WYKŁAD 12

Warstwy:

$H \leq G$

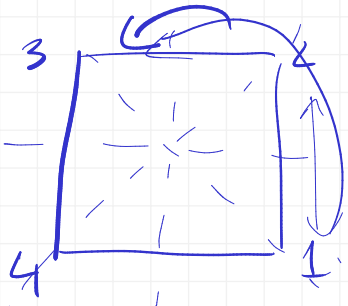
warstwa lewostronna H

$aH = \{ah : h \in H\}$

$a \in G$

Ha

Przykład 17.7. Naszą grupą będą obroty i odbicia kwadratu; niech wierzchołki kwadratu będą ponumerowane $1, 2, 3, 4$, w kolejności przeciwnej do ruchu wskazówek zegara, 1 w prawym dolnym rogu. Ta grupa ma 8 elementów (identyczność, obrót o 90^0, 180^0, 270^0, symetrie względem przekątnych, symetria pionowa i symetria pozioma) i możemy o niej myśleć jak o podgrupie S_4, czyli te elementy to $e; (1,2,3,4); (1,3)(2,4); (1,4,3,2); (1,3); (2,4); (1,4)(2,3); (1,2)(3,4)$.



90° (1 2 3 4)

8 el.

- $e; (1,2,3,4); (1,3)(2,4); (1432)$ ← warstwa lewo./prawostronna

$(1,3); (2,4); (1,2)(3,4); (2,3)(1,4)$ ←

$(1,3)\cdot\{e; (1,2,3,4); (1,3)(2,4); (1432)\}$

$= \{(1,3); (1,2)(3,4); (2,4); (1,4)(3,2)\}$

Weźmy podgrupę obrotów, ma 4 elementy $e; (1,2,3,4); (1,3)(2,4); (1,4,3,2)$.

$e, (14)(2,3)$ ← 4 warstwy lewostronne

- $e, (1,4)(2,3)$

$(1,3)\cdot\{e, (1,4)(2,3)\} = \{(1,3); (1,4,3,2)\}$

$\{e, (1,4)(2,3)\}\cdot(1,3) = \{(1,3); (1,2,3,4)\}$

Weźmy grupę generowaną przez symetrię pionową, ta grupa ma dwa elementy (symetria pionowa $(1,4)(2,3)$ i identyczność e).

Przykład 17.8. Grupa permutacji na 3 elementach (S_3). Podgrupa generowana przez cykl $(1,2,3)$ ma 3 elementy. Czyli ma dwie warstwy (ta podgrupa: permutacje parzyste i pozostałe elementy: permutacje nieparzyste).

Podgrupa generowana przez cykl $(1,2)$ (innymi słowy: wszystkie permutacje, które trzymają 3 w miejscu). Ma dwa elementy, czyli ma 3 warstwy lewostronne i 3 prawostronne.

$H = e, (1,2,3), (1,3,2)$ 6

$\to (1,2); (1,3); (2,3)$

$H = \{e, (1,2)\}$

Lewostronne

$\sigma(3) = 3$ $3 \to 3$

- $\{e, (1,2)\}$
- $(1,2,3) \cdot \{e, (1,2)\}$

$\{(1,2,3); (1,3)\}$ $\leftarrow$ $3 \to 1$

- $(1,3,2) \cdot \{e, (1,2)\}$

$\{(1,3,2); (2,3)\}$ $3 \to 2$

$\sigma H = \sigma' H$

$\sigma^{-1}\sigma' \in H$

$\sigma^{-1}\sigma'(3) = 3$

$\sigma^{-1}(k) = 3$

$\sigma(3) = k$ $k \to 3$

$\sigma'\sigma^{-1}(3) = 3$ ($\sigma'\sigma^{-1} \in H$)

$\{e, (1,2)\}$ $3 \to 3$

$\{e; (1,2)\} \cdot (1,2,3) = \{(1,2,3); (2,3)\}$

$\{e; (1,2)\} \cdot (1,3,2) = \{(1,3,2); (1,3)\}$

Rozdział 18

Homomorfizmy i grupy ilorazowe, podgrupy normalne.

