Algebra 2010
Notatki do wykładów

A. Paweł Wojda
Wydział Matematyki Stosowanej AGH

26 stycznia 2011

Spis treści

Rozdział 1

Wykład 1. 6.X.2010

1.1 Wstęp

Zacznijmy od kilku informacji o historii nazwy przedmiotu.
Nazwa **algebra** pochodzi od tytułu dzieła arabskiego matematyka działającego w IX wieku w Bagdadzie, Muhammada Ibn Mussa Al Chwarizimi: *Hisab al-dżabr wal mukabala* (w transkrybcji polskiej, oczywiście). Algebra jest zniekształconym **al-dżabr** z owego tytułu[1]. Tytuł ten oznacza *Sztuka redukcji i przenoszenia*, zaś samo dzieło arabskiego matematyka dotyczyło rozwiązywania równań algebraicznych stopni pierwszego i drugiego. Al Chwarizimi był główną postacią znakomitej instytucji którą był bagdadzki *Dom Nauki*, prekursor późniejszych uniwersytetów i instytucji naukowych. Nazwisko Al Chwarizimiego, także zniekształcone[2], stało się źródłem nazwy *algorytm*, tak ważnej we współczesnej matematyce i informatyce.
Zainteresowanych historią matematyki namawiam gorąco do przeczytania pięknej książki Marka Kordosa *Wykłady z historii matematyki* dzięki której można poznać historię matematyki, prześledzić jak powstawała i zrozumieć jak bardzo niebanalnymi były, dla pozbawionych współczesnego formalizmu algebraicznego uczonych, działających we wcale niedawnej przeszłości wieków średnich, najprostsze operacje algebraiczne.

Poza aspektami historycznymi, warto w tym miejscu zwrócić uwagę na jeszcze jedną sprawę. Ta część algebry, która jest obiektem *Notatek*, najczęściej nazywana jest *algebrą abstrakcyjną*. To piękna i dobra nazwa, która wyróżnia ten dział od *algebry liniowej*. Niestety przymiotnik *abstrakcyjna* sugruje też: *niekoniecznie potrzebna*. To oczywista nieprawda - nawet podczas tego wykładu

[1] W językach angielskim i francuskim podobieństwo słowa *algebra* czy też *algèbre* do arabskiego oryginału jest znacznie wyraźniejsze niż w języku polskim.

[2] Tytuł dzieła Al Chwarizimiego przetłumaczony na łacinę brzmiał *Algorithmi de numero Indorum*, co miało znaczyć: *Al Chwarizimiego dzieło o liczbach indyjskich*. To właśnie dzieki temu dziełu Europa poznała dziesiątkowy system pozycyjny i liczbę zero, które matematycy arabscy przejęli od Hindusów.

będziecie mieli okazje do poznania niektórych zastosowań. Więcej zastosowa algebry abstrakcyjnej poznacie z pewnością na innych przedmiotach (kodowanie, matematyka dyskretna, teoria algorytmów...).

Jak z pewnością zauważyliście, spis literatury jest znacznie obszerniejszy niż ten, który podałem podczas wykładu. Oczywiście nie musicie wszystkiego czytać, w każdym razie nie dzisiaj :)

A. Paweł Wojda

1.2 Arytmetyka liczb całkowitych

Poniżej przypomnimy niektóre definicje i wasności liczb całkowitych, które potrzebne nam będą w dalszym ciągu wykładu.
Zacznijmy od **twierdzenia o dzieleniu liczb całkowitych**.

Twierdzenie 1.1 *Dla dowolnych liczb całkowitych a i b, $b > 0$ istnieją jednoznacznie wyznaczone liczby $q, r \in \mathbf{Z}$ takie, że*

$$a = bq + r \tag{1.1}$$

przy czym $0 \leq r < b$.

Liczby q oraz r nazywamy, odpowiednio, **ilorazem** i **resztą** dzielenia a przez b.

Mówimy, że d jest **największym wspólnym dzielnikiem** liczb całowitych a i b jeżeli

- $d|a$ i $d|b$ oraz
- dla każdego $c \in \mathbf{Z}$: $c|a \ \wedge c|b \Rightarrow c|d$

Dowód twierdzenia 1.1 powinien być świetnie znany ze szkoły. Wykażemy jednak istotną dla nas własność występujących nim liczb a, b i r.

Fakt 1.2 $NWD(a, b) = NWD(b, r)$.

Rzeczywiście, oznaczmy $d = NWD(a, b)$ oraz $c = NWD(b, r)$. Skoro d dzieli a oraz b, dzieli także r (najlepiej widać ten fakt po napisaniu wzoru (1.1) w postaci $r = a - bq$). Ponieważ zaś c jest największym wspólnym dzielnikiem b i r, d dzieli c.
Równie łatwo dowodzimy, że $c|d$, skąd już natychmiast wynika fakt 1.2.

Algorytm Euklidesa

Niech $a, b \in \mathbf{Z}$, $a, b \neq 0$.
Tworzymy rekurencyjnie ciąg (r_n):
$r_0 = a, \quad r_1 = b$
$r_{n-1} = q_n r_n + r_{n+1}$, gdzie $0 \leq r_{n+1} < r_n$. Zauważmy, że skoro dla każdego n dla ktżego $r_n > 0$ zachodzi $r_{n+1} < r_n$, ciąg (r_n) jako ciąg nieujemny jest skończony, istnieje takie $k > 1$, że r_k 0 oraz $r_{k+1} = 0$. Mamy więc ciąg k równości:

$$\begin{cases} r_0 = q_1 r_1 + r_2 & r_2 < r_1 \\ r_1 = q_2 r_2 + r_3 & r_3 < r_2 \\ \ldots & \\ r_{k-2} = q_{k-1} r_{k-1} + r_k & r_k < r_{k-1} \\ r_{k-1} = q_k r_k & \end{cases} \tag{1.2}$$

Na mocy faktu 1.2 mamy: $NWD(r_0, r_1) = NWD(r_1, r_2) = \ldots = NWD(r_{k-2}, r_{k-1}) = NWD(r_{k-1}, r_k) = r_k$. To oznacza, że prawdziwe jest następujące twierdzenie.

Twierdzenie 1.3 *Niech $a, b \in \mathbf{Z}$, $a, b \neq 0$. Istnieje takie k całkowite, że $r_k \neq 0$ oraz $r_{k+1} = 0$ (gdzie ciąg (r_n) jest wyznaczony przy pomocy algorytmu Euklidesa). Co więcej, mamy wówczas $r_k = \text{NWD}(a, b)$.*

Zauważmy, że algorytm Euklidesa kończy się w liczbie kroków ograniczonej przez $|b|$ i w tym sensie jest to algorytm szybki, efektywny[3].

Twierdzenie 1.4 *Niech $a, b \in \mathbf{Z}$, nie równe równocześnie zero.*

$$NWD(a, b) = min\{d > 0 : d = ax + by, \quad x, y \in \mathbf{Z}\}$$

Dowód. Niech $A = \{d > 0 : d = \alpha a + \beta b, \alpha, \beta \in \mathbf{Z}\}$. Zauważmy, że $A \neq \emptyset$ oraz, że $\min A$ istnieje. Oznaczmy $d = \min A$. Oczywiście $d \in A$, a więc istnieją takie α i β, że $d = \alpha a + \beta b$. Wykażemy wpierw, że $d|a$. Rzeczywiście, przypuśćmy, że

$$a = qd + r$$

gdzie $d > r > 0$. Wówczas

$$0 < r = a - qd = a - q(\alpha a + \beta b) = a(1 - q\alpha) + b(-q\beta) < d$$

A to sprzeczne z definicją d jako najmniejszego elementu zbioru A[4].
W identyczny sposób dowodzimy, że $d|b$.
Załóżmy teraz, że pewna liczba całkowita c dzieli zarówno a jak b. Wówczas c dzieli $d = \alpha a +' betab$, co kończy dowód faktu, że d jest największym wspólnym dzielnikiem a i b. ■

Zauważmy, że korzystając ze ciągu związków (1.2) oraz faktu, że r_k jest największym wspólnym dzielnikiem a i b, można w inny sposób udowodnić twierdzenie 1.4, co więcej, widać także, że algorytm Euklidesa pozwala efektywnie wyrazić $NWD(a, b)$ jako liniową kombinację liczb a i b.

Jeśli $\text{NWD}(a, b) = 1$, wówczas mówimy, że a **i** b **są względnie pierwsze** i piszemy $(a, b) = 1$ lub $a \perp b$.

Wniosek 1.5 *Liczby całkowite a i b są względnie pierwsze wtedy i tylko wtedy gdy istnieją $\alpha, \beta \in \mathbf{Z}$ takie, że*

$$\alpha a + \beta b = 1$$

Co więcej, α i β dadzą się znaleźć przy pomocy algorytmu Euklidesa.

[3] Za algorytm *szybki* uważa się taki, który kończy działanie po czasie ograniczonym przez funkcję wielomianową *wielkości problemu*. W naszym przypadku rozsądnym jest przyjąć, że wielkość problemu, to $|b|$.

[4] A ma element najmniejszy (jak nie widzisz dlaczego, pomyśl nad uzasadnieniem, to nietrudne!), nie musimy się więc tu zajmować *subtelną* różnicą pomiędzy elementem najmniejszym a minimalnym tego zbioru.

1.3 Grupy

Definicja 1.1 (Przypomnienie) *Zbiór G z działaniem łącznym $*$, posiadającym element neutralny w G i taki, że każdy element w G ma element odwrotny nazywamy* **grupą**.
O grupie G mówimy, że jest **przemienna** *(lub* **abelowa***) jeśli działanie $*$ jest przemienne.*

Przykłady.

Grupa S_X (permutacji zbioru X z działaniem składania funkcji).

$\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ itp z działaniem dodawania.

$\mathbf{Q}^+$ z działaniem mnożenia.

$\mathbf{Z}_n$ z działaniem dodawania modulo n.

$\mathbf{Z}_5^* = \mathbf{Z}_5 - \{0\}$ z działaniem mnożenia modulo 5.

Rozdział 2

Wykład 2. 12.X.2008

2.1 Grupy c.d.

Wcześij zauważyliśmy, że zbiór $\mathbf{Z}_5* = Z_5 - \{0\}$ z dziełaniem mnożenia (a dokładniej: z działaniem indukowanym w $\mathbf{Z}_5$ przez mnożenie w zbiorze $\mathbf{Z}$ jest grupą. Łatwo jednak zauważyć, że $\mathbf{Z}_8 - \{0\}$ już grupą multyplikatywną nie jest. Rzeczywiście, w zbiorze $\{1, 2, 3, 4, 5, 6, 7\}$ reszt z dzielenia przez 8 zachodzi $2 \cdot 4 \equiv 0 \pmod 8$, a stąd łatwo wynika, że ani 2 ani 4 nie mają ze względu na dzielenie elementów odwrotnych.
Stąd pytanie: czy można zbiór $\mathbf{Z}8$ tak zmodyfikować, czy można wyrzucić z niego pewną liczbę elementów, by to co zostało byó grupą? Odpowiedź na to pytanie jest pozytywna.

Twierdzenie 2.1 *Niech $n \in \mathbf{N}^*$ i niech $a \in \mathbf{Z}_n$. a jest elementem odwracalnym ze względu na działanie mnożenia w $\mathbf{Z}_n$ wtedy i tylko wtedy, gdy liczby a i n są względnie pierwsze.*

Przykład 2.1 $(\mathbf{Z}_{10}, \cdot)$ *oczywiście nie jest grupą (elementem neutralnym dla mnożenia jest 1, nie istnieje element odwrotny do elemwntu 2). Co więcej, także $(\mathbf{Z}'_{10}, \cdot)$, gdzie $\mathbf{Z}' = \mathbf{Z} - \{0\}$, nie jest grupą. Grupą przemienną natomiast jest $(\mathbf{Z}^*_{10}, \cdot)$, gdzie $\mathbf{Z}^*_{10} = \{1, 3, 7, 9\}$.*

Definicja 2.1 *Niech $n \in \mathbf{N}$. Definiujemy*

$$\mathbf{Z}^*_n = \{z \in \mathbf{Z}_n : a \perp n\}.$$

Twierdzenie 2.2 *Niech $n \in \mathbf{N}$. Wówczas $(\mathbf{Z}^*_n, \cdot)$ jest grupą przemienną.*

Dowód. Wobec twierdzenia 2.1 oraz faktu, że istnienie elementu nautralnego dla mnożenia (to oczywiście 1) oraz łączność mnożenia są do sprawdzenia bardzo łatwe, sprawdzimy tylko, że mnożenie jest rzeczywiście działaniem zamkniętym w $\mathbf{Z}^*_n$.

Niech $a, b \in \mathbf{Z}_n^*$. Wiemy, że wówczas istnieją takie całkowite liczby s, t, u oraz v, że

$$sa + tn = 1$$
$$ub + vn = 1$$

Stąd

$$1 = (su)ab + n\alpha$$

gdzie $\alpha = tub + tvn + sav$). Czyli, na mocy wniosku 1.5, $ab \perp n$ ■

2.2 Funkcja φ Eulera

Definicja 2.2 (Funkcja φ Eulera) *Niech $n \in \mathbf{N}$. Przez $\varphi(n)$ oznaczamy liczbę takich $a \in \mathbf{N}$, że $a \perp n = 1$ (a i n są względnie pierwsze). Funkcję $\varphi : \mathbf{N} \to \mathbf{N}$ nazywamy* **funkcją Eulera**.

Definicja 2.3 *Jeśli grupa G na skończoną liczbę elementów, wówczas mówimy, że G jest* **skończona** *a jej liczbę elementów nazywamy* **rzędem grupy** G.

Przykład 2.2 *Rząd $\mathbf{Z}_n$ jest równy n.*
Rząd $\mathbf{Z}^*$ jest równy 4.

Następne twierdzenie nie wymaga dowodu.

Twierdzenie 2.3 (O rzędzie $\mathbf{Z}_n^*$) *Dla każdej liczby naturalnej $n \geq 2$*

$$\varphi(n) = |\mathbf{Z}_n^*|.$$

Własności funkcji Eulera: Niech P będzie liczbą pierwszą. Wówczas

- $\varphi(p) = p - 1$,
- $\varphi(p^2) = p^2 - p$,
- $\varphi(p^n) = p^n - p^{n-1}$
- Jeśli także q jest pierwsze, to $\varphi(pq) = pq - p - q + 1 = (p-1)(q-1)$.

Twierdzenie 2.4 (Formuła Sita[1] lub Zasada Włączania i Wyłączania) *Niech*
$A_1, A_2, ..., A_n$ będą zbiorami skończonymi. Wówczas zachodzi wzór

$$|A_1 \cup A_2 \cup ... \cup A_n| = \sum_{1 \leq i_1 < i_2 < ... < i_k \leq n} (-1)^{k+1} |A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_k}|.$$

[1]Dokładniej: "sita Eratostenesa". Eratostenes, (276-194 p.n.e) był kustoszem Biblioteki Aleksandryjskiej i jednym z największych umysłów starożytności. Sito Eratostenesa służyło do "odsiewania" liczb pierwszych od "plew" innych liczb (por. twierdzenie 2.5 i wniosek 2.6). Jego innym, wielkim osiągnięciem była próba zmierzenia promienia Ziemi przez zmierzenie długości cieni rzucanych w południe przez dwie tyczki: jednej ustawionej w Aleksandrii, drugiej zaś w Syene (dzisiejszy Asuan). Wynik jaki otrzymał różnił sie tylko o 1% od nam znanego, a było to w czasach kiedy w kulistość Ziemi wierzył mało kto!

Formuła sita posłuży nam do wykazania następującego twierdzenia.

Twierdzenie 2.5 *Niech $n = p_1...p_t$, gdzie p_i są różnymi liczbami pierwszymi dla $i = 1, ..., t$. Wówczas*

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - ... \frac{n}{p_t} + \frac{n}{p_1 p_2} + ... + \frac{n}{p_{t-1} p_t} - \frac{n}{p_1 p_2 p_3} - ... - \frac{n}{p_{t-2} p_{t-1} p_t} + ... \pm \frac{(-1)^t n}{p_1 p_2 ... p_t}$$

$$= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) ... \left(1 - \frac{1}{p_t}\right)$$

Przykład 2.3 $\varphi(42) = \varphi(2 \cdot 3 \cdot 7) = 12$

Wniosek 2.6 *Wzór na φ z twierdzenia 2.5 pozostaje identyczny jeśli położymy $n = p_1^{a_1} \cdot ... \cdot p_t^{a_t}$ gdzie $p_1 < ... < p_t$ są liczbami pierwszymi, $a_1, ..., a_t \in \mathbf{N}$.*

2.3 Homorfizmy grup, grupy izomorficzne

$h : G_1 \to G_2$ jest *homomorfizmem* grupy $(G_1, *)$ w grupę $(G_2, \circ)$ jeśli $h(x * y) = h(x) \circ h(y)$ dla dowolnych $x, y \in G_1$.
Homomorfizm h jest:

- **monomorfizmem**, jeśli h jest injekcją,
- **epimorfizmem**, jeśli h jest surjekcją,
- **izomorfizmem**, jeśli h jest bijekcją.

W tym ostatnim przypadku mówimy, że grupy G i H są **izomorficzne**.

Przykład 2.4 *Grupy Kleina i $\mathbf{Z}_4$ (addytywna) nie są izomorficzne.*

2.4 Grupy cykliczne

Definicja 2.4 (Rząd elementu grupy) *Najmniejsze $n \in \mathbf{N}$ takie, że*

$$g^n = e \tag{2.1}$$

nazywamy **rzędem** *elementu g grupy, jeśli $n \in \mathbf{N}$ spełniające (2.1) nie istnieje, wówczas mówimy, że rzędem g jest ∞.*

Twierdzenie 2.7 *Jeśli grupa G jest skończona, $g \in G$, wówczas rząd elementu g jest skończony.*

Dowód. Rozważmy ciąg (nieskończony)

$$e = g^0, g^1, g^2, g^3, ...$$

Skoro zbiór G ma skończoną liczbę elementów, w ciągu tym pewne elementy muszą się powtarzać, to znaczy istnieją $k, n \in \mathbf{N}$ takie, że

$$g^k = g^n \tag{2.2}$$

dla $k \neq n$. Załóżmy, że $0 \leq k < n$ i na dodatek, że n jest najmniejszą liczbą naturalną. dla której spełniony jest związek (2.2), przy czym $0 \leq k < n$. Mnożąc obie strony (2.2) przez g^{-1} otrzymujemy

$$g^{k-1} = g^{n-1}$$

To stoi w sprzeczności z wyborem n jako najmniejszej liczby naturalnej, dla której zachodzi równość postaci (2.2) chyba, że $k = 0$. Wtedy jednak mamy $g^0 = g^n$ co oznacza, że n jest poszukiwanym rzędem elementu g. ■

Definicja 2.5 (Generator grupy, grupa cykliczna) *Mówimy, że element g jest* **generatorem** *grupy G z działaniem $*$, jeżeli każdy element grupy G można otrzymać jako wynik działania $*$ na elementach g i g^{-1}.*
Jeśli grupa zawiera generator, to nazywamy ją cykliczną.

