.

Do dowodu tego twierdzenia będziemy potrzebować kilku prostych lematów. Od tej pory R jest pierścieniem skończonym z jedynką $1 \neq 0$.

Lemat 1

Dla $b \in R$, jeśli b^n jest lewym (odpowiednio, prawym) dzielnikiem zera dla pewnego $n \geqslant 1$, wtedy b jest lewym (odpowiednio, prawym) dzielnikiem zera.

Do dowodu tego twierdzenia będziemy potrzebować kilku prostych lematów. Od tej pory R jest pierścieniem skończonym z jedynką $1 \neq 0$.

Lemat 1

Dla $b \in R$, jeśli b^n jest lewym (odpowiednio, prawym) dzielnikiem zera dla pewnego $n \geqslant 1$, wtedy b jest lewym (odpowiednio, prawym) dzielnikiem zera.

Dowód

Niech $n > 1$ będzie najmniejszą liczbą naturalną, że b^n jest lewym dzielnikiem zera, oraz niech $t \neq 0$ będzie takie, że $b^n t = 0$.

Do dowodu tego twierdzenia będziemy potrzebować kilku prostych lematów. Od tej pory R jest pierścieniem skończonym z jedynką $1 \neq 0$.

Lemat 1

Dla $b \in R$, jeśli b^n jest lewym (odpowiednio, prawym) dzielnikiem zera dla pewnego $n \geqslant 1$, wtedy b jest lewym (odpowiednio, prawym) dzielnikiem zera.

Dowód

Niech $n > 1$ będzie najmniejszą liczbą naturalną, że b^n jest lewym dzielnikiem zera, oraz niech $t \neq 0$ będzie takie, że $b^n t = 0$. Wtedy równość $b(b^{n-1}t) = 0$ implikuje, że b jest lewym dzielnikiem zera, gdyż $b^{n-1}t \neq 0$. Dla prawych dzielników zera dowód jest analogiczny. $\square$

Lemat 2

Jeżeli $b \in R$, to albo b jest odwracalny, albo b jest zarówno lewym, jak i prawym dzielnikiem zera.

Ponieważ R jest skończony, to istnieją takie $i, j \in \mathbb{N}$, że $b^{i+j} = b^i$.

Lemat 2

Jeżeli $b \in R$, to albo b jest odwracalny, albo b jest zarówno lewym, jak i prawym dzielnikiem zera.

Dowód

Ponieważ R jest skończony, to istnieją takie $i, j \in \mathbb{N}$, że $b^{i+j} = b^i$. Stąd

$$b^{i+j} - b^i = b^i(b^j - 1) = (b^j - 1)b^i = 0.$$

Lemat 2

Jeżeli $b \in R$, to albo b jest odwracalny, albo b jest zarówno lewym, jak i prawym dzielnikiem zera.

Dowód

Ponieważ R jest skończony, to istnieją takie $i, j \in \mathbb{N}$, że $b^{i+j} = b^i$. Stąd

$$b^{i+j} - b^i = b^i(b^j - 1) = (b^j - 1)b^i = 0.$$

A zatem albo $b^j = 1$, albo b^i jest zarówno lewym i prawym dzielnikiem zera. Jeśli $b^j = 1$, to b jest odwracalny, a jeśli b^i jest dzielnikiem zera, to z Lematu 1 mamy, że b jest dzielnikiem zera. $\square$

Lemat 3

Przypuśćmy, że R posiada $n > 1$ lewych dzielników zera. Wtedy $|R| \leqslant n^2$.

Dowód

Z Lematu 2, R ma również dokładnie $n > 1$ prawych dzielników zera. Dla $x \in R$ niech $A(x) = \{r \in R \mid xr = 0\}$.