$\varphi : G \to H$

$\varphi(ab) = \varphi(a)\varphi(b)$

$\varphi(e) = e$

$\varphi(a^{-1}) = (\varphi(a))^{-1}$

18.1 Homomorfizmy

Definicja 18.1 (Jądro, obraz homomorfizmu)**.** Dla homomorfizmu $\varphi : G \to H$ jego *obraz* to $\operatorname{Im}\varphi = \{\varphi(g) : g \in G\} = \varphi(G)$ zaś *jądro* to $\ker\varphi = \{g : \varphi(g) = e\} = \varphi^{-1}(e)$.

Lemat 18.2. *Dla homomorfizmu $\varphi : G \to H$ jego jądro i obraz to podgrupy, odpowiednio G oraz H.*

- $\operatorname{Im}\varphi$

  $b, b' \in \operatorname{Im}\varphi \quad \exists_{a,a'} \varphi(a) = b,\ \varphi(a') = b'$

  $\varphi(aa') = \varphi(a)\varphi(a') = bb' \in \operatorname{Im}\varphi$

  $b = \varphi(a)$

  $\varphi(a^{-1}) = (\varphi(a))^{-1}$

  $\| \quad\quad \| \quad\quad \| \quad\quad \|$

  $b^{-1} \quad\quad b^{-1}$

- $\ker(\varphi)$

  $a, a' \quad \varphi(a) = \varphi(a') = e$

  $\varphi(aa') = e$

  $\varphi(e) = e$

  $\varphi(a^{-1}) = \varphi(a)^{-1}$

  $\varphi(a) = e$

  $\varphi(a^{-1}) = e$

  $\Uparrow$

  $\ker\varphi$

Jaki jest związek między podgrupami a homomorfizmami? Miedzy podgrupami a jądrem jakiegoś homomorfizmu?

Definicja 18.3 (Podgrupa normalna)**.** H jest *podgrupą normalną* G, gdy $aH = Ha$ dla każdego elementu $a \in G$; zapisujemy to jako $H \trianglelefteq G$.

Przykład 18.4.
1. Trywialna podgrupa $\{e\}$ jest zawsze normalna.
2. Grupa alternująca A_n jest normalną podgrupą S_n.
3. Grupa obrotów kwadratu jest normalną podgrupą jego symetrii.
4. Wszystkie podgrupy grupy przemiennej są normalne.
5. Centrum każdej grupy jest podgrupą normalną.
6. Podgrupa grupy S_4 : $\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ jest normalna.
7. Każda podgrupa indeksu 2 jest normalna.
8. Współrzędna w produkcie grup jest zawsze normalna.

Lemat 18.5. *Następujące warunki są równoważne dla podgrupy H*

1. $aH = Ha$ *dla każdego elementu* a;
2. $aH \subseteq Ha$ *dla każdego elementu* a;
3. $aH \supseteq Ha$ *dla każdego elementu* a;
4. $aHa^{-1} = H$ *dla każdego elementu* a;
5. $aHa^{-1} \subseteq H$ *dla każdego elementu* a;
6. $aHa^{-1} \supseteq H$ *dla każdego elementu* a.

Definicja 18.6 (Podgrupa sprzężona)**.** Dla $H \leq G$ podgrupa postaci gHg^{-1} to *podgrupa sprzężona* do H.

Fakt 18.7. *Podgrupy sprzężone są izomorficzne. W ogólności dla $g \in G$ przekształcenie $h \mapsto gxg^{-1}$ jest izomorfizmem grupy z samą sobą (może to być identyczność).*

$H \qquad gHg^{-1}$

$\varphi_g(h) = ghg^{-1} \qquad \varphi_{g^{-1}}$

Lemat 18.8. *Jeśli $\varphi : G \to H$ jest homomorfizmem, to $\ker\varphi$ jest podgrupą normalną.*