Przykład 2.5 1 *(a także -1) jest generatorem grupy* $\mathbf{Z}$ *(addytywnej grupy liczb całkowitych).*
2 *jest generatorem (multyplikatywnej) grupy* $\mathbf{Z}_5^*$.

Przykład 2.6 *Grupa $(\mathbf{Z}_4, +)$ jest cykliczna, grupa Kleina nie.*

Rozdział 3

Wykład 3 - 19.X.2009

3.1 Grupy cykliczne - c.d.

Twierdzenie 3.1 *Jeżeli G jest multyplikatywną grupą skończoną, $g \in G$, wówczas istnieje $n \in \mathbf{N}$ takie, że $g^n = g^{-1}$*

Dowód. Na mocy twierdzenia 2.7 g ma rząd skończony, a więc istnieje $k \in \mathbf{N}$ takie, że $g^k = e$. Stąd wynika, że $g^{k-1} \cdot g = g \cdot g^{k-1} = e$, a więc, że $g^{-1} = g^{k-1}$ (gdzie k jest rzędem elementu g). ■

Twierdzenie 3.2 *Każda grupa cykliczna jest przemienna.*

Dowód. Rzeczywiście, przypuśćmy, że $a, b \in G$, gdzie G jest grupą cykliczną, geerowaną przez element $g \in G$. Wówczas istnieją takie $k, l \in \mathbf{Z}$, że $a = g^k, b = g^l$. Wobec tego

$$ab = g^k g^l = g^{k+l} = g^{l+k} = g^l g^k = ba$$

■

Definicja 3.1 *Jeśli grupa G na skończoną liczbę elementów, wówczas mówimy, że G jest* **skończona** *a jej liczbę elementów nazywamy* **rzędem grupy** *G.*

Twierdzenie 3.3 *Każda skończona grupa cykliczna G jest izomorficzna z $(\mathbf{Z}_n, +)$, gdzie n jest rzędem grupy G.* [1]

Dowód. ... ■

Podczas wykładu zapomniałem podać następującego twierdzenia (no to teraz musicie (?) go sami sobie udowodnić!).

[1] Inaczej: jedyną, z dokładnością do izomorfizmu, grupą skończoną o n elementach jest $(\mathbf{Z}_n, +)$.

Twierdzenie 3.4 *Każda nieskończona grupa cykliczna jest izomorficzna z* $(\mathbf{Z}; +)$.

Oczywiście stąd wynika, że każda grupa cykliczna jest przeliczalna (ale to w ogóle od razu *widać*.

3.2 Twierdzenia Cayleya i Lagrange'a

3.2.1 Podgrupy - przypomnienie

Niech $(G; *)$ będzie grupą, $H \subset G$. Jeśli $(H; *)$ (a dokładniej: $(H, *|_{H\times H})$) jest grupą, wówczas mówimy, że H jest podgrupą grupy G.
Jako ćwiczenia należy udowodnić następujące twierdzenie.

Twierdzenie 3.5 (Znane!) *Niech G będzie grupą z działaniem $*$. Niepusty podzbiór H zbioru G jest podgrupą wtedy i tylko wtedy, gdy dla dowolnych elementów $a, b \in H$ zachodzi $a * b^{-1} \in H$.*

Twierdzenie 3.6 *Jeśli w grupie skończonej G zbiór $S \neq \emptyset$ jest zamknięty ze względu na działanie grupowe $(*)$, to S stanowi podgrupę G.*

Dowód. ... ■

Twierdzenie 3.7 (Trudne) *Każda podgrupa grupy cyklicznej jest cykliczna.*

Dowód tego ostatniego można znaleźć stronie 154 *Przeglądu Algebry współczesnej* Birkhofa i MacLane'a.

3.2.2 Twierdzenie Cayleya

Definicja 3.2 (Grupa transformacji) *Dowolną podgrupę grupy permutacji $S(X)$ nazywamy* **grupą transformacji**.

Twierdzenie 3.8 (Tw. Cayleya) *Dowolna grupa jest izomorficzna z pewną grupą tranformacji.*

Dowód. ... ■

Przykład 3.1 *Grupa Kleina jest izomorficzna z podgrupą S_4 składającą się z następujących permutaci: $id_{\{1,2,3,4\}}; (1,2)(3,4); (1,4)(2,3); ((1,3)(2,4)$.*

3.2.3 Twierdzenie Lagrange'a

Twierdzenie 3.9 (Lagrange'a) *Niech H będzie podgrupą grupy skończonej G, $a = |H|, b = |G|$. Wówczas $a|b$.*

Definicja 3.3 (Przystawanie modulo półgrupa) *Niech H będzie podgrupą grupy G, $a, b \in G$. Mówimy, że a* **przystaje do** *b* **modulo** *H (piszemy $a \equiv b \ (mod\ H)$ lub aR_Hb) jeżeli $ab^{-1} \in H$.*

Lemat 3.10 *Jeżeli H jest podgrupą G wówczas relacja przystawania modulo H jest w G relacją równoważności.*

Dowód. ...

Lemat 3.11 *Niech G będzie dowolną grupą, zaś H jej podgrupą. Wówczas klasą elementu neutralnego grupy G modulo H jest zbiór H.*

Dowód. ...

Lemat 3.12 *Niech G będzie dowolną grupą, zaś H jej podgrupą. Wówczas klasą elementu $a \in G$ modulo H jest zbiór Ha.*

Dowód. ...

Lemat 3.13 *Niech G będzie dowolną grupą, zaś H jej podgrupą, $a \in G$. Wówczas klasa Ha jest równoliczna z H.*

Dowód. ...

Z łatwością stwierdzamy, że twierdzenie Lagrange'a wynika z powyszych lematów.

Rozdział 4

Wykład 4 - 26.X.2009

4.0.4 Wnioski z twierdzenia Lagrange'a

Wniosek 4.1 *Każdy element grupy skończonej G ma rząd będący dzielnikiem rzędu grupy G.*

Wniosek 4.2 *Jeśli rząd grupy G jest liczbą pierwszą, to G jest cykliczna.*

Wniosek 4.3 (stary) *Jedynymi grupami grupami rzędu 4 są $\mathbf{Z}_4$ i grupa Kleina.*

4.0.5 Twierdzenie Eulera i Małe Twierdzenie Fermata

Twierdzenie 4.4 (Eulera) *Jeśli liczby naturalne a, n są względnie pierwsze, wówczas*

$$a^{\varphi(n)} \equiv 1 \ (mod \ \ n)$$

Twierdzenie 4.5 (Małe Twierdzenie Fermata) *Jeśli p jest liczbą pierwszą, $a \in \mathbf{Z}$, to*

$$a^p \equiv a(\ mod\ p)$$

4.1 Ćwiczenia

1. Niech G będzie grupą. Wykaż, że podzbiór niepusty $H \subset G$ jest podgrupą G wtedy i tylko wtedy, gdy $\forall x, y \in H : xy^{-1} \in H$.
2. Wykaż że jeśli w grupie skończonej G zbiór $S \neq \emptyset$ jest zamknięty ze względu na działanie grupowe, wówczas S jest podgrupą.
3. Wykaż, że podgrupa grupy cyklicznej jest cykliczna.

4.2 Chińskie twierdzenie o resztach – równania modularne

Twierdzenie 4.6 *Równanie modularne*

$$ax \equiv 1 \ (mod\ n) \tag{4.1}$$

ma rozwiązanie wtedy i tylko wtedy gdy a i n są względnie pierwsze (oczywiście takie rozwiązanie jest jedyne w $\mathbf{Z_n}$ i jest postaci $x \equiv a^{-1}b\ (mod\ n)$, lub inaczej: $x = x_0 + kn$, gdzie $k \in \mathbf{Z_n}$, zaś x_0 jest równy $a^{-1}b$ przy czym a^{-1} jest el. odwrotnym do a w $\mathbf{Z}_n$ ze względu na mnożenie).

Uwaga. Sposobem znajdowania elementu odwrotnego do elementu a w $\mathbf{Z}_n$ jest skorzystanie z algorytmu Euklidesa. Jest to możliwe zawsze wtedy gdy taki element istnieje, a mianowicie gdy a i n są względnie pierwsze. Rzeczywiście, $a \perp n$ wtedy i tylko wtedy, jeśli istnieją s i t całkowite spełniające

$$sa + tn = 1$$

Wówczas $sa = 1 + (-t)n$, co oznacza, że s jest w $\mathbf{Z}_n$ elementem odwrotnym do a.

Twierdzenie 4.7 (Chińskie o resztach[1]) *Niech $a, b \in \mathbf{Z}$, $m, n \in \mathbf{N}$, $m \perp n$. Wówczas układ równań*

$$\begin{cases} x \equiv a & (\ mod\ m) \\ x \equiv b & (\ mod\ n) \end{cases} \tag{4.2}$$

ma rozwiązanie. Co więcej, każde dwa rozwiązania tego układu różnią się o wielokrotność mn (można też powiedzieć, że rozwiązanie jest jedyne modulo mn lub, że zbiór rozwiązań (4.2) jest postaci $\{x_0 + k(mn) | k \in \mathbf{Z}\}$).

Dowód. (Jedyności rozwiązania modulo mn.).[2] Przypuśćmy, że x_0 i x_1 są rozwiązaniami układu równań modularnych (4.2). Wówczas

$$\begin{aligned} x_0 &\equiv a \mod m \\ x_1 &\equiv a \mod m \end{aligned}$$

i wobec tego

$$\begin{aligned} x_0 - x_1 &\equiv 0 \mod m \\ x_0 - x_1 &\equiv 0 \mod n \end{aligned}$$

Ostatnie przystawania (modulo m i modulo n) oznaczają, że $m | x_0 - x_1$ oraz $n | x_0 - x_1$. Ponieważ jednak $m \perp n$, wynika stąd, że $mn | x_0 - x_1$ czyli, że $x_0 - x_1 \equiv 0$

[1] Twierdzenie to ukazało się po raz pierwszyl ok. 350 roku n.e. w książce Sun Tsu.

[2] Podczas wykładu udowodniłem, że rozwiązanie układu 4.7 istnieje. Powiedziałem także, że z dowodu istnienia w*w zasadzie* wynika także jedyność rozwiązania (modulo mn), jednak obiecałem tutaj podać dowód bardziej przekowywujący. Teraz wywiązuję się z tej obietnicy.

(mod mn) (naprawdę przekonywującego uzasadnienia ostatniej aplikacji dostarcza *zasadnicze twierdzenie arytmetyki*, o którym będzie mowa później) . ■

Zauważmy, że dowód Chińskiego Twierdzenia o Resztach zawiera algorytm rozwiązywania równań mdularnych. Warto także zwrrócić uwagę na fakt, że w metodzie tej ważną rolę odgrywa umiejętność znajdowania elementów odwrotnych modulo, a więcd i tym razem mamy tu zastosowanie algorytmu Euklidesa.

Twierdzenie 4.7 pozwala łatwo (indukcyjnie) udowodnić następujące uogólnienie chińskiego twierdzenia o resztach - o tym uogólnieniu podczas wykładu nie mówiłem!

Twierdzenie 4.8 *Niech $m_1, \ldots, m_k \in \mathbf{N}$ będą parami pierwsze (t.zn. $m_i \perp m_j$ dla $i \neq j$). Wówczas układ równań*

$$\begin{cases} x & \equiv & a_1 & (\ mod\ m_1) \\ x & \equiv & a_2 & (\ mod\ m_2) \\ & & \ldots & \\ x & \equiv & a_k & (\ mod\ m_k) \end{cases} \tag{4.3}$$

ma jednoznaczne rozwiązanie modulo $m_1 \cdot \ldots \cdot m_k$.

4.3 Działanie grupy na zbiorze

Definicja. Niech G będzie grupą multyplikatywną. Mówimy, że G **działa na zbiorze** X jeśli jest określone odwzorowanie $\varphi : G \times X \to X$ spełniające następujące dwa warunki (piszemy $g(x)$ zamiast $\varphi(g, x)$):

1. dla dowolnych $g_1, g_2 \in G$ oraz dla każdego $x \in X$ $(g_1 \cdot g_2)(x) = g_1(g_2(x))$
2. dla dowolnego $x \in X$ $e(x) = x$ (gdzie e jest elementem neutralnym grupy G).

Przykłady: grupa Kleina jako podgrupa permutacji na zbiorze $\{1, 2, 3, 4\}$. Grupa izomtrii ośmiościanu foremnego (jednej z pięciu *brył platońskich* - wszystkie te bryły można było podczas wykładu nie tylko zobaczyć, ale nawet dotknąć).

Twierdzenie 4.9 *Jeśli grupa G działa na zbiorze X, $g \in G$, to g jest bijekcją.*

Dla grupy G działającej na zbiorze X oraz el. $x \in X$ **stabilizatorem** x nazywamy

$$Stab\ x = \{g \in G : g(x) = x\}$$

Przykład ..

Twierdzenie 4.10 *Stabilizator dowolnego elementu $x \in X$ jest podgrupą grupy G.*

Orbitą elementu $x \in X$ nazywamy zbiór

$$Orb\ x = \{g(x) : g \in G\}$$

Relacja R określona przez

$$xRy \Longleftrightarrow \exists g \in G :\ g(x) = y$$

jest w X równoważnościowa.

Twierdzenie 4.11 *Jeśli skończona grupa G działa na zbiorze X, wówczas dla każdego $x \in X$*

$$|G| = |Stab\ x| \cdot |Orb\ x|$$

Dowód. (zostanie dokończony podczas wykładu następnego).

Rozdział 5

Wykład 5 - 9.XI.2010

5.1 Grupy - c.d.

Przykład 5.1 *Przyjrzeliśmy się grupie izometrii sześcianu, takich jednak. które można przeprowadzić na modelu, bez jego niszczenia. Wykorzystując twierdzenie 4.11 stwierdziliśmy, że grupa tych izometrii ma* 24 *elementy.*

Dowód twierdzenia 4.11 z poprzedniego wykładu.

Przykład 5.2 *Kontynuacja poprzedniego przykładu. Zauważamy, że wszystkich izometrii sześcianu jest* 48.

5.1.1 Lemat Burnside'a

Dla danej grupy G działającej na zbiorze X oraz $g \in G$ zbiór punktów stałych g oznaczamy przez $Fix\ g$:

$$Fix\ g = \{x \in X : g(x) = x\}$$

Twierdzenie 5.1 (Lemat Burnside'a) *Niech G będzie grupą skończoną działającą na zbiorze skończonym X. Wówczas liczba N orbit zbioru X ze względu na G wynosi*

$$N = \frac{1}{|G|} \sum_{g \in G} |Fix\ g|$$

Przykłady ...
Dowód (metodą podwójnego zliczania)...

Przykład 5.3 *Wykorzystaliśmy Lemat Burnside'a by stwierdzić, że są dokładnie dwa naszyjniki o pięciu perłach:* 2 *czarnych i* 3 *białych.*

5.1.2 Podgrupy normalne

Warstwy prawo- i lewostronne

Już wiemy (dowiedzieliśmy sie tego przy okazji dowodu twierdzenia Lagrange'a), że dla dowolnej podgrupy H grupy multyplikatywnej G relacja:

$$aRb \Longleftrightarrow ab^{-1} \in H \tag{5.1}$$

jest równoważnościowa. Klasą równoważności dowolnego elementu $a \in G$ dla tej relacji jest zbiór

$$Ha = \{ha | h \in H\}$$

zwany **warstwą prawostronną** elementu a.
Podobnie można zdefiniować **warstwę lewostronną** elementu a:

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

Z łatwością można sprawdzić, że warstwy lewostronne są klasami równoważności dla relacji (także równoważnościowej) L zdefiniowanej w G wzorem $aLb \Longleftrightarrow a^{-1}b \in H$ (gdzie H jest podgrupą G).

Przykład. Warstwy (lewo- i prawostronne) dla podgrupy $\{id, (12)\}$ grupy S_3 permutacji zbioru $\{1, 2, 3\}$.

Twierdzenie 5.2 *Jeśli grupa G jest przemienna, to dla dowolnej podgrupy H i $a \in G$*

$$aH = Ha$$

Definicja 5.1 *Mówimy, że podgrupa H grupy G jest* **normalna** *(lub* **niezmiennicza***), jeśli dla dowolnego $a \in G$ i dla dowolnego $b \in H$ zachodzi $aba^{-1} \in H$.*

Twierdzenie 5.3 *Podgrupa H grupy G jest normalna wtedy i tylko wtedy gdy dla każdego $a \in G$*

$$aH = Ha$$

Dowód. Rzeczywiście, przypuśćmy wpierw, że H jest podgrupą niezmienniczą grupy G, $a \in H$ i $x \in aH$. Skoro $x \in aH$, istnieje takie $d \in H$, że $x = ad$. Możemy wówczas napisać $x = ad(a^{-1}a) = (ada^{-1})a$. Ponieważ podgrupa H jest niezmiennicza, mamy $ada^{-1} \in H$, a wobec tego $x \in Ha$.
Wykazaliśmy więc, że $aH \subset Ha$. Faktu, że $Ha \subset aH$ dowodzimy analogicznie. Przypuśćmy teraz, że $aH = Ha$ dla dowolnego elementu $a \in G$. Wykażemy, że podgrupa H jest niezmiennicza.
Niech $b \in H$ i $a \in G$. Wówczas oczywiście $ab \in aH$, a ponieważ $aH = Ha$ zachodzi także $ab \in Ha$. Istnieje więc takie $c \in H$, że $ab = ca$. Stąd już natychmiast wynika, że $aba^{-1} = c \in H$, co kończy dowód. ■

Z twierdzenia 5.3 wynika, że jeżeli H jest podgrupą niezmienniczą grupy G, wówczas relacje, R i L zdefiniowane powyżej są identyczne. Zamiast pisać wtedy aRb czy też aLb będziemy pisać $a \overset{H}{\equiv} b$ (mówimy w takiej sytuacji, że **element** a **grupy** G **przystaje modulo** H **do elementu** b).