Ponieważ R ma n prawych dzielników zera i $n > 1$, to istnieje takie $0 \neq x \in R$, że $1 < |A(x)| \leqslant n$. Niech $0 \neq y \in A(x)$. Zauważmy, że skoro

$$x(yr) = (xy)r = 0, \quad \text{to} \quad yR \leqslant A(x) \quad \text{i stąd} \quad |yR| \leqslant n.$$

Rozważmy teraz grupy $(R, +)$ oraz $(yR, +)$. Definiujemy funkcję $f : R \to yR$ wzorem $f(r) = yr$, dla każdego $r \in R$.

Zauważmy, że $Ker(f) = A(y)$, a zatem $R/A(y)$ oraz yR są izomorficzne jako grupy abelowe. W szczególności, $|R| = |A(y)||yR| \leqslant n \cdot n = n^2$. $\square$

Możemy przystąpić do dowodu Twierdzenia 2.

Dowód

Niech D będzie zbiorem (lewych lub prawych) dzielników zera pierścienia R. Przypuśćmy, że $|T| > |R| - \sqrt{|R|}$.

Możemy przystąpić do dowodu Twierdzenia 2.

Dowód

Niech D będzie zbiorem (lewych lub prawych) dzielników zera pierścienia R. Przypuśćmy, że $|T| > |R| - \sqrt{|R|}$. Ponieważ żaden dzielnik zera nie jest odwracalny, to z Lematu 2 mamy, że $|T| + |D| = |R|$.

Możemy przystąpić do dowodu Twierdzenia 2.

Dowód

Niech D będzie zbiorem (lewych lub prawych) dzielników zera pierścienia R. Przypuśćmy, że $|T| > |R| - \sqrt{|R|}$. Ponieważ żaden dzielnik zera nie jest odwracalny, to z Lematu 2 mamy, że $|T| + |D| = |R|$. Jeśli $D = \{0\}$, to R jest ciałem na mocy Twierdzenia 1. W przeciwnym wpadku $|D| > 1$.

Możemy przystąpić do dowodu Twierdzenia 2.

Dowód

Niech D będzie zbiorem (lewych lub prawych) dzielników zera pierścienia R. Przypuśćmy, że $|T| > |R| - \sqrt{|R|}$. Ponieważ żaden dzielnik zera nie jest odwracalny, to z Lematu 2 mamy, że $|T| + |D| = |R|$. Jeśli $D = \{0\}$, to R jest ciałem na mocy Twierdzenia 1. W przeciwnym wpadku $|D| > 1$. Założenia Lematu 3 są spełnione, zatem

$$|R| \leqslant |D|^2 \quad \text{oraz} \quad \sqrt{|R|} \leqslant |D|.$$

Możemy przystąpić do dowodu Twierdzenia 2.

Dowód

Niech D będzie zbiorem (lewych lub prawych) dzielników zera pierścienia R. Przypuśćmy, że $|T| > |R| - \sqrt{|R|}$. Ponieważ żaden dzielnik zera nie jest odwracalny, to z Lematu 2 mamy, że $|T| + |D| = |R|$. Jeśli $D = \{0\}$, to R jest ciałem na mocy Twierdzenia 1. W przeciwnym wpadku $|D| > 1$. Założenia Lematu 3 są spełnione, zatem

$$|R| \leqslant |D|^2 \quad \text{oraz} \quad \sqrt{|R|} \leqslant |D|.$$

Jednak ponieważ

$$|T| > |R| - \sqrt{|R|} \quad \text{oraz} \quad |T| = |R| - |D|,$$

otrzymujemy, że $\sqrt{|R|} > |D|$. Sprzeczność. To kończy dowód. $\square$

Bibliografia

D. MacHale, When is a Finite Ring a Field?, IMS Bulletin 37, 1996

D. MacHale, Wedderburn's Theorem Revisited, IMS Bulletin 20, 1986

D. MacHale, Wedderburn's Theorem Revisited (Again), IMS Bulletin 20, 1988

N. Ganesan, Properties of Rings with Finite Number of Zero Divisors II, Math. Annalen 161 (1965) 241-246.