• $\ker\varphi \leq G$ wiemy

normalne $N = \ker\varphi$

wystarczy, że $gNg^{-1} \subseteq N$

— " — $\varphi(gNg^{-1}) = \{e\}$

$\varphi(g)\varphi(N)\varphi(g^{-1}) = \varphi(g)\ \varphi(g^{-1})$

$= \varphi(gg^{-1}) = \varphi(e) = e$

$\forall g \quad gNg^{-1} \subseteq N$

$\Rightarrow \forall_g\ gNg^{-1} = N \qquad \ker\varphi \trianglelefteq G$

18.2 Działanie na warstwach

$H \leq G \qquad aH \cdot bH = \{a'b' : a' \in aH,\ b' \in bH\}$

Popatrzmy na działanie mnożenia podzbiorów grupy w ograniczeniu do warstw (prawostronnych) $H \trianglelefteq G$. Wtedy

Fakt: $H \trianglelefteq G \qquad aH \cdot bH = (ab)H$

$(aH)(bH) = (Ha)(bH) = H(ab)H = (ab)HH = ab(H \cdot H) = (ab)H$

Definicja 18.9 (Grupa ilorazowa)**.** Gdy H jest podgrupą normalną G, to zbiór warstw H w G, czyli G/H, ma strukturę grupy dla działania:

$$aH \cdot bH = (ab)H$$

Grupę tę nazywamy *grupą ilorazową*.

Lemat 18.10. *„Grupa ilorazowa" jest grupą.*

18.3 Naturalny homomorfizm $G \mapsto G/H$.

Lemat 18.11. *Niech $H \trianglelefteq G$ będzie podgrupą normalną G. Wtedy naturalny rzut z G na warstwy G, tj. $\pi_H : G \mapsto G/H$, gdzie $\pi_H(a) = aH$, jest homomorfizmem; co więcej, $H = \ker \pi_H$.*

- $a \mapsto aH$
- homomorfizm

a, b

$\pi_H(a)\,\pi_H(b) = aH \cdot bH = ab \cdot H = \pi_H(ab)$ homomorfizm

- jądro: a: $aH = H$ ← el. neutralny w G/H

$a \in H$

$\ker \pi_H = H$

$\varphi: G \xrightarrow{na} H$ $\quad \ker\varphi = K \trianglelefteq G$

$\pi_K: G \xrightarrow{na} G/K$ $\quad \ker \pi_K = K$

---

różnowartościowe

$\varphi(aH) = \varphi(bH) \Leftrightarrow$

$\varphi(a^{-1}b\,H) = e$

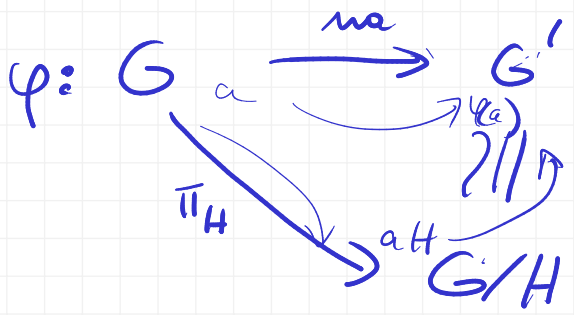
$\varphi(a^{-1}b) = e$

$a^{-1}b \in H$

$a^{-1}bH = H$

$bH = aH$

Twierdzenie 18.12. *Niech $\varphi : G \to G'$ będzie homomorfizmem. Wtedy istnieje izomorfizm $\psi : G/\ker\varphi \to \operatorname{Im}\varphi$.*



ker $\varphi = H \trianglelefteq G$

• izomorfizm φ: $G/H \to G'$ $\quad H = \ker\varphi$

$\varphi(aH) = \varphi(a)$ ← dobrze określone

Czy to jest dobrze określone?