Twierdzenie 5.4 *Niech H będzie podgrupą grupy multyplikatywnej G. H jest podgrupą normalną wtedy i tylko wtedy gdy relacja R (zdefiniowana wzorem $aRb \Leftrightarrow ab^{-1} \in H$) jest zgodna z działaniem grupowym grupy G.*

Dowód. Przypuśćmy, że H jest podgrupą normalną grupy G, $a \overset{H}{\equiv} b$ oraz $c \overset{H}{\equiv} d$. Wówczas istnieją takie α i β, że $ab^{-1} = \alpha \in H$ i $cd^{-1} = \beta \in H$. Stąd zaś łatwo wynika, że $ac = \alpha(b\beta b^{-1})bd$. Skoro $\beta \in H$ i H jest podgrupą niezmienniczą, zachodzi $b\beta b^{-1} \in H$. Mamy więc $(ac)(bd)^{-1} = \alpha(b\beta b^{-1}) \in H$, co oznacza, że $ac \overset{H}{\equiv} bd$ a więc udowodniliśmy, że relacja przystawania modulo podgrupa niezmiennicza H jest zgodna z działaniem grupowym w G.
Załóżmy teraz, że relacja R jest zgodna z działaniem grupowym. Skorzystamy z twierdzenia 5.3 by wykazać, że podgrupa H jest niemiennicza.
Niech $b \in Ha$. Wówczas aRb (na mocy twierdzenia 5.3). Wiemy także, że $a^{-1}Ra$. Ze zgodności R z działaniem grupowym wynika, że $(a^{-1}a)R(a^{-1}b)$, czyli $eR(a^{-1}b)$. Stąd zaś łatwo wywnioskować, że $a^{-1}b \in H$ i wobec tego $b \in aH$. Dowód wynika teraz z twierdzenia 5.3. ■

Rozdział 6

Wykład 6 - 16.XI.2010

6.1 Grupy - c.d.

6.1.1 Grupy ilorazowe

Jeśli H jest podgrupą normalną grupy G wówczas w zbiorze G/H można wprowadzić dzieałanie wzorem

$$Ha \cdot Hb = Hab \tag{6.1}$$

Twierdzenie 6.1 *Jeśli H jest podgrupą normalną grupy G, to G/H (z działaniem zdefiniowanym wzorem $Ha \cdot Hb = Hab$) jest grupą (zwaną* **grupą ilorazową***).*

Dowód. ...

Twierdzenie 6.2 *Dla dowolnego morfizmu grup $f : G \to H$ zbiór $Ker\ f = f^{-1}(\{e_H\})$ jest podgrupą normalną grupy G.*

Dowód. ...

Twierdzenie 6.3 (O morfiźmie grup) *Jeśli $f : G \to H$ jest morfizmem grup, to grupa ilorazowa $G/Ker\ f$ jest izomorficzna z $Im\ f$.*
Dokładniej: jeśli oznaczymy przez $k : G \to G/Ker\ f$ **morfizm kanoniczny** *dany wzorem $k(g) = (Ker\ f)g$, zaś przez $h : G/Ker\ f \to Im\ f$ odwzorowanie zadane wzorem $h((Ker\ f)a) = f(a)$, to h jest izomorfizmem grup i zachodzi wzór $f = h \circ k$.*

Dowód. ...

6.2 Zasady kryptografii z kluczem publicznym

Wyobraźmy sobie, że mamy trzy osoby: Alicję, Boba i Ewę. Alicja chce przesłać Bobowi pewne informacje tak, by Ewa (ani nikt inny poza Bobem) nie mógł

odgadnąć ich treści mimo, że informacje te przekazywane są w sposób jawny[1]. Warto w tym miejscu zdać sobie sprawę, że każdą informację można traktować jako liczbę. Standardowym zapisem jest powszechnie znany kod ASCII który można z łatwością zdobyć, na przykład za pomocą internetu (w kodzie tym każdemu znakowi odpowiada 3-cyfrowa liczba, *a* to 097, spacja to 032, *o* to 111 itd). Kod ASCII ma jednak oczywistą wadę: wszyscy go znają, a w każdym razie wiedzą jak sie w niego zaopatrzyć. Tak więc Alicja i Bob będą musieli przesyłane dane zaszyfrować (funkcję szyfrującą oznaczać będziemy przez E[2], na dodatek wychodząc z założenia, że wszystkie przesyłane wiadomości są podsłuchiwane (przez Ewę).

Powiedzmy, że Alicja chce zaszyfrować i następnie przesłać Bobowi liczbę naturalną l. By osiągnąć swój cel, Alicja i Bob będą postępowali według następującego schematu:

1	Bob znajduje funkcję szyfrującą (szyfrującą) E oraz dekodującą D, a więc takie by $D(E(l)) = l$
2	Bob przesyła tekstem otwartym (Ewa widzi przekaz) funkcję E Alicji
3	Alicja koduje informację którą chce przesłać Bobowi według otrzymanej przez niego instrukcji (tę instrukcje zna także Ewa). Inaczej mówiąc Alicja oblicza wartość $m = E(l)$
4	Alicja wysyła Bobowi m (Ewa oczywiście także widzi przesyłaną informację)
5	Bob liczy $D(m)$ i poznaje treść przesyłki Alicji

Wydaje się, że znalezienie w tej sytuacji skutecznej metody szyfrowania chroniącej przesyłane informacje przed niezdrową[3] ciekawością Ewy będzie bardzo trudne. Okazuje się, że taka metoda istnieje, choć opiera się na bardzo, na pozór, kruchej podstawie. Tą podstawą jest przekonanie (hipoteza), że nie istnieje skuteczna metoda faktoryzacji liczb naturalnych. Rzeczywiście, choć pomnożenie *ręcznie*, a więc bez użycia komputera dwóch dużych, powiedzmy o 500 pozycjach dziesiętnych liczb, wydaje się czynnością kłopotliwą, wymagającą dużej ilości czasu i papieru, dla komputera jest proste i odbywa się w mgnieniu oka, dając w rezultacie liczbę o 1000 miejscach dziesiętnych. Nawet naszemu domowemu komputerowi taka czynność zajmie mniej niż sekundę. Jeśli jednak odwrócimy zagadnienie, czyli jeśli otrzymamy 1000-pozycyjną liczbę $n = pq$, gdzie p i q są nieznanymi nam liczbami pierwszymi, i zadanie nasze będzie polegało na znalezieniu p i q, to będziemy musieli wykonać liczbę dzieleń (prób) rzędu 10^{500}, co nawet najszybszemu komputerowi zajmie niewyobrażalną ilość

[1] *Rozszyfrujmy* kilka spraw. Dlaczego Alicja, Bob i Ewa? To proste. Alicja, bo na literę A, Bob bo na literę B, E bo po angielsku *podsłuchiwacz* to *eavesdropper* (a więc na literę E, jak Ewa (*Eve*)). Rozsądnie jest także założyć, że wszystkie przesyłane informacje mogą być śledzone. Czyż nie tak jest gdy wyjmujemy pieniądze z bankomatu lub, w jeszcze większym stopniu, gdy płacimy za zakupy dokonywane za pośrednictwem internetu?

[2] E od angielskiego *encoding*

[3] A przede wszystkiem niebezpieczną dla Alicji i Boba!

czasu[4]. Na dodatek, gdyby wynaleziono komputery o wiele szybsze niż znane do tej pory, wystarczy zwiększyć liczbę cyfr znaczących n z 1000 do 2000 by liczba operacji potrzebnych do znalezienia faktoryzacji wzrosła 10^{1000} krotnie.

Poniżej pokażemy w jaki sposób rozważania na temat złożoności obliczeniowej mnożenia i znajdowania rozkładu liczb na czynniki pierwsze mogą być przydatne w kryptografii.

6.2.1 Metoda Rabina

Metodę szyfrowania Rabina[5] można opisać następująco. Niech n będzie ustaloną, wystarczająco dużą, powiedzmy 300-cyfrową liczbą (okaże się, że celem uniknięcia zniekształcenia informacji l w procesie szyfrowania n musi być dobrane tak, by $l < n$). Funkcją kodującą jest

$$E(l) = l^2 (\bmod n)$$

Oznacza to tyle, że Bob prześle Alicji liczbę n i funkcję kodującą. Alicja obliczy $l^2 \pmod n$, prześle tę informacje Bobowi. Ewa, podsłuchiwaczka, będzie znała zarówno l^2 jak i n, a jednak, z powodów opisanych wyżej, nie będzie w stanie obliczyć l. Zauważmy. że tak świetnie liczące pierwiastki kalkulatory (czy komputery) są w tej sytuacji zupełnie bezużyteczne. Na przykład gdybyśmy obliczyli przy pomocy kalkulatora $\sqrt{10}$ to otrzymalibyśmy 3.1621..., co nijak ma się do pierwiastka z 10 (mod 13) (dwie liczby dają w kwadracie 10 (mod 13), mianowicie 6 i 7). Jak to jednak możliwe, że Bob będzie w stanie zrobić to, czego nie jest w stanie uczynić Ewa, to znaczy obliczyć l?

Nim jednak przejdziemy do szczegółowego omówienia metody musimy poznać pewne wiadomości dotyczące residuów kwadratowych.

Kwadratowe residua i pierwiastki modulo

Niech $n \in \mathbf{N}, a \in \mathbf{Z}_n$. Mówimy, że a jest **kwadratowym residuum modulo** n, jeżeli istnieje $b \in \mathbf{Z}_n$ takie, że $a = b^2 \pmod n$.

Przykłady: residua w grupie w grupie $\mathbf{Z}_2 1$. Zaobserwowaliśmy fakt, że skoro zdarza się, że w $\mathbf{Z}_n$ jedno residuum jest kwadratem więcej niż jednego elementu, są także takie elementy $\mathbf{Z}_n$, które nie są residuami.

Zauważmy, że jeśli $b^2 \equiv a \pmod n$ wówczas:

$$(n-b)^2 = n^2 - 2nb + b^2 \equiv b^2 \equiv a \pmod n$$

Wniosek std taki, że jeśli b jest pierwiastkiem kwadratowym modulo n z a, wówczas także $-b \pmod n$ także $n - b$ (czyli $-b \pmod n$) jest pierwiastkiem modulo n z a. Jeśli n jest liczbą pierwszą, wówczas sytuacja jest zupełnie jasna.

[4]Sam sprawdź. Przyjmij, że jedno dzielenie wymaga 1 mikrosekundy, a dla ułatwienia obliczeń, że minuta ma 100 sekund, doba 100 godzin, rok 1000 dni.

[5]Nazwa od twórcy metody: Michaela Rabina

Twierdzenie 6.4 *Niech p będzie liczbą pierwszą i niech $a \in \mathbf{Z}_p$. Wówczas a ma dokładnie dwa pierwiastki kwadratowe w $\mathbf{Z}_p$.*

Dowód. Przypuśćmy, że x i y są dwoma różnym pierwiastkami kwadratowymi z a w $\mathbf{Z}_p$, przy czym $y \not\equiv -x \pmod{p}$. Mamy więc

$$y \not\equiv x \text{ oraz } y \not\equiv -x \pmod{p}$$

a wobec tego

$$x - y \not\equiv 0 \text{ oraz } x + y \not\equiv 0 \pmod{p}$$

Otrzymujemy więc $(x - y)(x + y) = x^2 - y^2 \equiv a - a = 0 \pmod{p}$. To zaś jest sprzeczne z faktem, że w $\mathbf{Z}_p$ (dla p pierwszego) iloczyn dwóch elementów różnych od zera jest także różny od zera. Tak więc nie istnieje element $y \in Z_p$, różny od x i od $-x \pmod{p}$, który jest kwadratowym pierwiastkiem z a. ■

Rozdział 7

Wykład 7 - 23.XI.2010

7.1 Zasady kryptografii z kluczem publicznym c.d.

Kwadratowe residua i piewiastki modulo c.d.

Twierdzenie 7.1 *Niech $p \in \mathbf{N}$ będzie liczbą pierwszą, $p \equiv 3$ (mod 4) i niech a będzie residuum kwadratowym w $\mathbf{Z}_p$. Wówczas pierwiastkami kwadratowymi a w $\mathbf{Z}_p$ są $a^{\frac{p+1}{4}}$ (mod p) oraz $-a^{\frac{p+1}{4}}$ (mod p).*

Opis metody Rabina

1. Bob wybiera dwie duże liczby pierwsze p i q takie, by $p \equiv q \equiv 3 \pmod 4$. Następnie oblicza $n = pq$ i przesyła Alicji (a wszystko to podgląda Ewa).

2. Alicja konwertuje swoją wiadomość w kodzie ASCII otrzymując liczbę l i oblicza $m = l^2 \pmod n$. Następnie przesyła Bobowi m. Ewa widzi m, zna już n, nie umie jednak obliczyć p i q, bo to jest właśnie trudny problem faktoryzacji.

3. Bob znajduje pierwiastki z m obliczając wpierw $a = m^{\frac{p+1}{4}} \pmod p$, $b = -m^{\frac{p+1}{4}} \pmod p$, $c = m^{\frac{q+1}{4}} \pmod q$ oraz $d = -m^{\frac{q+1}{4}} \pmod q$, a następnie rozwiązując cztery układy równań modularnych:

$$\begin{cases} x \equiv a \pmod p \\ x \equiv c \pmod q \end{cases} \quad \begin{cases} x \equiv a \pmod p \\ x \equiv d \pmod q \end{cases}$$

$$\begin{cases} x \equiv b \pmod p \\ x \equiv c \pmod q \end{cases} \quad \begin{cases} x \equiv b \pmod p \\ x \equiv d \pmod q \end{cases}$$

Układy równań modularnych mają jednoznaczne rozwiązania modulo $n = pq$ dzięki lematowi chińskiemu. Otrzymamy więc aż cztery rozwiazania, choć wiemy, że dobre jest tylko jedno z nich. To jednak, by wśród rozwiązań odróżnić

właściwe będzie dla Boba bardzo proste. Po przejściu z kodu ASCII na litery otrzyma jedną wiadomość sensowną i trzy ciągi znaków nie mających sensu.

Na pierwszy rzut oka może się wydawać, że metoda liczenia pierwiastków wykorzystująca twierdzenie 7.1 nie jest zbyt efektywna. Należy przecież liczyć bardzo wysokie potęgi. Na szczęście okazuje się, ż celem obliczenia k-tej potęgi liczby b wystarczy wykonać liczbę mnożeń, która jest proporcjonalna nie do k a do $\log k$. Przyjrzyjmy się tej sytuacji na przykładzie.

Przykład 7.1

7.1.1 Metoda RSA

O ile metoda Rabina wykorzystuje Małe Twierdzenie Fermata, to metoda RSA[1] opiera się na twierdzeniu Eulera. Podobnie jak to było w przypadku opisu metody Rabina załóżmy, że Alicja chce przesłać Bobowi zaszyfrowaną informację $l \in \mathbf{N}$.

Opis metody RSA.

1. Bob:
   (a) Znajduje 2 duże liczby pierwsze p, q, liczy $n = pq$ oraz $\varphi(n) = (p-1)(q-1)$ (także w tym przypadku zakładamy, że $n \geq l$).
   (b) Wybiera (dowolne) $e \in \mathbf{Z}^*_{\varphi(n)}$ (a więc e jest względnie pierwsze z $\varphi(n)$).
   (c) Przesyła Alicji n i e
   (d) Oblicza $d = e^{-1}$ w $\mathbf{Z}^*_{\varphi(n)}$.
2. Ewa: Widzi! Widzi zarówno n jak i e. Wie także jaka jest funkcja szyfrująca.
3. Alicja:
   (a) Liczy $m = l^e \pmod n$
   (b) Wysyła m Bobowi.

Bob: Liczy

$$m^d = (l^e)^d \equiv l \pmod n \tag{7.1}$$

Prawdziwo wzoru 7.1 wymaga uzasadnienia. Oto one.

(a) Przypadek: $l \perp n$. Skoro $ed \equiv 1 \pmod{\varphi(n)}$ mamy: $ed = 1 + k\varphi(n)$ (gdzie n jest pewną liczbą całkowitą. Wówczas

$$l^{ed} = l^{1+k\varphi(n)} = l(l^{\varphi(n)})^k \equiv l(\bmod n)$$

[1]Nazwa metody od pierwszych liter nazwisk jej twórców: Rivest, Shamir i Adleman.

(b) Przypadek: l i n nie są względnie pierwsze. Wtedy albo $p|l$ albo $q|l$ (gdyby $p|l$ i $q|l$ to mielibyśmy sprzeczność z założeniem, że $l < n$. Załóżmy, że $p|l$ oraz $q \not| l$.

Mamy teraz: $l^{ed} = l^{1+k(p-1)(q-1)} = l(l^{q-1})^{k(p-1)}$. Ale $q \perp l$ (bo q jest liczbą pierwszą i q nie dzieli l). Wiemy że, $\varphi(q) = q - 1$. A więc $l^{ed} \equiv l \cdot 1^{k(p-1)} = l \pmod q$.

Ostatecznie otrzymaliśmy

$$l^{ed} \equiv l \ (mod\ q)$$

Mamy także

$$l^{ed} \equiv l \ (mod\ p)$$

(bo $l \equiv 0 \pmod p$). Z chińskiego twierdzenia o resztach l jest jedynym modulo $n = pq$ rozwiązaniem układu równań

$$l \equiv m^d \ (mod\ q)$$

$$l \equiv m^d \ (mod\ p)$$

7.2 Pierścienie

W definicji pierścienia, którą podajemy poniżej, stosujemy powszechnie znaną ze zbiorów liczbowych ($\mathbf{R}, \mathbf{N}, \mathbf{Z}$ etc) konwencję nie pisania znaku działania $\cdot$ (inaczej: działania multyplikatywnego), o ile tylko nie prowadzi to do nieporozumień. W wyrażeniach postaci $(ab)+c$ opuszczamy nawias i piszemy $ab+c$, co oznacza, że jeśli nie ma nawiasu, to stosujemy regułę pierwszeństwa *mnożenia* przed *dodawaniem* (właściwie powinniśmy powiedzieć: *pierwszeństwa działania multyplikatywnego* (to znaczy: oznaczanego przez $\cdot$) *przed działaniem addytywnym* (to znaczy: oznaczanym przez $+$)).
Będziemy pisać $a - b$ zamiast $a + (-b)$.