$\varphi(aH) = \varphi(a)\cdot\varphi(H) = \varphi(a)$

$\varphi(a'H) = \ldots = \varphi(a')$

na: $G' = \varphi(G)$

$\varphi(aH) = \varphi(a) = b'$

• homomorfizm:

$\varphi(aH)\varphi(bH) = \varphi(a)\varphi(b)$

$= \varphi(ab) = \varphi(abH)$

18.4 Kongruencje, konstrukcja $\mathbb{Z}_n$

$H \trianglelefteq G$ $\quad G \to G/H$

To pozwala na zdefiniowanie kongruencji dla podgrupy normalnej $H \trianglelefteq G$:

$$a \equiv_H b \leftrightarrow aH = bH \iff a \equiv_H b \leftrightarrow a^{-1}b \in H \iff a \equiv_H b \leftrightarrow ba^{-1} \in H$$

(Zauważmy też, że $aH = Ha$ oraz $bH = Hb$.)

$a \equiv b$

$b \equiv c$

To jest *kongruencja*:

Definicja 18.13 (Kongruencja w grupie)**.** Relacja $\equiv \subseteq G^2$ na grupie G jest *kongruencją*, jeśli:

✓ **relacja równoważności** jest relacją równoważności *oraz*

zachowuje działania zachowuje działania, tzn. dla każdych $a, a', b, b' \in G$ zachodzi:

$$a \equiv b \wedge a' \equiv b' \to aa' \equiv bb'$$
$$a \equiv b \to a^{-1} \equiv b^{-1}$$

$a \quad b$

$\varphi(a) = \varphi(b)$

$\varphi(a') = \varphi(b')$

Poprawność definicji kongruencji $\equiv_H$ można policzyć wprost, ale nie trzeba: wynika z tego, że przekształcenie $a \mapsto aH$ jest homomorfizmem.

$\varphi(aa') = \varphi(a)\varphi(a')$

$\varphi(bb') = \varphi(b)\varphi(b')$

18.4.1 Konstrukcja $\mathbb{Z}_m$

Ważny przykład: $\mathbb{Z}_n$: kongruencja na $\mathbb{Z}$ względem podgrupy „liczby podzielne przez n”, zwyczajowo określanej jako $n\mathbb{Z}$. Jako że $\mathbb{Z}$ jest przemienna, to ta podgrupa jest normalna. Czyli mamy podgrupę normalną, konstrukcję $\mathbb{Z}_n$ oraz kongruencję na $\mathbb{Z}$.

$(\mathbb{Z}, +)$ przemienna

$\mathbb{Z} \supset n\mathbb{Z}$ ← liczby podzielne przez n

$\mathbb{Z}/n\mathbb{Z}$ $\quad 0, \ldots, n-1$

i-ta wartwa $= \{n\mathbb{Z} + i\}$ $\quad i \in \{0, \ldots, n-1\}$

$(\mathbb{Z}_n, +_n)$

$i + n\mathbb{Z} + j + n\mathbb{Z}$

$(i+j) + n\mathbb{Z}$

$\equiv_n$

Rozdział 19

Pierścienie, ciała, arytmetyka modularna

19.1 Pierścienie

Definicja 19.1 (Pierścień)**.** Pierścień, oznaczany zwykle przez R, to zbiór z dwoma działaniami $+, \cdot$, spełniającymi warunki:

- $(R, \cdot)$ jest półgrupą (niekoniecznie przemienną)
- $(R, +)$ jest grupą przemienną

Ponadto zachodzi rozdzielność mnożenia względem dodawania

- $a(b+c) = ab + ac$, $(b+c)a = ba + ca$

Pierścień jest *z jednością*, jeśli ma element neutralny dla mnożenia. Pierścień jest *przemienny*, jeśli $ab = ba$ (czyli półgrupa ze względu na mnożenie jest półgrupą przemienną).

Dalej będziemy się zajmować w zasadzie tylko i wyłącznie pierścieniami przemiennymi z jednością.

Definicja 19.2. Ciało $\mathbb{F}$ to pierścień przemienny z jednością, w którym $(\mathbb{F}, \cdot)$ jest grupą, tzn. każdy element ma element odwrotny, oraz elementy neutralne dodawania i mnożenia są różne („$0 \neq 1$”).

Przykład 19.3.

- liczby całkowite $\mathbb{Z}$
- macierze o współczynnikach z dowolnego ciała (pierścień nieprzemienny!)
- $\mathbb{Z}_m$: liczby modulo m z dodawaniem i mnożeniem
- $R[x]$ wielomiany o współczynnikach z R
- $R[[x]]$ szeregi formalne o współczynnikach z R.

Twierdzenie 19.4. *$\mathbb{Z}_m$ jest ciałem $\iff$ m jest pierwsze.*

Dowód pokażemy w dalszej części rozdziału.

19.2 Arytmetyka modularna $\mathbb{Z}_m$

.

Definicja 19.5 (Liczenie modulo, $\mathbb{Z}_m$)**.** a przystaje do b modulo m gdy $m|(a-b)$. Oznaczenie:

$$a \equiv_m b \ .$$

Reszta z dzielenia przez m:

$$a \mod m = b \iff a \equiv_m b \wedge b \in \{0, 1, \ldots, m-1\} \ .$$

~~W zasadzie to liczymy tylko reszty z dzielenia itp. dla liczb dodatnich.~~

Lemat 19.6. *Dla dowolnego $m \in \mathbb{Z}_+$ relacja $\equiv_m$ jest* kongruencją ze względu na mnożenie i dodawanie, *tzn.:*

$$a \equiv_m b \wedge a' \equiv_m b' \Rightarrow aa' \equiv_m bb'$$
$$a \equiv_m b \wedge a' \equiv_m b' \Rightarrow a + a' \equiv_m b + b' \ .$$

Wniosek 19.7. Przekształcanie $n \mapsto n \bmod m$ jest homomorfizmem pierścieni $\mathbb{Z}$ i $\mathbb{Z}_m$.

To ważne o tyle, że wykonując działania mod m możemy dowolnie przełączać się między $\mathbb{Z}$ i $\mathbb{Z}_m$.

W sumie to chcielibyśmy więcej: czy „prawa" przenoszą się między $\mathbb{Z}$ i $\mathbb{Z}_m$? Na pewno nie wszystkie: umiemy powiedzieć, że w $\mathbb{Z}$ są conajmniej 3 różne elementy, ale to nie jest prawda w $\mathbb{Z}_3$. Okazuje się, że prawa się przenoszą, jeśli nie używają negacji.

Definicja 19.8 (Formuła pozytywna)**.** Niech t_1, t_2 będą wyrażaniami zbudowanymi z nawiasów, zmiennych $x_1, x_2, \ldots, x_n$, elementów z A oraz działań $+, \cdot$. Wtedy formuła ψ składająca się spójników $\wedge, \vee$ oraz równości $t_1 = t_2$, gdzie t_1, t_2 są jak wyżej, nazywamy *formuła pozytywną.*

Lemat 19.9. *Niech ψ będzie formuła pozytywną, zaś $\varphi : A \mapsto B$ będzie homomorfizmem na pierścień B.*

Jeśli

$$Q_1 x_1 Q_2 x_2 \ldots Q_n x_n \psi(x_1, x_2, \ldots, x_n)$$

zachodzi w A, to w B zachodzi:

$$Q_1 x_1 Q_2 x_2 \ldots Q_n x_n \psi'(x_1, x_2, \ldots, x_n) \ ,$$

gdzie ψ' jest uzyskane z ψ przez zamianę stałych c w wyrażeniach przez $\varphi(c)$ zaś Q_i jest kwantyfikatorem (uniwersalnym lub egzystencjalnym).

Dowód to indukcja po strukturze. Podstawa indukcji wynika z tego, że to homomorfim i nie ma negacji.

Wniosek 19.10. W $\mathbb{Z}_m$ zachodzą wszystkie prawa, o których myślimy.

19.3 Algorytm Euklidesa

Wracamy do naszego ulubionego ciała: $\mathbb{Z}_p$. Kiedyś już powiedzieliśmy, że jest tam element odwrotny. A co w $\mathbb{Z}_m$? Jest? Nie ma? Dla którego jest, czy można efektywnie wyznaczyć?