Definicja 7.1 *Zbiór P z dwoma działaniami $+$ (dodawania) oraz $\cdot$ (mnożenia) nazywamy pierścieniem jeśli:*

- *P z działaniem dodawania jest grupą przemienną,*
- *działanie mnożenia jest łączne,*
- *dla dowolnych elementów $a, b, c \in P$: $a(b + c) = ab + ac$ oraz $(a + b)c = ac + bc$ (rozdzielność mnożenia względem dodawania)*

Element neutralny dla działania $+$ pierścienia P nazywamy **zerem** *pierścienia (i najczęściej oznaczamy przez 0).*

Jeśli działanie $\cdot$ jest przemienne to P nazywamy **pierścieniem przemiennym**.

Jeśli $ab = 0 \Rightarrow a = 0$ lub $b = 0$ to P jest **pierścieniem bez dzielników zera**.

Jeśli zaś w P istnieje taki element $1 \in P$, że dla dowolnego $x \in P$ zachodzi: $1x = x1 = x$ to P nazywamy **pierścieniem z jedynką** *(a element 1* **jedynką** *pierścienia P).*
Pierścień przemienny z jedynką i bez dzielników zera nazywamy **pierścieniem całkowitym**.

Pierścien całkowity P w którym każdy element różny od zera ma element odwrotny ze względu na mnożenie[2] *nazywamy* **ciałem**. *(Tego akurat odczas wykładu nie powiedziałem, ale wiecie to skąd inąd!)*

Twierdzenie 7.2 *Pierścień P jest bez dzielników zera wtedy i tylko wtedy dla dowolnych elementów spełniony jest warunek:*

$$\forall a,b,c \in P,\ c \neq 0 \begin{cases} ac = bc & \Rightarrow \quad a = b \\ ca = cb & \Rightarrow \quad a = b \end{cases} \qquad (\text{ prawa skracania}) \qquad (7.2)$$

Dowód. Przypuśćmy wpierw, że w pierścieniu P spełniony jest warunek (7.2) oraz, że dla pewnych $a, b \in P$ zachodzi $ab = 0$. Wówczas mamy ciąg implikacji: $ab = 0 \Rightarrow ab = a0 \Rightarrow ab - a0 = 0 \Rightarrow a(b-0) = 0 \Rightarrow a(b-0) = a0$. Z ostatniej równości oraz z drugiej z implikacji warunku (7.2) wynika, że jeśli $a \neq 0$, wówczas $b - 0 = 0$, a więc $b = 0$.
Przypuśćmy teraz, że pierścień P jest bez dzielników zera. Wówczas, dla dowolnego $c \in P, c \neq 0$ prawdziwe są implikacje $ac = bc \Rightarrow ac - bc = 0 \Rightarrow ac + (-b)c = 0 \Rightarrow (a + (-b))c = 0 \Rightarrow a + (-b) = 0 \Rightarrow a = b$. Podobnie dowodzimy prawa lewostronnego skracania. ■

7.2.1 Przykłady pierścieni

Z pewnością najlepiej znanymi pierścienimi są zbiory liczbowe: liczb całkowitych, wymiernych, rzeczywistych i zespolonych ze zdefiniowanymi w znany sposób działaniami dodawania zczególną rolę w teorii pierścieni odgrywa pierścień liczb całkowitych.
Z łatwością można sprawdzić, że poniższe zbiory ze wskazanymi w nich działaniami są pierścieniami.

- Zbiór macierzy $\mathbf{R}^{n\times n}$, (o n wierszach i n kolumnach), z działaniami określonymi w zwykły sposób.
- Łatwo sprawdzić, że w zbiorze liczb całkowitych $\mathbf{Z}$ relacja *przystawania modulo n* zdefiniowana przez

  $$a \equiv b \pmod{n} \iff n | b - a$$

  jest zgodna z działaniami dodawania i mnożenia w $\mathbf{Z}$. Można więc zdefiniować działania indukowane dodawania i mnożenia w zbiorze klas $\mathbf{Z}/(\mathrm{mod}\ n)$. Nietrudno także wykazać, że z tymi działaniami $\mathbf{Z}/(\mathrm{mod}\ n)$ jest pierścieniem (z jedynką, bez dzielników zera wtedy i tylko wtedy gdy n jest liczbą pierwszą).

[2] Inaczej: dla każdego $a \in P, a \neq 0$ istnieje $a' \in P$ taki, że $aa' = 1$.

- Niech P będzie pierścieniem przemiennym. Zbiór $\{\sum_{i=0}^{\infty} a_i \mathbf{x}^i | a_i \in P\}$ nazywamy zbiorem **szeregów formalnych** Łatwo można wykazać (**ćwiczenie!**), że zbiór ten tworzy pierścień !

- Pierścień **wielomianów** $P[\mathbf{x}]$ o współczynnikach w pierścieniu P to zbiór szeregów formalnych, w których skończona liczba współczynników jest różna od zera.
  Inaczej: oznaczmy przez $\mathbf{x}^i = (\underbrace{0, ..., 0}_{i\ zer}, 1, \underbrace{0, ...}_{zera})$. Zdefiniujmy mnożenie naszych $\mathbf{x}$-ów wzorem $\mathbf{x}^i \mathbf{x}^j = \mathbf{x}^{i+j}$. Wówczas, jak to łatwo można udowodnić[3], zbiór szeregów foralnych o skończonej liczbie współczynników ! różnych od zera z działaniami określonymi wzorami:
  - $(\sum_{i=0}^{\infty} a_i \mathbf{x}^i) + (\sum_{i=0}^{\infty} b_i \mathbf{x}^i) = \sum_{i=0}^{\infty} (a_i + b_i) \mathbf{x}^i$
  - $(\sum_{i=0}^{\infty} a_i \mathbf{x}^i) \cdot (\sum_{j=0}^{\infty} b_j \mathbf{x}^j) = \sum_{l=0}^{\infty} c_l \mathbf{x}^l$, gdzie $c_l = \sum_{k=0}^{l} a_k b_{l-k}$ jest pierścieniem przemiennym (z jedynką, o ile w P jest jedynka).

7.3 Podpierścienie

Podpierścieniem pierścienia P nazywamy dowolny podzbiór $A \subset P$, $A \neq \emptyset$ jeśli A wraz z działaniami + i $\cdot$ (zacieśnionymi do zbioru A) jest pierścieniem.

Twierdzenie 7.3 *Niech P będzie pierścieniem. $A \subset P$, $A \neq \emptyset$. A jest podpierścieniem P wtedy i tylko wtedy, gdy*

1. $\forall a, b \in A\ a - b \in A$,
2. $\forall a, b \in A\ ab \in A$.

7.4 Zadania

Zadanie 1 Sprawdź, że zbiory:

- $\mathbf{Z} < \sqrt{-1} >= \{a + ib | a, b \in \mathbf{Z}\}$
- $\mathbf{Z} < \sqrt{3} >= \{a + \sqrt{3}b | a, b \in \mathbf{Z}\}$

z działaniami dodawania i mnożenia w zbiorze liczb zespolonych lub rzeczywistych, są pierścieniami. Podaj przykłady innych, podobnie skonstruowanych pierścieni.

Zadanie 2 W pierścieniu P oznaczmy przez P' zbiór dzielników zera pierścienia P. Sprawdź, że w zbiorze $P - P'$ mnożenie jest działaniem.
Zbadaj własności mnożenia w $P - P'$ dla pierścienia $\mathbf{Z}/(\mathrm{mod}\ 6)$

[3] W domu lub podczas ćwiczeń!

Zadanie 3 Element a pierścienia P nazywamy **nilpotentnym**, jeżeli istnieje liczba całkowita l taka, że $a^p = 0$. Jeśli dodatkowo zachodzi $a^{l-1} \neq 0$, to l nazywamy **rzędem** elementu nilpotentnego $a \neq 0$. Rzędem elementu nilpotentnego 0 jest z definicji 1.
Co można powiedzieć o elementach nilpotentnych w pierścieniu całkowitym?
Zbadaj elementy nilpotentne pierścienia $\mathbf{Z}/(\text{ mod } 12)$.
Wykaż, że suma i iloczyn elementów nilpotentnych jest nilpotenna. Co można powiedzieć o ich rzędzie (nilpotencji)?

Zadanie 4 W przykładzie pierścieni $\mathbf{Z}/mod(n)$ wystąpiły sformułowania *łatwo sprawdzić* i *nietrudno wykazać*. Sprawdź więc i wykaż. Przyjrzyj się pierścieniom $\mathbf{Z}/mod(6)$ i $\mathbf{Z}/mod(7)$ (wypisz elementy tych pierścieni, utwórz tabelki ziałań, wskaż dzielniki zera (o ile istnieją)).

7.4.1 Ideały

Definicja 7.2 *Niech P będzie pierścieniem, $I \subset P, I \neq \emptyset$. Mówimy, że I jest* **ideałem** *pierścienia P jeśli spełnione są następujące dwa warunki:*

1. $a, b \in P \Rightarrow a - b \in P$
2. $\alpha \in P, a \in I \Rightarrow \alpha a \in I, a\alpha \in I$

Przykład 7.2 *W dowolnym pierścieniu P zbiory $\{0\}$ i P są ideałami.*

Przykład 7.3 W dowolnym pierścieniu przemiennym P, dla dowolnego $a \in P$, zbiór $(a) = \{\alpha a | \alpha \in P\}$ jest ideałem. Ideały tej postaci nazywać będziemy **ideałami głównymi** . W takiej sytuacji mówimy też, że ideał główny (a) jest **generowany** przez element a.

Rozdział 8

Wykład 8 - 30.XI.2010

8.1 Pierścienie c.d.

8.1.1 Pierścienie główne

Definicja 8.1 *Pierścień P nazywamy* **pierścieniem głównym** *jeżeli każdy jego ideał jest ideałem głównym.*

Najlepiej znanym przykładem pierścienia głównego jest pierścień liczb całkowitych.

Twierdzenie 8.1 *Pierścień liczb całkowitych* $\mathbf{Z}$ *jest pierścieniem głównym.*

Dowód. Ideał zerowy $\{0\}$ jest oczywiście ideałem głównym generowanym przez 0. Przypuśćmy, że A jest ideałem w $\mathbf{Z}$, $A \neq \{0\}$. Zauważmy, że do A należy co najmniej jedna liczba dodatnia. Rzeczywiście, skoro $A \neq \{0\}$, w A jest jakaś liczba $a \neq 0$. Wobec tego także $-a \in A$ (wiemy, że 0 jest w dowolnym ideale, a zatem i $0 - a = a \in A$), zaś jedna z liczb: a lub $-a$ jest dodatnia.
Niech teraz a_0 będzie najmniejszą liczbą dodatnią w A. Oczywiście A zawiera wszystkie wielokrotności liczby a, a więc $A \supset (a)$. Wystarczy więc wykazać, że $A \subset (a)$.
Na mocy twierdzenia o dzieleniu z resztą w zbiorze liczb całkowitych, istnieją $q, r \in \mathbf{Z}$ spełniające

$$b = qa + r, \qquad 0 \leq r < a$$

$r = b - qa$, a więc $r \in A$, a ponieważ a jest najmniejszym dodatnim elementem A, mamy $r = 0$ i w konsekwencji $a|b$. ■

8.1.2 Więcej o pierścieniach wielomianów

Dla wielomianu $v = v_0 + v_1 x + \ldots \in P[x]$ największe k_0 dla którego $v_{k_0} \neq 0$ nazywamy **stopniem wielomianu** v i oznaczmy przez $\partial(v)$. Stopniem wielomianu

zerowego jest $-\infty$[1]. Współczynnik v_{k_0} nazywamy wtedy **współczynnikiem dominującym** wielomianu v.

Z łatwością można sprawdzić, prawdziwość następujących dwóch twierdzeń.

Twierdzenie 8.2 *Dla dowolnego pierścienia P zbiór $P[x]$ jest pierścieniem. Jeśli P jest pierścieniem całkowitym, wówczas także $P[x]$ jest pierścieniem całkowitym.* ■

Twierdzenie 8.3 *Dla dowolnego pierścienia P i wielomianów $v, w \in P[x]$ zachodzą wzory:*

$$\partial(v+w) \leq \max\{\partial v, \partial w\}$$

$$\partial(vw) \leq \partial v + \partial w$$

Co więcej, druga z tych nierówności jest równością o ile P jest pierścieniem (przemiennym) bez dzielników zera. ■

Zauważmy, że z każdym wielomianem $w \in P[x]$, $w = w_0 + w_1 x + \ldots + w_n x^n$ można skojarzyć **funkcję wielomianową**:

$$w : P \ni x \to w(x) = w_0 + w_1 x + \ldots + w_n x^n \in P$$

Zbiór funkcji wielomianowych o współczynnikach w pierścieniu P oznaczamy przez $P(x)$. Jest oczywiste, że także $P(x)$ jest pierścieniem (przemiennym jeśli P jest przemienny, całkowitym, jeśli P jest całkowity).

8.1.3 Podzielność w pierścieniach

Definicja 8.2 *Niech P będzie pierścieniem całkowitym, $a, b \in P$. Mówimy, że a* **dzieli** *b jeżeli istnieje $c \in P$ takie, że $b = ac$. Piszemy wówczas $a|b$.*
Jeśli $a|b$ i $b|a$ to elementy a i b nazywamy **stowarzyszonymi**.

Przykłady...

Definicja 8.3 *Elementy stowarzyszone z 1 (jedynką pierścienia) nazywamy* **jednościami pierścienia**.

Twierdzenie 8.4 *Zbiór jedności pierścienia P tworzy grupę (multyplikatywną). (Grupę tę nazywamy* **grupą jedności pierścienia**).

Przykłady.

[1]Zauważmy, że wielomian zerowy $v = 0$ nie ma współczynnika $v_{k_0} \neq 0$. Można więc postąpić na dwa sposoby: albo nie definiować w ogóle stopnia wielomianu zerowego, albo zdefiniować go jako $-\infty$ i definiując $a + -\infty = 0$, $\max\{a, -\infty\} = a$, dla dowolnego $a \in \mathbf{Z}$, by wzory na stopień sumy i iloczynu wielomianów pozostały prawdziwe (sprawdź, że rzeczywiście tak jest!).

1. Zbiór $\{-1, 1\}$ jest zbiorem jedności w pierścieniu liczb całkowitych.

2. W pierścieniu $\mathbf{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbf{Z}\}$ (sprawdź, że to pierścień!) prawdziwy jest wzór
$$(2 - \sqrt{3})(2 + \sqrt{3}) = 1$$
Stąd
$$(2 - \sqrt{3})^k (2 + \sqrt{3})^k = 1$$
dla dowolnego k naturalnego. A więc w pierścieniu $\mathbf{Z}[\sqrt{3}]$ zbiór jedności jest nieskończony.

Każde przedstawienie elementu a pierścienia P w postaci

$$a = a_1 \cdot \ldots \cdot a_n \tag{8.1}$$

nazywamy **rozkładem na czynniki**. O rozkładzie 8.1 mówimy, że jest **właściwy**, jeśli

1. $n \geq 2$,

2. żaden z czynników $a_1, \ldots, a_n$ nie jest jednością.

Jeśli żaden właściwy rozkład elementu a nie istnieje, wówczas mówimy, że a jest **nierozkładalny**.

Element a pierścienia P nazywamy **pierwszym**, jeżeli zachodzi implikacja:

$$a|bc \Rightarrow a|b \text{ lub } a|c$$

Wbrew temu co pamiętamy ze szkoły, pojęcia elementów nierozkładalnych i pierwszych są różne, choć *całkowite liczby* nierozkładalne i pierwsze to jednak to samo. Poniższe twierdzenie podaje relację zawierania pomiędzy zbiorami elementów pierwszych i nierozkładalnych dowolnego pierścienia całkowitego.

Twierdzenie 8.5 *W dowolnym pierścieniu całkowitym P, każdy element pierwszy jest nierozkładalny.*

Dowód. Niech $a \in P$ będzie elementem pierwszym pierścieni całkowitego P. Przypuśćmy, że istnieje rozkład a, czyli

$$a = a_1 \cdot \ldots \cdot a_k \tag{8.2}$$

dla pewnego $k \geq 2$. Wówczas istnieje $i \in \{1, \ldots, k\}$ takie, że $a|a_i$. Ponieważ (na mocy (8.2)) $a_i|a$, elementy a oraz a_i są stowarzyszone.
Wykażemy teraz, że jeśli dwa elementy x, y są stowarzyszone w pierścieniu całkowitym P, powiedzmy $x|y$ i $y|x$, wówczas $x = yz$, gdzie z jest jednością.
Rzeczywiście,
$$\left.\begin{array}{ll} x|y \Rightarrow & \exists z \in P : \quad y = zx \\ y|x \Rightarrow & \exists t \in P : \quad x = ty \end{array}\right\} \Rightarrow y = zty$$

Stąd i z faktu, że P jest pierścieniem całkowitym (a więc z jedynką i prawem skracania) wnioskujemy łatwo, że $zt = 1$, czyli, że z i t są stowarzyszone z jedynką, czyli jednościami pierścienia P.
Odnosząc te rozważania do a i a_i otrzymujemy $a = a_1 \cdot \ldots \cdot a_{i-1}a_{i+1} \cdot \ldots \cdot a_k a_i = a_i z$, przy czym z jest jednością. Korzystając z przemienności i ponownie z prawa skracania otrzymujemy, że $a_1 \cdot \ldots \cdot a_{i-1}a_{i+1} \cdot \ldots \cdot a_k = z$, a więc, jak łatwo zauważyć, także $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k$ są jednościami, co kończy dowód. ■

Bardzo znanym przykładem na to, że twierdzenie odwrotne do twierdzenia 8.5 nie jest prawdziwe, jest **pierścień Dedekinda** $\mathbf{Z} < \sqrt{5}i >= \{a+bi\sqrt{5} | a, b \in \mathbf{Z}\}$.
Wykażemy wpierw, że liczba 2 jest elementem nierozkładalnym pierścienia Dedekinda. rzeczywiście,

$$2 = (a + bi\sqrt{5})(c + di\sqrt{5})$$

daje układ równań

$$\begin{aligned} ac - 5bd &= 2 \\ bcd + ad &= 0 \end{aligned}$$

Traktując ten układ jako układ o niewiadomych c i d otrzymamy

$$c = \frac{2a}{a^2 + 5b^2} \qquad d = \frac{-2b}{a^2 + b^2}$$

(zauważmy, że a i b nie mogą być równocześnie równe zero).
Ponieważ c i d są całkowite, zachodzi $a^2 + 5b^2 \leq 2|a|$ (lub $a = 0$). Stąd

$$|a| \leq 2$$

i wobec tego

$$a \in \{0, -1, 1, -2, 2\}$$

- Gdyby $a = 0$ wówczas mielibyśmy $ac = 0$ i w konsekwencji $2 = -5bd$, co dla całkowitych b i d jest niemożliwe.
- Gdyby $a = 1$ mielibyśmy $c = \frac{2}{1+5b^2}$, a więc $b = 0$ i w konsekwencji $c = 2$ i $d = 0$. Nasz rozkład byłby więc z konieczności postaci $2 = 1 \cdot 2$, a więc nie byłby rozkładem właściwym (jeden z czynników jest jednością).
- Gdyby $a = 2$ wówczas mielibyśmy $c = \frac{4}{4+5b^2}$ a stąd wnioskujemy łatwo, że $b = 0, c = 1, d = 0$ i wobec tego $2 = 2 \cdot 1$ – sprzeczność z przypuszczeniem, że rozkład liczby 2 (w $\mathbf{Z} < \sqrt{5}i >$) jest właściwy.
- Podobnie jak powyżej sprawdzamy, że a nie może być równe ani -1 ani -2.