Konstrukcyjna metoda używała będzie *algorytmu Euklidesa*. Opiera się on na obserwacji, że $\mathrm{nwd}(a,b) = \mathrm{nwd}(a-b,b)$ oraz $\mathrm{nwd}(0,b) = \mathrm{nwd}(b,0) = b$. Można to przyspieszyć, poprzez $\mathrm{nwd}(a,b) = \mathrm{nwd}(a \bmod b, b)$.

Definicja 19.11. Liczba $0 \neq k \in \mathbb{N}$ jest największym wspólnym dzielnikiem $a, b \in \mathbb{Z}$, jeśli $k|a$, $k|b$ i dla każdego ℓ zachodzi $\ell|a, \ell|b \implies \ell|k$.

Oznaczenie: $\mathrm{nwd}(a,b)$.

Uwaga. nwd jest największy w sensie porządku częściowego zdefiniowanego przez podzielność.

Lemat 19.12. 1. *Jeśli $k|a$ i $k|b$ to $k|(a+b)$ i $k|(a-b)$.*

2. *Jeśli $k|a$ i $k|b$ to $k|(a \bmod b)$.*

3. *Jeśli $k|(a \bmod b)$ i $k|b$ to $k|a$.*

Indukcja: nwd pary liczb się nie zmienia w trakcie algorytmu.

Zbiór dzielników a, b

Algorytm 2 Algorytm Euklidesa

Założenie: a, b są nieujemne, choć jedna jest dodatnia

```
1: while a > 0 oraz b > 0 do
2:     if a < b then
3:         zamień a, b
4:     a ← a − b                          ▷ Może też być a mod b
5: if a ≥ b then
6:     return a
7: else
8:     return b
```

Wniosek 19.13. Algorytm Euklidesa zwraca największy wspólny dzielnik.

Lemat 19.14. *Algorytm Euklidesa (w wersji z modulo) działa w czasie wielomianowym (od długości zapisu liczb). To ograniczenie jest ścisłe.*

Dowód pozostawiamy jako zadanie.

Lemat 19.15. *W czasie algorytmu Euklidesa możemy przechowywane liczby reprezentować jako kombinacje liniowe (o współczynnikach całkowitych) a oraz b.*

To pozwala na

Lemat 19.16. *Dla $a, b \in \mathbb{Z}_+$ istnieją $x, y \in \mathbb{Z}$ takie że*

$$\operatorname{nwd}(a, b) = xa + yb.$$

Dokładnie jedna z tych liczb jest dodatnia i jedna niedodatnia. Dodatkowo, liczby te można wybrać tak, że $|x| < b$, $|y| < a$. Jeśli $\operatorname{nwd}(a, b) = 1$ to są dokładnie dwa takie wyrażenia (w jednym x jest dodatnie a w drugim ujemne).

Proty dowód pozostawiamy jako ćwiczenie.

Lemat 19.17. *W pierścieniu $\mathbb{Z}_m$ element a ma element odwrotny* $\iff$ $\mathrm{nwd}(a, m) = 1$.

$\Leftarrow$ $\mathrm{nwd}(a,m)=1$ $\quad |x|<m$

x, y $\quad xa + ym = 1$

$xa = 1 - ym$ / mod m

$xa \equiv_m 1$

x - el. odwrotny $\quad$ $x \neq m$ $\quad$ $(x) \bmod m$

$\Rightarrow$ a ma el. odw $\Rightarrow \mathrm{nwd}(a,m)=1$

$\mathrm{nwd}(a,m)>1 \Rightarrow a$ nie ma el. odwr.

$\mathrm{nwd}(a,m)=l>1$ $\quad b$ $\quad ab \equiv_m 1$

$\exists k \in \mathbb{Z}$ $\quad ab = 1 + km$

$l \mid a \Rightarrow l \mid ab$

$l \mid m \Rightarrow l \mid km$

$l \mid 1$ ↯

Uwaga. Zauważmy, że Lemat 19.17 w szczególności daje dowód Twierdzenia 19.4.

$\mathbb{Z}_m$ - ciało $\iff$ m - pierwsze

- m - pierwsze $\quad \mathbb{Z}_m \quad a \in \mathbb{Z}_m \quad \{1, \dots, m-1\}$

$\mathrm{nwd}(a, m) = 1$ $\quad$ R pierwsze

- $\mathbb{Z}_m$ - ciało $\quad \mathrm{nwd}(a, m) = 1 \quad 0 < a < m$

m nie ma dzielników m - pierwsze

19.4 Elementy odwracalne

$\mathbb{Z}_m \quad R$

Definicja 19.18 (elementy odwracalne)**.** Element a pierścienia R nazywamy *odwracalnym*, jeśli istnieje $b \in R$ takie że $ab = 1$.

Zbiór elementów odwracalnych pierścienia R oznaczamy jako R^*. $\quad \mathbb{Z}_m^*$

Twierdzenie 19.19. *Dla dowolnego pierścienia R z jednością zbiór elementów odwracalnych R^* jest grupą na mnożenie.* $\quad (R, \cdot) \quad (R^*, \cdot)$

- $1 \in R^*$

  $1 \cdot 1 = 1$

- $a \in R$

  a^{-1} ramna -1

  $a^{-1}a$

- $a, b \in R^*$

  a^{-1} b^{-1} $\quad b^{-1}a^{-1} \in$ el. dwr. do ab

- Twierdzenie: R - półgrupa R^*

  $R^* \Rightarrow$ grupa

$nwd(27, 58)$

$= nwd(27, 4)$

$= nwd(3, 4)$

$= nwd(3, 1)$

	27	58
58	0	1
27	1	0
4	-2	1
3	13	-6
1	-15	7

$4 = 58 - 2 \cdot 27$

$3 = 27 - 6 \cdot 4$

$7 \cdot 58 - 15 \cdot 27 = 1$

$(-15) \cdot 27 = 1 - 7 \cdot 58$

$27^{-1} \equiv_{58} 43$

$27 \cdot 43 \equiv_{58} 1$

Uwaga. $\mathbb{Z}_m^*$ nie ma struktury pierścienia, w szczególności nie jest ciałem!

Twierdzenie 19.20. *Dla ciała skończonego $\mathbb{F}$ grupa $\mathbb{F}^*$ jest cykliczna.*

To twierdzenie jest dość trudne, Rozdział 22 zawiera dowód w przypadku $\mathbb{F} = \mathbb{Z}_p$.

Definicja 19.21 (Symbol Eulera)**.** $\varphi(m)$ to liczba liczb względnie pierwszych z m mniejszych od m.

Wniosek 19.22 (Twierdzenie Eulera). Niech a, m są względnie pierwsze. Wtedy

$$a^{\varphi(m)} = 1 \mod m$$

19.5 Chińskie twierdzenie o resztach

Definicja 19.23 (Produkt pierścieni.)**.** Produkt pierścieni definiujemy standardowo: dla pierścienie R, R' ich produkt $R \times R'$ ma jako zbiór iloczyn kartezjański zbiorów R, R' a działania są po współrzędnych.

Lemat 19.24. *Proste własności:*

- $R \times R'$ *i* $R' \times R$ *są izomorficzne*
- *produkt kartezjański jest łączny (z dokładnością do izomorfizmu):* $R_1 \times (R_2 \times R_3)$ *i* $(R_1 \times R_2) \times R_3$ *są izomorficzne*

- *Jeśli R_1 jest izomorficzne z R'_1 a R_2 z R'_2, to $R_1 \times R_2$ jest izomorficzne z $R'_1 \times R'_2$.*

Twierdzenie 19.25 (Chińskie Twierdzenie o resztach)**.** *Jeśli $m_1, m_2, \ldots, m_k$ są parami względnie pierwsze, to naturalny homomorfizm z $\mathbb{Z}_{m_1 m_2 \cdots m_k}$ w $\prod_{i=1}^{k} \mathbb{Z}_{m_i}$, gdzie na i-tej współrzędej bierzemy modulo $\mathbb{Z}_{m_i}$, jest izomorfizmem.*

2, 3, 5, 7, 11, 13

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 > 20.000$