Zauważmy teraz, że

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

Wobec tego $2|6$. Łatwo także sprawdzić, że 2 nie dzieli ani $1 + \sqrt{5}$ ani $1 - \sqrt{5}$. Sprawdziliśmy, że w pierścieniu Dedekinda $\mathbf{Z} < \sqrt{-5} >$ liczba 2 jest elementem nierozkładalnym, który nie jest elementem pierwszym.

Rozdział 9

Wykład 9 - 7.XII.2010

9.1 Pierścienie c.d. c.d.

9.1.1 Pierścienie Gaussa

Definicja 9.1 *Pierścień P nazywamy* **pierścieniem z rozkładem** *jeżeli każdy, nie będący jednością pierścienia P, element $a \in P$ da się przedstawić jako iloczyn skończonej liczby elementów nierozkładalnych w P.*
Dwa rozkłady elementu a:

$$a = a_1 \cdot ... \cdot a_m \quad a = b_1 \cdot ... \cdot b_n$$

nazywamy **jednakowymi** *jeżeli*

1. $m = n$,
2. *istnieje permutacja $\sigma : [1, m] \to [1, m]$ taka, że elementy a_i oraz $b_{\sigma(i)}$ są stowarzyszone.*

Pierścień całkowity P nazywamy **pierścieniem Gaussa** [1] *jeśli każdy nie będący jednością element pierścienia P ma rozkład jednoznaczny (tzn. ma rozkład na iloczyn elementów nierozkładalnych i każde dwa rozkłady dowolnego elementu na iloczyn elementów nierozkładalnych są jednakowe).*

Przykład 9.1 $\mathbf{Z}$*, $K[x]$ - gdzie K jest dowolnym ciałem, są pierścieniami Gaussa (dowód tych faktów będzie nieco później).*
Pierścień Dedekinda nie jest pierścieniem Gaussa (np. rozkład liczby 6 w tym pierścieniu nie jest jednoznaczny: $6 = 3 \cdot 2 = (1 + \sqrt{-5})((1 - \sqrt{-5}))$*.*

Twierdzenie 9.1 *Pierścień całkowity z rozkładem P jest pierścieniem Gaussa wtedy i tylko wtedy gdy każdy element nierozkładalny $a \in P$ jest w P elementem pierwszym.*

[1] Carl Friedrich Gauss 1777-1855

Dowód. ...

Uwaga. Pierścień Dedekinda $\mathbf{Z}[\sqrt{-5}]$ nie jest pierścieniem Gaussa. W tym pierścieniu element 6 ma dwa różna rozkłady na czynniki nierozkładalne.

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-1})$$

9.1.2 Powrót do wielomianów

Twierdzenie 9.2 *Niech P będzie pierścieniem całkowitym i niech $p \in P[x]$ będzie wielomianem którego współczynnik dominujący jest odwracalny. Dla każdego wielomianu $v \in P[x]$ istnieją wielomiany $q, r \in P[x]$ takie, że*

$$v = qp + r, \quad \partial r < \partial p \text{ lub } r = 0 \tag{9.1}$$

Wielomiany q i r o tych własnościach wyznaczone są jednoznacznie.

Dowód. Wykażemy wpierw istnienie wielomianów p oraz r.
Oznaczmy przez k stopień wielomianu v i przez m stopień wielomianu p. Dowód poprowadzimy przez indukcję ze względu na k.
Twierdzenie jest prawdziwe dla $k < m$. Rzeczywiście, wówczas $v = 0p + v$, $k = \deg v < \deg p = m$.
Przypuśćmy, że $k \geq m$ a także, że jeśli $v^* \in P[x]$ jest wielomianem stopnia $k' < k$ wówczas istnieją wielomiany q^* oraz r^* takie, że $v^* = q^*p + r^*$, $\deg r^* < \deg p$ lub $r = 0$.
Oznaczmy przez v_k i p_m współczynniki dominujące wielomianów v i p. Z założenia element p_m jest odwracalny. Wielomian $\bar{v} = v - v_k p_m^{-1} x^{k-m} p$ jest stopnia mniejszego od k. Z założenia indukcyjnego istnieją więc wielomiany $\bar{q}$ oraz r takie, że $\bar{v} = \bar{q}p + r$, $\deg r < \deg p$ lub $r = 0$. Wówczas $v - v_k p_m^{-1} x^{k-m} p = \bar{q}p + r$, a zatem $v = (v_k p_m^{-1} x^{k-m} + \bar{q})p + r$, co kończy dowód istnienia wielomianów q i r.

Pozostaje wykazać jedyność wielomianów q i r spełniających warunki (9.1). Przypuśćmy, że

$$v = qp + r$$

oraz

$$v = \bar{q}p + \bar{r}$$

przy czym $\partial r < \partial p$ lub $r = 0$ i $\partial \bar{r} < \partial p$ lub $\bar{r} = 0$. Wówczas $r - \bar{r} = (\bar{q} - q)p$, $\partial(r - \bar{r}) < \partial p$ lub $r - \bar{r} = 0$. Stąd już łatwo wywnioskować, że $\bar{q} = q$ i $r = \bar{r}$. ■

Wniosek 9.3 *Niech P będzie pierścieniem z jedynką. Reszta z dzielenia wielomianu $v \in P[x]$ przez wielomian $x - c$ jest równa $v(c)$.*

Dowód. Na mocy twierdzenia o dzieleniu wielomianów możemy napisać

$$v = q(x - c) + r$$

gdzie deg $r = 0$ lub $r = 0$. Wówczas $v(c) = q(c)(c - c) + r(c)$, co oznacza, że $r(c) = v(c)$. ponieważ zaś wielomian r może mieć jedynie współczynnik r_0 różny od zera (mówimy, że r *jest stały*), $r_0 = v(c)$. ■

Element c pierścienia P nazywamy **pierwiastkiem wielomianu** $v \in P[x]$ jeśli $v(c) = 0$.
Niech $v \in P[x]$, gdzie P jest pewnym pierścieniem całkowitym, $x = q(x - c) + r$, gdzie r jest wielomianem stopnia zero. Z wniosku 9.3 wynika, że c jest pierwiastkiem wielomianu v wtedy i tylko wtedy, gdy $x - c$ dzieli v. Zapiszmy to spostrzeżenie

Wniosek 9.4 *Niech P będzie pierścieniem całkowitym. Wielomian $v \in P[x]$ jest podzielny przez wielomian $x - c$ wtedy i tylko wtedy, gdy c jest pierwiastkiem wielomianu v.* ■

Z wniosku 9.4 bardzo łatwo można wykazać jeszcze jeden, bardzo ważny wniosek.

Wniosek 9.5 *Niech P będzie pierścieniem całkowitym. Dowolny wielomian $v \in P[x]$ stopnia k ma co najwyżej k pierwiastków.* ■

Twierdzenie 9.6 *Pierścień wielomianów $\mathbf{K}[x]$ nad dowolnym ciałem $\mathbf{K}$ jest pierścieniem głównym.*

Dowód. Niech B będzie ideałem pierścienia $\mathbf{K}[x]$. Jeśli $B = \{0\}$, to B jest oczywiście ideałem głównym, $B = (0)$. Przypuśćmy więc, że $B \neq \{0\}$. Wtedy w B są wielomiany niezerowe. Niech d będzie wielomianem niezerowym, minimalnego stopnia w B. Wykażemy, że $B = (d)$. W tym celu wystarczy wykazać, że dla dowolnego $b \in B$ istnieje $q \in \mathbf{K}[x]$ takie, że $b = qd$.

Z twierdzenia o dzieleniu wielomianów (twierdzenie 9.2) wynika, że istnieją takie wielomiany $q, r \in \mathbf{K}[x]$, że

$$b = qd + r \quad \deg r < \deg d$$

Stąd $r = b - qd \in B$. Jednak w ideale B jedynym wielomianem stopnia silnie mniejszego niż deg d jest wielomian $r = 0$, a więc $b = qd$, co należało udowodnić. ■

9.1.3 Jeszcze o pierścieniach głównych

Już niebawem okaże się, że bardzo ważną własnością pierścieni głównych jest, że dowolny wstępujący ciąg ideałów pierścienia głównego jest stacjonarny. Tę własność wykażemy w następnym twierdzeniu.

Twierdzenie 9.7 *W pierścieniu głównym P każdy wstępujący ciąg ideałów*

$$C_1 \subset C_2 \subset \ldots \subset C_k \subset \ldots$$

jest stacjonarny, tzn. istnieje $k_0 \in \mathbf{N}$ takie, że

$$C_{k_0} = C_{k_0+1} = \ldots$$

Dowód. Suma ideałów $C = \bigcup_{i=1}^{\infty} C_i$ iest ideałem (por. zad. **??**). Ponieważ P jest pierścieniem głównym, istnieje $a \in P$ takie, że $C = (a)$. Oczywiście $a \in C$, a więc istnieje $k_0 \in \mathbf{N}$ takie, że $a \in C_{k_0}$.
Z definicji C (jako mnogościowej sumy C_I, $i \in \mathbf{N}$): $C_{k_0} \subset C$. Z drugieje strony, skoro $a \in C_{k_0}$, to z definicji ideału $(a) \subset C_{k_0}$, a więc $C \subset C_{k_0}$ i ostatecznie: $C = C_{k_0}$. ■

Największym wspólnym dzielnikiem elementów a i b pierścienia całkowitego P nazywamy element $d \in P$ spełniający warunek:

$$d|a,\ d|b \quad \text{oraz dla każdego } c \in P: \quad c|a, c|b \Rightarrow c|d$$

Największy wspólny dzielnik elementów a i b oznaczamy przez NWD(a, b) lub, częściej, przez (a, b).

Jeżeli największym wspólnym dzielnikiem elementów a i b jest jedynka pierścienia (inaczej: jeżeli $(a, b) = 1$), wówczas mówimy, że a i b są **względnie pierwsze**. Wówczas jedynymi wspólnymi dzielnikami a i b są 1 i elementy stowarzyszone z 1 (a więc, elementy odwracalne pierścienia). Zamiast pisać $(a, b) = 1$ często piszemy $a \perp b$.

W pierścieniach głónych największy wspólny dzielnik dwóch elementów zawsze istnieje i można go zapisać w specjalnej postaci. Twierdzenie które o tym mówi nazwiemy **twierdzeniem o NWD w pierścieniu głównym**.

Twierdzenie 9.8 *Każde dwa elementy a, b pierścienia głównego P mają największy wspólny dzielnik $d \in P$ który jest ich kombinacją liniową, tzn. istnieją $s, t \in P$ takie, że*

$$d = sa + tb$$

Dowód będzie na wykładzie następnym.

Rozdział 10

Wykład 10 - 17.XII.2010

10.1 Pierścienie c.d. c.d.

10.1.1 Pierścienie główne c.d.

Zgodnie z obietnicą, zacznijmy od dowodu twierdzenia 9.8.

Dowód. Rozważmy zbiór

$$S = \{s_1 a + t_1 b | s_1, t_1 \in P\}$$

Sprawdźmy wpeirw, że S jest ideałem. Rzeczywiście, jeżeli $s, t \in S$ wówczas istniej w P elementy $\alpha_1, \alpha_2, \beta_1, \beta_2$ takie, że $s = \alpha_1 a + \beta_1 b$ oraz $t = \alpha_2 a + \beta_2 b$ i wobec tego

$$s - t = (\alpha_1 + \alpha_2)a + (\beta_1 + \beta_2)b \in S$$

Dla dowolnego $c \in P$ zachodzi

$$cs = c(\alpha_1 a + \beta_1 b) = (c\alpha_1)a + (c\beta_1)b \in S$$

Ponieważ z założenia P jest pierścieniem głównym, ideał S jest główny, a więc istnieje $d \in P$ takie, że $S = (d)$. Element a można zapisać w postaci $a = 1a + 0b$, a więc $a \in S$. Podobnie wykazujemy, że $b \in S$. Stąd wynika pczywiście, że $d|a$ oraz $d|b$.
Jeśli $c|a$ i $c|b$ wtedy istnieją $\alpha, \beta \in P$ takie że $a = \alpha c$ oraz $b = \beta c$. Wówczas

$$d = sa + tb = s\alpha c + t\beta c = (a\alpha + t\beta)c$$

i wobec tego $c|d$. ■

Jeżeli największym wspólnym dzielnikiem elementów a i b jest jedynka pierścienia (inaczej: jeżeli $(a, b) = 1$), wówczas mówimy, że a i b są **względnie pierwsze**. Wówczas jedynymi wspólnymi dzielnikami a i b są 1 i elementy stowarzyszone z 1 (a więc, elementy odwracalne pierścienia). Zamiast pisać $(a, b) = 1$ często piszemy $a \perp b$.

10.2 Pierścienie euklidesowe

Definicja 10.1 *Pierścień całkowity P nazywamy* **euklidesowym** *jeśli istnieje funkcja $h : P^* \to \mathbf{N}^+$ taka, że dla wszystkich $a \in P, b \in P^*$ istnieją $q, r \in P$ takie, że*

1. $a = bq + r$
2. *oraz albo $r = 0$ albo $h(r) < h(b)$.*

Przykłady.

1. $\mathbf{Z}$ z funkcją $h(n) = |n|$
2. $K[x]$ gdzie Kjest pewnym ciałem, z funkcją $h(v) = 2^{\partial(v)}$
3. $\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}$ zaś $h(a + bi) = a^2 + b^2$
   Wykażemy, że funkcja h tak zdefiniowana rzeczywiście spełnia postulaty definicji pierścienia euklidesowego.
   Niech $a+bi \in \mathbf{Z}[i]$ i niech $c+di \in \mathbf{Z}[i]^*$. Oczywiście $\frac{a+bi}{c+di} = e+fi$, gdzie e i f są liczbami wymiernymi (żeby to zobaczyć wystarczy wymnożyć licznik i mianownik wyrażenia $\frac{a+bi}{c+di}$ przez $c-di$ i wykonać dzielenie). Wybierzmy teraz e_0 oraz f_0 tak, by $|e - e_0| \leq \frac{1}{2}$ i $|f - f_0| \leq \frac{1}{2}$.
   Przyjrzyjmy się liczbie

$$r = a + bi - (c + di)(e_0 + f_0 i)$$

   Oczywiście $a + bi = (c + di)(e_0 + f_0 i) + r$. Pozostaje więc wykazać, że $h(r) < |c + di|^2$.

$$h(r)| = |r|^2 = |a + bi - (c + di)(e_0 + f_0 i)|^2 =$$

$$= |(c + di)(e + fi) - (c + di)(e_0 + f_0 i)|^2 \leq |c + di|^2 |e + fi - e_0 - f_0 i|^2 =$$

$$= |c + di|^2((e - e_0)^2 + (f - f_0)^2) \leq |c + di|^2(\frac{1}{4} + \frac{1}{4}) < |c + di|^2 = h(c + di)$$

Twierdzenie 10.1 *Każdy pierścień euklidesowy jest pierścieniem głównym.*

Dow. ...

W pierścieniach euklidesowych funkcjonuje algorytm Euklidesa podobny do tego, który znamy dla liczb całkowitych.

ALGORYTM EUKLIDESOWY W PIERŚCIENIU EUKLIDESOWYM

Niech P będzie pierścieniem euklidesowym, $a, b \in P$.
Określmy rekurencyjnie następujący ciąg (r_i).

- $r_0 = a, r_1 = b$
- $r_i = q_{i+1}r_{i+1} + r_{i+2}$ gdzie $h(r_{i+2}) < h(r_{i+1})$

Oczywiście mamy wtedy $h(r_1) < h(r_2) < ...$, a ponieważ funkcja h na mocy definicji (pierścienia euklidesowego) przyjmuje wartości naturalne, ciąg (r_i) jest skończony. Powiedzmy, że ostatnim niezerowym wyrazem ciągu (r_i) jest r_k (oznacza to, że $r_{k+1} = 0$ i r_{k+1} jest ostatnim wyrazem ciągu (r_i)). Mamy wtedy równość $r_{k-1} = q_k r_k$.
Zauważmy także, że z równości

$$r_i = q_{i+1}r_{i+1} + r_{i+2}$$

wynika, że

- jeśli jakiś element $d \in P$ dzieli r_i oraz r_{i+1} wówczas d dzieli r_{i+2}
- jeśli $d \in P$ dzieli r_{i+1} oraz r_{i+2} wówczas d dzieli r_i

Stąd łatwo wywnioskować, że $r_r = NWD(r_{k-1}, r_{k-2}) = ... = NWD(r_1, r_0) = NWD(a, b)$.
Co więcej, korzystając z ciągu równości $r_i = q_{i+1}r_{i+1} + r_{i+2}$ łatwo wyliczyć wartość $r_k = NWD(a, b)$.

10.3 Zasadnicze Twierdzenie Arytmetyki

Następujące twierdzenie nazywa się Zasadniczym Twierdzeniem Arytmetyki (lub Twierdzeniem o Jednoznacznej Faktoryzacji).

Twierdzenie 10.2 *Każdy pierścień główny jest pierścieniem Gaussa.*

Dow. ...

Oczywiście, skoro każdy pierścień euklidesowy jest pierścieniem głównym, prawdziwy jest następujący wniosek.

Wniosek 10.3 *Każdy pierścień Euklidesa jest pierścieniem Gaussa.*

10.4 Ciało ułamków pierścienia całkowitego

Zakładam podstawową wiedzę n.t. ciał. Przypomnijmy więc tylko krótko, że ciałem (przemiennym) nazywamy zbiór F wyposażony w dwa działania, addytywne i multyplikatywne, który

- jest pierścieniem całkowitym oraz
- każdy element $a \in F$ różny od zera ma element odwrotnny ze względu na działanie oznaczone multyplikatywnie (a więc istnieje $a^{-1} \in F$ takie, że $a \cdot a^{-1} = 1$).

Podczas wykładu przypomnieliśmy sobie definicję podciała oraz warunek konieczny i wystarczający, by podzbiór ciała był podciałem.
Niech P będzie pierścieniem całkowitym, $P^* = P - \{0\}$. wzbiorze $Q = P \times P^*$ zdefiniujmy dwa działania:

$$(a, b) + (c, d) = (ad + bc, bd) \tag{10.1}$$

$$(a, b) \cdot (c, d) = (ac, bd) \tag{10.2}$$

oraz relację R:

$$(a, b)R(c, d) \iff ad = bc \tag{10.3}$$

Twierdzenie 10.4 *Dla dowolnego pierścienia całkowitego P relacja R zdefiniowana przez 10.3 jest relacją równoważności zgodną z działaniami 10.1 i 10.2.*

Dzięki twierdzeniu 10.4 w zbiorze ilorazowym $P \times P^*/R$ można wprowadzić działania dodawania i mnożenia:

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)] \tag{10.4}$$

$$[(a, b)] \cdot [(c, d)] = [(ac, bd)] \tag{10.5}$$

Twierdzenie 10.5 (O ciele ułamków) *Dla dowolnego pierścienia całkowitego P zbiór $P \times P^*/R$ z działaniami zdefiniowanymi wzorami 10.4 i 10.5 jest ciałem przemiennym.*

Ciało występujące w tezie twierdzenia 10.5 nazywamy **ciałem ułamków** pierścienia P. Z oczywistch powodów będziemy raczej stosowali zapis $\frac{a}{b}$ zamiast $[(a, b)]$ dla elemntów ciała ułamków.

Rozdział 11

Wykład 11 - 21.XII.2010

11.1 Pierścienie ilorazowe

Twierdzenie 11.1 *Niech P będzie pierścieniem, a $D \subset P$ jego podpierścieniem. Relacja R_D zdefiniowana w D wzorem*

$$aR_Db \iff a - b \in D$$

jest relacją równoważności w D.

Dow. ... Ćwiczenie!

Zbiór klas równoważności P/R_D nazywamy **ilorazem pierścienia P przez podpierścień D i oznaczamy przez P/D.**

Twierdzenie 11.2 *W dowolnym pierścieniu P i dla dowolnego podpierścienia $D \subset P$ relacja R_D jest zgodna z działaniami pierścienia wtedy i tylko wtedy, gdy D jest ideałem pierścienia P.*

Dow. ... Ćwiczenie!

Z faktu, że w przypadku gdy I jest ideałem pierścienia P, relacja R_I jest zgodna z działaniami pierścienia, pozwala w ilorazie P/I wprowadzić działania wzorami

$$[a]_{R_I} + [b]_{R_I} = [a + b]_{R_I}$$
$$[a]_{R_I} \cdot [b]_{R_I} = [ab]_{R_I}$$

gdzie $[c]_{R_I}$ oznacza klasę równoważności elementu $c \in P$ względem relacji R_I. Przyjrzyjmy się tym klasom. Dla dowolnego elementu $a \in P$ mamy

$$[a]_{R_I} = \{b \in P : b - a \in I\}$$

Stąd klasa $[a]_{R_I}$ równa jest zbiorowi tych elementów $b \in P$ dla których istnieje element $c \in I$ taki, że $b = a + c$. Taki zbiór zapisujemy $[a]_{R_I} = a + I$. Teraz wzory na działania w $P?I$ przyjmują postaci

$$(a + I) + (b + I) = a + b + I$$

oraz

$$(a+I)(b+I) = ab+I$$

Łatwo zaobserwować, że I jest w P/I elementem neutralnym ze względu na dodawanie.

Twierdzenie 11.3 (O ilorazie pierścienia przez ideał) *Jeśli I jest ideałem pierścienia P, to P/I jest pierścieniem (przemiennym, jeśli P jest przemienny, z jedynką, jeśli P jest z jedynką).*

Dow. ... Ćwiczenie

Zauważmy, że zerem pierścienia P/I jest I. Jeśli P jest pierścieniem, zaś I jego ideałem, wówczas pierścień P/I nazywamy **pierścieniem ilorazowym**.

11.2 Homomorfizmy pierścieni

Odwzorowanie $h : P \to Q$ pierścienia P w pierścień Q jest **homomorfizmem** jeśli spełnia warunki

1. $h(a+b) = h(a) + h(b)$
2. $h(ab) = h(a)h(b)$

dla dowolnych $a, b \in P$. $Im\ h = h(P)$ nazywamy **obrazem** zaś $Ker\ h = h^{-1}[0]$ **jądrem** homomorfizmu h.

Twierdzenie 11.4 *1. Obraz homomorfizmu pierścieni $h : P \to Q$ jest podpierścieniem pierścienia Q.*

2. Jądro homomorfizmu pierścieni $h : P \to Q$ jest ideałem pierścienia P.

Twierdzenie 11.5 *Jeśli P jest pierściniem a I jego ideałem, wówczas odwzorowanie $k : P \to P/I$ zdefiniowane wzorem*

$$k(a) = a + I$$

jest homomorfizmem (zwanym **homomorfizmem kanonicznym***).*

Twierdzenie 11.6 *Dla dowolnych pierścieni P, Q homomorfizm pierścieni $h : P \to Q$ jest monomorfizmem wtedy i tylko wtedy, gdy $Ker\ h = \{0\}$.*

Dow. Ćwiczenie!

Twierdzenie 11.7 (Podstawowe o izomorfiźmie pierścieni) *Jeśli $h : P \to Q$ jest epimorfizmem pierścienia na pierścień Q, wówczas zachodzi wzór*

$$h = \tilde{h} \circ k$$

gdzie $k : P \to P/Ker\ h$ jest homomorfizmem kanonicznym, zaś $\tilde{h} : P/Ker\ h \to Q$ izomorfizmem przyporządkowującym każdej klasie elementów $P/Ker\ h$ ich wspólną wartość w homomorfiźmie k.

Dow. ...

Twierdzenie 11.7 można wypowiedzieć inaczej tak: *każdy epimorfizm pierścieni można przedstawić jako złożenie homomorfizmu kanonicznego i pewnego izomorfizmu.*

11.3 Wielomiany nieprzywiedlne

Niech v będzie wielomianem o wspczynnikach w pewnym pierścieniu całkowitym P. Taki wielomian można w dość oczywisty sposób traktować jako wielomian nad ciałem ułamków F pierścienia P. Można sformułować pytanie, kiedy element $\frac{a}{b}$ ciała F może być pierwiastkiem v?. Okazuje się, że jeśli P jest pierścieniem Gaussa odpowiedź na to tytanie jest taka, jak w znanym zeszkoły średniej twierdzeniu dotyczącym wielomianów o współczynnikach całkowitych.

Twierdzenie 11.8 *Jeśli element $\frac{a}{b}$ ciała ułamków F pierścienia Gaussa P jest pierwiastkiem wielomianu*

$$P[x] \ni v = a_0 + a_1 x + \cdots + a_n x^n$$

stopnia n, wówczas a dzieli a_0 i b dzieli a_n.

Dow. ...

Bardzo często zamiast mówić, że wielomian jest nierozkładalny mówimy, że jest **nieprzywiedlny**. Kryterium Eisensteina[1] bardzo ważnym, często stosowanym warunkiem wystarczającym nieprzywiedlności wielomianów nad pierścieniem Gaussa.

Twierdzenie 11.9 *Niech P będzie pierścieniem Gaussa, $p \in P[x]$, $p = a_0 + a_1 x + \cdots + a_n x^n$. Jeśli istnieje element pierwszy a w P taki, że*

1. $a | a_0,\ a | a_1,\ \ldots, a | a_{n-1}$,
2. $a \not| a_n$,
3. $a^2 \not| a_0$

[1]Ferdinand Eisenstein (1823-1852) jest postacią ze wszech miar godną uwagi. Pochodził z bardzo skromnej rodziny, był pochodzenia żydowskiego. Wiele zawdzięczał Aleksandrowi von Humboldtowi, który odkrył jego talent i pomagał mu w karierze. W roku 1844 dwudziestojednoletni Eisenstein opublikował 23 artykuły naukowe i rok pźniej otrzymał honorowy doktorat Uniwersytetu we Wrocławiu (jeszcze przed tem nim uzyskał habilitacje, w wieku lat 24 w Berlinie). Był członkiem Akademii Getyndze i w Berlinie. Gauss miał o nim powiedzieć, że *było tylko trzech matematyków o epokowym znaczeniu: Archimedes, Newton i Eisenstein.* No cóż, w końcu jednak wyszło na to, że to jednak wyniki Gaussa przetrwały i wpłynęły na rozwój nauki, przede wszystkim zaś matematyki w znacznie większym stopniu. Choć porównywanie tu nie bardzo ma jakikolwiek sens.

wówczas p jest nierozkładalny[2] *w P (a co za tym idzie, także w F - ciele ułamków pierścienia P).*

Dowód. Twierdzenie udowodnimy metodą nie wprost. Przypuśćmy, że istnieją wielomiany $b_0 + b_1x + \cdots + b_kx^k$ oraz $c_0 + c_1x + \cdots + c_lx^l$ w $P[x]$. Wówczas

$$a_0 = b_0c_0$$

Ponieważ $a|a_0$ i a jest elementem pierwszym, a dzieli jeden z elementów b_0, c_0. Co więcej, a nie moż dzielić zarówno b_0 jak i c_0, w przeciwnym bowiem przypadku a dzieliłoby a_0^2. Bez straty ogólności możemy założyć, że $a|b_0$ i $a \not| c_0$.
Oczywiście $a_1 = b_0c_1 + b_1c_0$. Ponieważ $a|a_1$ i $a|b_0$ więc $a|b_1c_0$. Skoro jednak $a \not| c_0$, a dzieli b_1..
Przypuśćmy, że wykazaliśmy już, że

$$a|b_0, a|b_1, \cdots, a|b_{j-1}$$

dla pewnego $j < n$. Z faktu, że $a_j = b_0c_j + a_1c_{j-1} + + \cdots + b_jc_0$, $a|b_0, a|b_1, \cdots$, $a|b_{j-1}, a|a_j$ wynika, że $a|b_jc_0$ a stąd $a|b_j$ (pamiętamy, że $a \not| c_0$).
Teraz już oczywistym jest, że udowodniliśmy (metodą indukcji), że $a|b_k$. Poniweaż jednak $b_kc_l = a_n$, korzystając kolejny raz z tego, że a jest elementym pierwszym pierścienia P, dochodzimy do wniosku, że $a|a_n$. Ta sprzeczność z założeniami twierdzenia kończy jego dowód. ■

Zauważmy, że dla dowolnego $n \geq 1$ wielomian $x^n + 2$ jest nierozkładalny na mocy kryterium Eisensteina.[3] Mamy więc przykład nieskończonego zbioru wielomianów nierozkładalnych.

11.4 Wielomiany wielu zmiennych

Niech będzie dany pierścień P całkowity. Wówczas $(P[\mathbf{x}])[\mathbf{y}]$ nazywamy **pierścieniem wielomianów dwóch zmiennych**. Pierścień ten oznaczamy przez $P[\mathbf{x}, \mathbf{y}]$.

Użycie powyżej nazwy *pierścień* dla *zbioru* wielomianów dwóch zmiennych jest pozornym nadużyciem. Nie udowodniliśmy przecież, że $P[\mathbf{x}, \mathbf{y}]$ jest rzeczywiście pierścieniem. Jednak wiemy już, że $P[\mathbf{x}]$ jest pierścieniem i to całkowitym. Wobec tego $P[\mathbf{x}, \mathbf{y}]$ jako zbiór wielomianów (zmiennej $\mathbf{y}$) o współczynnikach w pierścieniu całkowitym $P[\mathbf{x}]$ jest pierścieniem (całkowitym).
Wielomian n zmiennych $\mathbf{x_1}, ..., \mathbf{x_n}$ definiujemy rekurencyjnie poprzez (rekurencyjną) definicję pierścienia wielomianów n zmiennych:

$$P[\mathbf{x_1}, ..., \mathbf{x_n}] = \mathbf{P}[\mathbf{x_1}, ..., \mathbf{x_{n-1}}][\mathbf{x_n}]$$

[2]Podczas wykładu, zupełnie niepotrzebnie i bez sensu, powiedziałem i napisałem na tablicy, że P nie jest rozkładalny na iloczyn wielomianów stopnia co najmniej 1. Odwołuję!

[3]Oczywiście 2 można tu zastąpić dowolną liczbą pierwszą i otrzymać także wielomian nierozkładalny w $\mathbf{Z}[x]$.

Bardzo łatwo stwierdzić, że ogólna postać wielomianu $v \in P[\mathbf{x_1}, ..., \mathbf{x_n}]$ jest następująca

$$v(\mathbf{x_1}, ..., \mathbf{x_n}) = \sum \mathbf{a_{i_1,...,i_n}} \mathbf{x^{i_1}} \cdot ... \cdot \mathbf{x^{i_n}}$$

($a_{i_1,...,i_n} \in P$ nazywamy współczynnikami wielomianu v).

11.4.1 Wielomiany symetryczne

Twierdzenie 11.10 (Wzory Viety) *Niech K będzie ciałem. Jeśli $K[x] \ni v = a_0 + a_1x + \ldots + a_nx^n$ jest wielomianem stopnia n o n pierwiastkach $\alpha_1, \ldots, \alpha_n$ (niekoniecznie różnych) należących do pewnego ciała $L \supset K$, wówczas*

$$v = k(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$$

i zachodzą wzory (zwane **wzorami Viety***):*

$$a_n = k$$

$$a_{n-1} = -k(\alpha_1 + \ldots + \alpha_n)$$

$$a_{n-2} = k(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n)$$

$$\ldots$$

$$a_0 = k(-1)^n\alpha_1 \cdot \ldots \cdot \alpha_n$$

Dowód - praktycznie oczywisty: wystarczy porównać współczynniki wielomianu we wzorze

$$a_0 + a_1x + \ldots + a_nx^n = k(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$$

■

Z twierdzenia 11.10 wynika natychmiast następujący wniosek.

Wniosek 11.11 *Jeśli wielomian $v \in K[x]$ ma pierwiastki $\alpha_1, \ldots, \alpha_n$ należące do ciała L zawierającego K (ciało K jest podciałem ciała L), wówczas*

$$\sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} \alpha_{i_1} \cdot \ldots \cdot \alpha_{i_k} \in K$$

dla każdego $k \le n$.

Rozdział 12

Wykład 12 - 4.I.2011

12.1 Wielomiany wielu zmiennych c.d.

12.1.1 Wielomiany symetryczne c.d.

r-tym podstawowym wielomianem symetrycznym $S_r(x_1, \ldots, x_n)$ nazywamy wielomian n zmiennych $x_1, \ldots, x_n$ który jest sumą wszystkich różnych iloczynów r różnych zmiennych.

Przykład.
$n = 4, r = 1$: $S_1(x_1, \ldots, x_5) = x_1 + x_2 + x_3 + x_4 + x_5$
$n = 5, r = 3$: $S_3(x_1, \ldots, x_5) = x_1x_2x_3 + x_1x_2x_4 + \ldots + x_3x_4x_5$

Wniosek 12.1 (Inna postać tw.Viety) *Jeżeli $\alpha_1, \ldots, \alpha_n \in L$ są pierwiastkami wielomianu $v \in K[x]$ (gdzie ciało K jest podciałem ciała L), $v = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$ to*

$$a_r = (-1)^r S_r(\alpha_1, \ldots, \alpha_n)$$

Stąd wynika kolejny ważny wniosek.

Wniosek 12.2 *Jeśli $\alpha_1, \ldots, \alpha_n \in L$ są pierwiastkami wielomianu $v \in K[x]$ (gdzie K jest podciałem ciała L), to*

$$S_r(\alpha_1, \ldots, \alpha_n) \in K$$

dla każdego $r, 1 \leq r \leq n$.

12.1.2 Twierdzenie Wilsona

Twierdzenie Wilsona (1741-1793)[1] dotyczy rozpoznawania liczb pierwszych, jest więc ważne chociażby ze względu na zastosowania w teori szyfrowania. Nie-

[1] John Wilson, autor twierdzenia o którym mowa, twierdzenia w sposób trwały związanego z jego nazwiskiem nie udowodnił, a jedynie stwierdził, odkrył - należy sądzić, raczej podejrzewał, że jest prawdziwe. Przypisanie twierdzenia Wilsona Wilsonowi więc jest nie do końca słuszne. Pierwszy dowód podał Lagrange w 1773 roku.

stety ze względu na liczbę operacji arytmetycznych jakie trzeba wykonać, nie za widać jak możnaby je stosować do rozpoznawania bardzo dużych liczb pierwszych (przez *duże* liczby rozumiemy oczywiście liczby naturalne o co najmniej setkach miejsc znaczących).

12.2 Twierdzenie Wilsona

Twierdzenie 12.3 (Twierdzenie Wilsona) *Liczba $p \in \mathbf{N}$ jest pierwsza wtedy i tylko wtedy, gdy*

$$(p-1)! + 1 \equiv 0(\ mod\ p)$$

Dow. ...

12.2.1 Podstawowe twierdzenie o wielomianach symetrycznych

Wielomian $v \in P[\mathbf{x_1}, ..., \mathbf{x_n}]$ nazywamy **symetrycznym** jeżeli dla dowolnej permutacji $\sigma \in S_n$ zachodzi wzór

$$v(\mathbf{x_{\sigma 1}}, ..., \mathbf{x_{\sigma n}}) = \mathbf{v}(\mathbf{x_1}, ..., \mathbf{x_n})$$

Twierdzenie 12.4 (Podstawowe o wielomianach symetrycznych) *W dowolnym opierścieniu z jedynką D dla każdego wielomianu symetrycznego $v \in D[x_1, \ldots, x_n]$ istnieje dokładnie jeden wielomian $w \in D[x_1, \ldots, x_n]$ taki, że*

$$v(x_1, \ldots, x_n) = w(S_1(x_1, \ldots, x_n), \ldots, S_n(x_1, \ldots, x_n)) \tag{12.1}$$

Podczas wykładu podałem dowód istnienia wielomianu w, natomiast nie udowodniłem, że taki wielomian jest wyznaczony jednoznacznie.

Dowód jednoznaczności. Niech wielomian w spełnia warunek 12.1 twierdzenia i niech p będzie największym jednomianem wielomianu w (*największym* w takim sensie, w jakim to zostało zdefiniowane podczas wykładu dowodu istnienia). Powiedzmy, że

$$p(S_1, S_2, ..., S_n) = cS_1^{\beta_1} S_2^{\beta_2} ... S_n^{\beta_n}$$

Wówczas największym jednomianem wielomianu

$$w(S_1(x_1, x_2, ..., x_n), S_2(x_1, x_2, ..., x_n), ..., S_n(x_1, x_2, ..., x_n))$$

jest

$$cx_1^{\beta_1+\beta_2+...+\beta_n} x_2^{\beta_2+\beta_3+...+\beta_n} \cdot ... \cdot x_n^{\beta_n}$$

Wynika stą, że największy jednomian od zmiennych $x_1, x_2, ..., x_n$ wielomianu w (a więc i wielomianu v!) powstaje w ten sposób z największego jednomianu zmiennych $S_1, S-2, ..., S_n$ wielomianu w. Mamy więc

$$cx^{\alpha_1} \cdot x^{\alpha_2} \cdot ... \cdot x^{\alpha_n} = cx_1^{\beta_1+\beta_2+...+\beta_n} \cdot x_2^{\beta_2+\beta_3+...+\beta_n} \cdot ... \cdot x_n^{\beta_n}$$

Pamiętamy (?), że podczas w pierwszej części dowodu, tej przeprowadzonej podvczas wykładu, przyjęliśmy, że największym jednomianem wielomianu v jest $cx^{\alpha_1} \cdot x^{\alpha_2} \cdot ... \cdot x^{\alpha_n}$. Stąd zaś wynika, że α_i oraz β_i spełniają następujący układ równań.

$$\begin{array}{ccccccccc} \beta_1 & + & \beta_2 & + & ... & + & \beta_n & = & \alpha_1 \\ & & p_2 & + & ... & + & p_n & = & \alpha_2 \\ & & & & ... & & & & \\ & & & & & & p_n & = & \alpha_n \end{array}$$

Eksperci z zakresu algebry liniowej, jakimi s studenci II roku Matematyki na WMS AGH rozpoznają bez trudu, że układ ten ma rozwiązania wyznaczone jednoznaczne :).

Wniosek 12.5 *Dla każdego wielomianu (jednej zmiennej) $v \in K[x]$ stopnia n o pierwiastkach $a_1, ..., a_n$ wpewnym ciele L ($K \subset L$) i dla każdego wielomianu symetrycznego $p \in K[x_1, ..., x_n]$ (n zmiennych) zachodzi*

$$p(a_1, ..., a_n) \in K$$

Dow. ...

12.3 Pierścienie wielomianów nad pierścieniami Gaussa

Niech P będzie pewnym pierścieniem (na razie nie koniecznie Gaussa). Oczywiście każdy element pierścienia P można traktować jako element pierścienia $P[x]$, mianowicie jako wielomian stopnia zerowego. Udowodniliśmy następujące twierdzenie.

Twierdzenie 12.6 *Każdy element pierwszy pierścienia P jest także elementem pierwszym pierścienia $P[x]$.*

Rozdział 13

Wykład 13 - 11.I.2011

13.1 Wielomiany nad pierścieniami Gaussa c.d.

Definicja 13.1 *Mówimy, że wielomian* $p = a_0 + a_1x + \ldots + a_nx^n$ *jest* **pierwotny** *jeżeli* $(a_0, a_1, \ldots, a_n) = 1$ *(współczynniki wielomian"u* p *są względnie pierwsze).*

Uwaga. Każdy wielomian nierozkładalny jest pierwotny. Wielomian $x^2 + 2x + 1 \in \mathbf{Z}[x]$ jest przykładem wielomianu pierwotnego, który nie jest nierozkładalny.

Twierdzenie 13.1 *Każdy element pierwszy dowolnego pierścienia* P *jest także elementem pierwszym* $P[x]$*.*

Dow. ...

Twierdzenie 13.2 (Lemat Gaussa) *Jeśli* P *jest pierścieniem Gaussa,* $p, q \in P[x]$ *są wielomianami pierwotnymi to iloczyn* pq *jest wielomianem pierwotnym.*

Dow. ...

Twierdzenie 13.3 *Iloczyn dowolnej liczby wielomianów pierwotnych nad pierścieniem Gaussa jest wielomianem pierwotnym.*

Twierdzenie 13.4 *Jeśli* p *jest wielomianem nierozkładalnym nad pierścieniem Gaussa* P*, wówczas* p *jest także nierozkładalny nad ciałem ułamków pierścienia* P*.*

Dow. ...

Wniosek 13.5 *Niech* P *będzie pierścieniem Gaussa. Każdy wielomian nierozkładalny w* $P[x]$ *jest elementem pierwszym pierścienia* $P[x]$*.*

Dow. ...

13.2 Twierdzenie Gaussa

Twierdzenie 13.6 *Pierścień wielomianów nad pierścieniem Gaussa jest pierścieniem Gaussa.*

Dow. ...

13.3 Rozszerzenia ciał

Rozszerzeniem ciała K nazywamy ciało L takie, że istnieje monomorfizm $T : K \to L$. Piszemy wtedy $L : K$ (taki napis czytamy *ciało L jest rozszerzeniem ciała K*).
Oczywiście, jeśli ciało K jest podciałem ciała L, wówczas $L : K$. Co więcej, z taką sytuacją będziemy mieli do czynienia najczęściej (choć nie zawsze). Czasami ciało K nazywamy *małym* zaś L *dużym*.

Niech $L : K$ i $X \subset L$.
Ciałem generowanym w K przez X nazywamy najmniejsze ciało zawierające X i K. Takie ciało oznaczamy przez $K < X >$. Jeśli zabiór X jest skończony, na przykład $X = \{a_1, ..., a_n\}$ wówczas piszemy $K < a_1, ..., a_n >$ zamiast $K < \{a_1, ..., a_n\} >$.

Ciało generowane przez $X \subset K$ jest równe[1]:

- przecięciu wszystkich podciał ciała L zawierających X,
- zbiorowi elementów które można otrzymać w ciągu skończonym operacji (działań w ciele) na elementach z X i K.

Przykład 13.1 $\mathbf{Q} < i, \sqrt{2} >$

Rozszerzenie ciała K o element $a \in L$ nazywamy **rozszerzeniem prostym** i oznaczamy przez $K < a >$ (zamiast $K < \{a\} >$).

Ćwiczenie 13.1 *Sprawdź, że* $\mathbf{Q} < i, -i, \sqrt{3}, -\sqrt{3} >$ *jest rozszerzeniem prostym.*

13.4 Ciało rozkładu

Przypomnijmy znane już wcześniej pierścienie ilorazowe.
Jeżeli I jest ideałem pierścienia P, wówczas iloraz P/I jest pierścieniem. Pamiętamy, że zerem tego pierścienia jest I zaś elementami zbiory postaci

$$I + a$$

gdzie $a \in P$. Działania w pierścieniu są wtedy określona wzorami:

$$(I + a) + (I + b) = I + (a + b)$$

[1]Podczas wykładu dowodów tych faktów nie podawałem. Polecam Waszej uwadze jako ćwiczenie.

$$(I + a)(I + b) = I + ab$$

Przypomnijmy także, że jeśli K jest ciałem, to $K[\mathbf{x}]$ jest pierścieniem głównym. łatwo jest udowodnić następujące twierdzenie. Ćwiczenie!

Twierdzenie 13.7 *Jeśli K jest ciałem, $v \in K[\mathbf{x}]$, $\partial v = n$, wówczas*

$$K[\mathbf{x}]/(v) = \{(v) + w : \ w \in K[\mathbf{x}], \partial w \leq n - 1\}$$

Przykład. Ułóż tabelkę działań dla $\mathbf{Z}_2[\mathbf{x}]/(\mathbf{x}^2 + 1)$, $\mathbf{Z}_5[\mathbf{x}]/(\mathbf{x}^2 + \mathbf{x} + 3)$, ... może jeszcze coś?

Twierdzenie 13.8 *Jeśli K jest ciałem a $v \in K[\mathbf{x}]$ wielomianem nierozkładalnym nad K, wówczas $K[\mathbf{x}]/(v)$ jest ciałem.*

Dow. ...

Ćwiczenie. Dla jakich wartości $a \in \mathbf{Z}_3$ pierścień ilorazowy $\mathbf{Z}_3[\mathbf{x}]/(\mathbf{x}^2 + a)$! jest ciałem?

Zauważmy, że ciało $K[\mathbf{x}]/(v)$ (gdzie v jest wielomianem nieprzywiedlnym nad K) zawiera podciało izomorficzne z K. Tym podciałem jest zbiór

$$\{[a] : a \in K\} = \{(v) + a : a \in K\}$$

Izomorfizmem jest $T : K \ni a \to (v)+a$. Dlatego też $K[\mathbf{x}]/(v)$ jest rozszerzeniem K $(K[\mathbf{x}]/(v) : K)$.

Ciałem rozkładu wielomianu $v \in K[\mathbf{x}]$ nazywamy najmniejsze ciało, w którym v rozkłada się na iloczyn czynników liniowych

$$v = a(\mathbf{x} - b_1) \dots (\mathbf{x} - b_n)$$

Inaczej mówiąc, jest to ciało $K(b_1, \dots, b_n)$

Twierdzenie 13.9 (O ciele rozkładu) *Dla dowolnego ciała K i wielomianu $v \in K[\mathbf{x}]$ istnieje rozszerzenie $L : K$ w którym v rozkłada się na iloczyn czynników liniowych.*

Podczas wykładu nie zdążyliśmy twierdzenia 13.9 udowodnić. Dowód zostanie podany na wykładzie następnym i będzie się opierał na poniższym lemacie.

Lemat 13.10 *Jeśli v jest wielomianem nierozkładalnym nad ciałem K, wówczas w ciele $K[\mathbf{x}]/(v)$ element $\mathbf{x} + (v)$ jest pierwiastkiem wielomianu v.*

Dow. ...

Rozdział 14

Wykład 14 - 18.I.2011

14.1 Zasadnicze Twierdzenie Algebry

Mówimy, że ciało K jest **algebraicznie zamknięte** jeżeli każdy wielomian $v \in K[\mathbf{x}]$ ma w K wszystkie ∂v pierwiastki w K, czyli

$$v = a(\mathbf{x} - u_1)(\mathbf{x} - u_2) \cdot ... \cdot (\mathbf{x} - u_d)$$

gdzie $d = \partial v$, $u_1, ..., u_d, a \in K$.

Twierdzenie 14.1 *Ciało liczb zespolonych jest algebraicznie zamknięte.*

Dowód (niedokończony, c.d. będzie na wykładzie następnym).
Podzielić go można na kilka części.
1. Wykażemy, że twierdzenie wystarczy wykazać dla wielomianach o współczynnikach rzeczywistych.
Niech $v \in \mathbf{C}[\mathbf{x}]$. Oznaczmy przez $\bar{v}$ wielomian powstały przez sastąpienie wszystkich współczynników v ich sprzężeniami, tzn. jeśli $v(\mathbf{x}) = a_0 + a_1\mathbf{x} + ... + a_d\mathbf{x}^d$ wówczas $\bar{v}(\mathbf{x}) = \bar{a_0} + \bar{a_1}\mathbf{x} + ... + \bar{a_d}\mathbf{x}^d$.
Zauważmy, że wielomian

$$w = v\bar{v}$$

ma współczynniki rzeczywiste. Rzeczywiście, $w(\mathbf{x}) = \sum_{l=0}^{d}(\sum_{i=0}^{l} \bar{a_i}a_{l-i})\mathbf{x}^l$. Łatwo sprawdzić, że

$$\bar{b_l} = \sum_{i=0}^{l} a_i\bar{a}_{l-i} = b_l$$

Czyli $b_l \in \mathbf{R}$ dla wszystkich l.
Jeśli, dla pewnego $u \in \mathbf{C}$ $w(u) = 0$, wówczas $v(u)\underline{\bar{v}(u)} = 0$, czyli $v(u) = 0$ lub $\bar{v}(u) = 0$. W drugim przypadku mamy $0 = \bar{v}(u) = \overline{v(\bar{u})}$. A to oznacza, że $\bar{u}$ jest pierwiastkiem wielomianu v.
A więc, wielomian v (dowolny wielomian o współczynnikach rzespolonych) ma

pierwiastek w zbiorze liczb zespolonych wtedy i tylko wtedy, gdy pewien wielomian o współczynnikach rzeczywistych (mianowicie $v\bar{v}$) ma pierwiastek zespolony.

2. Dalsza część dowodu przez indukcję. Niech $v \in \mathbf{R}$, $\partial v = d = 2^n m$, gdzie m jest liczbą nieparzystą (łatwo zaobserwować, że każdą liczbę naturalną d różną od zera można zapisać w tej postaci). **Indukcję poprowadzimy za względu na** n.

Jeśli $n = 0$, wówczs v jest stopnia nieparzystego - wiemy (także jeszcze ze szkoły!), że każdy wielomian o współczynnikach rzeczywistych i stopnia nieparzystego ma pierwiastek (i to rzeczywisty).

Przypuśćmy więc, że $n \geq 1$ i niech $u_1, ..., u_d$ będą pierwiastkami wielomianu v w jego ciele rozkładu[1]. Wówczas $v(\mathbf{x}) = a(\mathbf{x} - u_1) \cdot ... \cdot (\mathbf{x} - u_d)$ gdzie $a \in \mathbf{R}$. Oczywiście

$$v(\mathbf{x}) = a\mathbf{x}^d + aS_1(u_1, ..., u_d)\mathbf{x}^{d-1} + ...(-1)^d aS_d(u_1, ..., u_d)\mathbf{x}^d$$

i dla każdego $k = 1, ..., d$ $S_k(u_1, ..., u_d) \in \mathbf{R}[\mathbf{x}]$.

Dla dowolnego $h \in \mathbf{Z}$ zdefiniujmy wielomian

$$v_h(\mathbf{x}, \mathbf{x}_1, ..., \mathbf{x}_d) = \prod_{1 \leq i < j \leq d} (\mathbf{x} - \mathbf{x}_i - \mathbf{x}_j - h\mathbf{x}_i\mathbf{x}_j)$$

Oczywiście $v_h \in \mathbf{R}[\mathbf{x}, \mathbf{x}_1, ..., \mathbf{x}_d] = \mathbf{R}[\mathbf{x}][\mathbf{x}_1, ..., \mathbf{x}_d]$. Co więcej, dla ustalonego $h \in \mathbf{Z}$ wielomian v_h jest wielomianem symetrycznym ze względu na zmienne wielomianowe $\mathbf{x}_1, ..., \mathbf{x}_d$. A więc, na mocy Zasadniczego Twierdzenia o Wielomianach Symetrycznych, v_h jest wielomianem $S_1(\mathbf{x}_1, ..., x_d), ..., S_d(x_1, ..., x_d)$ o współczynnikach w $\mathbf{R}[\mathbf{x}]$. Skoro $S_1(u_1, ..., u_d), ..., S_d(u_1, ..., u_d) \in \mathbf{R}$ także wielomian $v_h(\mathbf{x}, u_1, ..., u_d)$ (a więc wielomian zmiennej $\mathbf{x}$) ma współczynniki w $\mathbf{R}$ (dla każdego całkowitego h). Stopień tych wielomianów (bo dla każdego $h \in \mathbf{Z}$ mamy jeden) wielomianu **ze względu na x** wynosi

$$\partial v_h = \binom{d}{2} = \frac{1}{2}d(d-1) = 2^{n-1}m(2^n m - 1)$$

Z założenia indukcyjnego, v_h ma pierwiastek w $\mathbf{C}$ (to, że te wielomiany mają pierwiastki, to nic ciekawego, wiadomo z Twierdzenia o Ciele Rozkładu - ważne jest to, że te pierwiastki są w $\mathbf{C}$!).

Wobec tego każdy wielomian (dla każdego $h \in \mathbf{Z}$) ma pierwiastek w $\mathbf{C}$, a stąd relacja

$$u_i + u + j + hu_i u_j \in \mathbf{C}$$

jest spełniona dla nieskończonej liczby parametrów h. Muszą więc istnieć i oraz j (ustalone) oraz takie h i h', oba całkowite, $h \neq h'$, że

$$u_i + u_j + hu_i u_j \in \mathbf{C}$$

[1] Tu właśnie korzystamy z Twierdzenia o Ciele Rozkładu.

$$u_i + u_j + h' u_i u_j \in \mathbf{C}$$

Stąd łatwo wywnioskować, że

$$u_i + u_j \in \mathbf{C}$$

oraz

$$u_i u_j \in \mathbf{C}$$

A więc $(\mathbf{x} - u_i)(\mathbf{x} - u_j) \in \mathbf{C}[\mathbf{x}]$. Równanie zaś kwadratowe o współczynnikach zespolonych ma rozwiązania zespolone (a więc $u_i, u_j \in \mathbf{C}$). ■

Wniosek 14.2 *Niech $v \in \mathbf{R}[\mathbf{x}]$. Wówczas v ma jednoznaczny rozkład na iloczyn postaci*

$$v = a(x - c_1) \cdot ... \cdot (x - c_l)(x^2 d_1 x + e_1) \cdot ... \cdot (x^2 + d_k x + e_k)$$

gdzie $c_1, ..., c_l, d_1, ..., d_k, e_1, ..., e_k \in \mathbf{R}$, $l + 2k$ jest stopniem wielomianu v, zaś wielomiany stopnia drugiego (trójmiany kwadratowe) są nad $\mathbf{R}$ nierozkładalne i każdy z nich odpowiada pewnemu pierwiastkowi zespolonemu v.

14.2 Rozszerzenia skończone, algebraiczne i przestępne

[Rozszerzenia skończone, algebraiczne i przestępne]

Jeśli L i K są ciałami i $L : K$ i wymiar przestrzeni wektorowej L nad ciałem K wynosi n to mówimy, że $n = [L : K]$ jest wymiarem ciała L nad K. Rozszerzenie L nazywamy wówczas **skończonym**. **Bazą** ciała L nad K nazywamy bazę L (traktowanego jako przestrzeń wektorowa nad K). L jest **rozszerzenienm nieskończonym** L, jeśli nie jest rozszerzeniem skończonym.

Element $a \in L$ nazywamy **algebraicznym** nad K jeśli a jest pierwiastkiem pewnego, nie zerowego wielomianu $v \in K[x]$. **Liczbą algebraiczną** nazywamy dowolny element algebraiczny nad ciałem $\mathbf{Q}$.

Przykład 14.1 *Sprawdź, że $i, \sqrt{3}, \sqrt{2 + \sqrt{2}}$ oraz $i + \sqrt{3}$ są liczbami algebraicznymi. Wskaż ich wielomiany minimalne.*

Element $a \in L$ nazywamy **elementem przestępnym** nad K (gdzie $L : K$), jeżeli a nie jest algebraiczny nad K. Elementy przestępne nad $\mathbf{Q}$ nazywamy **liczbami przestępnymi**.

Rozszerzenie L ciała K nazywamy **algebraicznym** jeżeli każdy element $a \in L$ jest algebraiczny nad K.

Przykład 14.2 *Wszystkie dotychczasowe przykłady.*
$\mathbf{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$
Podaj inne, nietrywialne przykłady.

Twierdzenie 14.3 (O rozszerzeniach skończonych) *Każde rozszerzenie skończone jest rozszerzeniem algebraicznym. Co więcej, jeśli* $[L : K] = k$ *i* $a_1, \ldots, a_k$ *jest bazą* L *nad* K*, to* $L = K(a_1, \ldots, a_k)$ *i każdy element* $b \in L$ *jest elementem algebraicznym stopnia co najwyżej* k *nad* K*.*

Dow. Podczas wykładu zdążyliśmy wykazać tylko pierwszą część twierdzenia, wrócimy do niego na następnym wykładzie.

Rozdział 15

Wykład 15 - 25.I.2011

Ustalenia dotyczące egzaminu

I termin: Pisemny 3 lutego o 9.00
Ustny: 9, 10 i 11 lutego

II termin: Pisemny 21 lutego o 9.00
Ustny 22-23 lutego

II termin: Pisemny 24 lutego o 9.00
Ustny 25-26 lutego

Wszystkie egzaminy pisemne w B7, parter
Egzaminy ustne w moim gabinecie (I pietro B7, p. 1.12). Dokładne listy z orientacyjnymi godzinami rozpoczęcia pytania poszczególnych osób ustalę po otrzymaniu listy zaliczeń i prześlę na nasze konto.
Jeśli liczba osób na egzamin ustny nie będzie zbyt duża, wówczas egzamin ustny rozpocznie się 10 lutego (I termin), ta decyzja jednak może być podjęta dopiero po otrzymaniu wyników zaliczeń. Podobnie będzie z następnymi terminami.
Choć dokładne listy egzaminów ustnych zostaną podane później, już teraz podaję zasadę ogólną, którą będę się kierował. Kolejność egzaminowania będzie zgodna z numerami grup i kolejnością osób na listach, które otrzymam z dziekanatu.

15.1 Rozszerzenia skończone, algebraiczne i przestępne c.d.

Przypomnijmy, że rozszerzeniem prostym ciała K nazwaliśmy rozszerzenie $K < a >$ o jeden element, mianowicie o a. Oczywistym jest, że $K < a >= \{\frac{u(a)}{v(a)} : u, v \in K[\mathbf{x}], v(a) \neq 0\}$. Okazuje się, że rozszerzenie proste nie musi być skończonym.

Twierdzenie 15.1 *Niech K będzie dowolnym ciałem. Wówczas $K < \mathbf{x} >$ jest rozszerzeniem przestępnym.*

Dowód. Łatwo zauważyć, że element $\mathbf{x} \in K < \mathbf{x} >$ jest elementem przestępnym ciała $K < \mathbf{x} >$.

Twierdzenie 15.2 (O wielomianie minimalnym) *Dla każdego elementu $a \in L$ algebraicznego nad K istnieje dokładnie jeden wielomian unormowany*[1] *$v \in K[\mathbf{x}]$ taki, że*

- *v jest nierozkładalny na K,*
- *$v(a) = 0$,*
- *v dzieli każdy wielomian $w \in K[\mathbf{x}]$ którego a jest pierwiastkiem*[2]*.*

Dow. ...

Wielomian v o którym mówi twierdzenie 15.2 nazywamy **wielomianem minimalnym elementu algebraicznego** a, zaś stopień tego wielomianu **stopniem elementu** a.

Teraz podałem dowód twierdzenia 15.2 (o rozszerzeniach skończonych) z poprzedniego wykładu.

Powyżej widzieliśmy, że rozszerzenie proste nie musi być skończonym. Tak jednak nie może się stać, gdy element o który ciało rozszerzamy jest elementem algebraicznym nad tym ciałem.

Twierdzenie 15.3 (O Rozszerzeniach Prostych o Element Algebraiczny) *Dla dowolnego elementu algebraicznego a nad ciałem K, rozszerzenie $K < a >$ jest skończone.*

Dow. ...

Podczas wykładu powiedziałem, że dowód następnego twierdzenia jest niezbyt trudnym (dla studentów po całorocznym wykładzie z algebry liniowej) ćwiczeniem. Obiecałem jednak, że dowód ten znajdzie się w *Notatkach.* Teraz z danej bietnicy wywiązuję się.

Twierdzenie 15.4 *Rozszerzenie skończone rozszerzenia skończonego jest rozszerzeniem skończonym.*
Dokładniej: jeśli $M : L$ i $L : K$ są rozszerzeniami skończonymi, wówczas

$$[M : K] = [M : L][L : K]$$

[1] To znaczy taki, którego współczynnik dominujący (przy najwyższej potędze) jest równy jedynce.

[2] O tym twierdzeniu na wykładzie nie mówiłem. Pozostaje dla ciekawych, ale na egzaminie nie będę z niego pytał. Ani z tego co jest tuż po tym twierdzeniu (3 linijki).

Dowód. Niech $a_1, ..., a_k$ będzie bazą M nad L, zaś $b_1, ..., b_m$ bazą L nad K. Oczywiście $a_i \in M$ dla $i = 1, ..., k$ i $b_j \in L$ dla $j = 1, ..., m$.
Wówczas dla dowolnego elementu $a \in M$ możemy napisać:

$$\begin{array}{rcll} a & = & \sum_{i=1}^{k} \alpha_i a_i & = \\ & = & \sum_{i=1}^{k} a_i (\sum_{j=1}^{m} \beta_{ij} b_j) & = \\ & = & \sum_{i=1}^{k} \sum_{j=1}^{m} \beta_{ij} \cdot (a_i \cdot b_j) & \end{array}$$

gdzie $\alpha_i \in L$ dla $i = 1, ..., k$ oraz $\beta_{ij} \in K$ dla $i = 1, ..., k;\ j = 1, ..., m$ (oczywiście każdy element α_i zapisujemy tu w postaci $\alpha_i = \sum_{j=1}^{m} \beta_{ij} b_j$, korzystając z faktu, że elementy $b_1, ..., b_m$ tworzą bazę L nad K). Stąd natychmiast wynika, że $m \cdot k = [M : L] \cdot [L : K]$ elementów postaci $a_i \cdot b_j$ generuje M nad K. Pozostaje wykazać, że te elementy są liniowo niezależne. Rzeczywiście, przypuśćmy, że

$$\sum_{i=1,...,k;\ j=1,...,m} \gamma_{ij} \cdot (a_i \cdot b_j) = 0$$

dla pewnych $\gamma_{ij} \in K,\ i = 1, ..., k;\ j = 1, ..., m$. Wówczas

$$\sum_{i=1}^{k} a_i (\sum_{j=1}^{m} b_j \gamma_{ij}) = 0$$

Ponieważ $\sum_{j=1}^{m} b_j \gamma_{ij} \in L$ dla każdego $i = 1, ..., k$, zaś elementy $a_1, ..., a_k$ jako elementy bazy M nad L są liniowo niezależne, mamy

$$\sum_{j=1}^{m} b_j \gamma_{ij} = 0$$

dla każdego $i = 1, ..., k$. Teraz wystarczy skorzystać z liniowej niezależności $b_1, ..., b_m$ nad K i faktu, że $\gamma_{ij} \in K$ by łatwo wywnioskować, że $\gamma ij = 0$ dla wszystkich i oraz j. ■

15.1.1 Liczby konstruowalne i niekonstruowalne.

Wszystkie informacje, które podałem na ten temat podczas wykładu (nie licząc faktów z życia Gaussa, które z łatwością wyszperacie w internecie), można znaleźć w książce Gilberta i Nicholsona [7], rozdział 13, strony 284-208.

Rozdział 16

Pytania

1. Wykaż, że zbiór liczb pierwszych jest nieskończony.
   Wykaż, że szereg
   $$\sum_{p-l.\ pierwsza} \frac{1}{p}$$
   jest rozbieżny.

2. Wykaż, że przedział liczb naturalnych beż liczb pierwszych może być dowolnie liczny (mieć dowolnie dużą, z góry ustaloną liczbę elementów).

3. Wykaż, że pierścień A jest bez dzielników zera wtedy i tylko wtedy gdy obowiązuje w nim prawo skracania.
   Podaj przykłady pierścieni (z dzielnikami zera i bez).

4. Wypowiedz i udowodnij twierdzenie o algorytmie dzielenia liczb całkowitych.

5. Zdefiniuj element piewszy i element nierozkładalny w pierścieniu. Twierdzenie o elemencie pierwszym (że jest, przy odpowiednich założeniach o pierścieniu) nierozkadalny. Przykąd, że twierdzenie dowrotne jest nieprawdziwe.

6. Pierścienie Gaussa. Twierdzenie o elemencie nierozkładalnym w pierścieniu Gaussa.

7. Zdefiniuj pierścień i ideał. Podaj i udowodnij warunek konieczny i wystarczający by podzbiór pierścienia był ideałem.
   Definicje ideału i pierścienia głównego.

8. Wykaż, że $(\mathbf{Z}; +, \cdot)$ jest pierścieniem głównym.

9. Wypowiedz i udowodnij twierdzenie o dzieleniu wielomianów nad pierścieniem całkowitym.
   Niech D będzie pierścieniem całkowitym. Sformułuj i udowodnij

   - wniosek o ilorazie wielomianu $w \in D[x]$ przez $x - c$ (gdzie $c \in D$),

- wkw by $c \in D$ było pierwiastkiem wielomianu $w \in D[x]$.
- wielomian stopnia k ma w D co najwyżej k pierwiastków.

10. Wykaż, że pierścień wielomianów $\mathbf{K}[x]$ nad ciałem $\mathbf{K}$ jest pierścieniem głównym.
11. Wykaż, że dowolny ciąg rosnący ideałów w pierścieniu głównym jest stacjonarny.
12. Wykaż, że dla dowolnych elementów a i b w pierścieniu głównym D istnieją $s, t \in D$ takie, że $\mathrm{NWD}(a, b) = d = sa + tb$.
13. Algorytm Euklidesa.
14. Pierścienie euklidesowe.
15. Zasadnicze Twierdzenie Arytmetyki.
16. Ciało. Ciało ułamków pierścienia całkowitego.
17. Podpierścień. Ideał. Pierścień ilorazowy.
18. Ideał pierwszy. Kiedy pierścień ilorazowy jest bez dzielników zera?
19. Ideał maksymalny pierścienia i ideał pierwszy.
20. Warunek konieczny i wystarczający by P/I był ciałem (P jet pierścieniem przem. z 1 zaś I jego ideałem).
21. Podstawowe twierdzenie o homomorfi"xmie pierścieni.
22. Wielomian pierwotny. Lemat Gaussa.
23. Wielomian nierozkładalny $v \in P[x]$, gdzie P jest pierściaeniem Gaussa jest nierozkładalny także w pierścieniu wielomianów nad ciałem ułamków.
24. Wykaż, że a jest elementem odwracalnym w $\mathbf{Z}_n$ wtedy i tylko wtedy gdy a i n są względnie pierwsze.
25. Zdefiniuj zbiór $\mathbf{Z}_n^*$ i wykaż, że $(\mathbf{Z}_n^*; \bigotimes)$ jest grupą przemienną.
26. Zdefiniuj funkcję φ Eulera. Wykaż, że dla dowolnego n $|\mathbf{Z}_n^*| = \varphi(n)$.
27. Sformułuj i udowodnij formułę sita.
28. Wyprowadź wzór na $\varphi(n)$ (dla znanego rozkładu n na iloczyn liczb pierwszych).
29. Wykaż, że w dowolnej multyplikatywnej grupie skończonej G, dla dowolnego elementu $g \in G$, istnieje n takie, że $g^n = g^{-1}$.
30. Zdefiniuj grupę cykliczną. Wykaż, że każda grupa cykliczna G jest izomorficzna z $(\mathbf{Z}_n; +)$, gdzie $n = |G|$.

31. Zdefiniuj grupę transformacji. Twierdzenie Cayleya.
32. Twierdzenie Lagrange'a. Wykaż, że rząd dowolnego elementu grupy skończonej jest dzielnikiem rzędu grupy.
33. Wykaż, że jeśli rząd grupy G jest liczbą pierwszą, to G jest cykliczna.
34. Małe twierdzenie Fermata.
35. Omów rozwiązania równania

$$ax \equiv b \pmod{n}$$

gdzie a i n są względnie pierwsze.

36. Chińskie Twierdzenie o Resztach.
37. Zasady kryptografii z kluczem publicznym.
38. Metoda Rabina.
39. Zdefiniuj rząd elementu w pierścieniu. Wykaż, że w pierścieniu całkowitym wszystkie elementy są tego samego rzędu (charakterystyka pierścienia całkowitego).
40. Wykaż, że charakterystyką pierścienia całkowitego jest 0 (∞) lub liczba pierwsza.
41. Wykaż, że w każdym pierścieniu o charakterystyce 0 podpierścień, generowany pzrez e jest izomorficzny z $\mathbf{Z}$.
42. Wykaż, że jeśli D jest pierścieniem o czarakterystyce p (l. pierwsza) to

$$D \ni a \to a^p \in D^p$$

jest izomorfizmem pierścieni.

43. Podaj i udowodnij wkw by podzbiór ciała był podciałem.
44. Wykaż, że w ciele o charakterystyce 0 podciało generowane przez 1 jest izomorficzne z $\mathbf{Q}$.
45. Wykaż, że w ciele o charakterystyce $p \neq 0$ podciało generowane przez 1 jest izomorficzne z $\mathbf{Z}_p$.
46. Zdefiniuj rozszerzenie ciała i rozszerzenie pojedyńcze (przestępne i algebraiczne), podaj przykłady.
47. Wykaż, że jeśli c jest elementem przestępnym względem ciała F, to ciało $F(c)$ jest izomorficzne z $F(x)$ (ciałem funkcji wymiernych zmiennej x, zaś izomorfizm można dobrać tak by

$$c \to x$$

$$a \to a \quad \forall a \in F$$

48. Wykaż, że każdy element algebraiczny a względem ciała F jest pierwiastkiem jedynego wielomianu w unormowanego i nierozkładalnego. Co więcej, a jest pierwiastkiem wielomianu v (o współczynnikach w F) wtedy i tylko wtedy jeśli v jest w $F[x]$ wielokrotnością w.

49. Niech $a \in K$, K – ciało, a – element algebraiczny względem podciała F. Wykaż, że podciało $F(a($ generowane przez a składa się z elementów które są wartościami funkcji wymiernych (o współczynnikach w F) od a Wykaż, że funkcja

$$F(x) \ni f \to f(a) \in F(a)$$

jest homomorfizmem ciał.

Bibliografia

[1] M. Aigner i G.M. Ziegler, Dowody z Księgi, PWN, Warszawa 2002.

[2] A. Białynicki-Birula, Algebra, PWN, Warszawa 1980.

[3] G. Birkhoff i S. Mac Lane, Przegląd algebry współczesnej, PWN, Warszawa 1963.

[4] G. Birkhoff i S. Mac Lane, Algèbre, Gauthier-Villars, Paryż 1971.

[5] G. Birkhoff i T.C. Bartee, Współczesna algebra stosowana, PWN, Warszawa 1983.

[6] D.A. Cox, Galois theory, Wiley 2004.

[7] W.J Gilbert, W.K. Nicholson, Algebra współczesna z zastosowaniami, WNT, Warszawa 2008.

[8] D.W. Hardy i C.L. Walker, Applied Algebra: Codes, Ciphers and Discrete Algorithms, Prentice Hall 2003.

[9] N. Koblitz, Algebraiczne aspekty kryptografii, WNT, Warszawa 200

[10] A.I. Kostrykin, Wstęp do algebry, cz. 1 Podstawy algebry, PWN Warszawa 2004.

[11] A.I. Kostrykin, Wstęp do algebry, cz. 3 Podstawowe struktury algebraiczne, PWN Warszawa 2005

[12] W.K. Nicholson, Introduction to Abstract Algebra, Third Edition, Wiley 2007.

[13] Z. Opial, Algebra wyższa, PWN, Warszawa 1975.

[14] E.R. Scheinerman, Mathematics - Discrete Introduction, Brooks/Cole 2000.

[15] I. Stewart, Galois Theory, Chapman and Hall Mathematics, Londyn, Nowy York 1989.