(tylko) Konspekt wykładu Algebra I*: Pierścienie 2019

http://www.mimuw.edu.pl/%7Eaweber

v.26.1.2020

Notatki zawierają odsyłacze do podręczników

[AMcD] M. F. Atiyah, I. G. MacDonald, Introduction To Commutative Algebra (wiele wydań)

[BB] A. Białynicki-Birula, Zarys algebry, Bibl.Mat. 63, PWN, Warszawa 1987

[BT] A. Bojanowska, P. Traczyk, Algebra I (skrypt)
http://www.mimuw.edu.pl/%7Eaboj/algebra/algnowa13.pdf

[Br] J. Browkin, Teoria ciał, Bibl.Mat.49, PWN, Warszawa 1977

[Is] I. M. Isaacs, Algebra: A Graduate Course

1 Pierścienie

1.1 Definicja pierścienia przemiennego z 1: $(R, +, \cdot, 0, 1)$

1.2 Jedyność jedynki, $a \cdot 0 = 0$

1.3 *Niektóre elementy definicji pierścienia bywają opuszczane (przemienność, jedynka, a nawet czasami łączność mnożenia).*

1.4 *Macierze kwadratowe nad ustalonym ciałem (pierścień nieprzemienny z 1)*

1.5 *Pierścień grupowy (dla grupy skończonej)*

$$\mathbb{Z}(G) = Funkcje(G, \mathbb{Z}) \ni \sum_{g \in G} a_g e^g \,.$$

$$e^g \cdot e^h := e^{gh} \,.$$

Mnożenie w pierścieniu grupowym można zapisać jako splot funkcji na grupie

$$f_1 * f_2(g) = \sum_{h \in G} f_1(h) f_2(h^{-1} g) \,.$$

Mnożenie jest nieprzemienne jeśli grupa jest nieprzemienna.

1.6 *Funkcje na przestrzeni topologicznej o nośniku zwartym $C_0(X; \mathbb{R})$ (nie ma 1 jeśli X nie jest zwarta)*

1.7 Przykłady pierścieni (od tej pory będą tylko pierścienie przemienne z 1):

$\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}_n$, ciała.

1.8 Podpierścień. Podpierścienie $\mathbb{Q}$:

- $\mathbb{Z}[1/p]$,
- $\mathbb{Z}_{(p)}$

1.9 Pierścień wielomianów $\mathbb{Z}[x]$, $\mathbb{K}[x]$, pierścień szeregów formalnych $\mathbb{Z}[[x]]$, $\mathbb{K}[[x]]$, pierścień szeregów Laurenta $\mathbb{K}((x))$, $\mathbb{K}[\epsilon]$, $\epsilon^2 = 0$

1.10 Pierścień funkcji wielomianowych na $\mathbb{K}^n$

1.11 Pierścień liczb p-adycznych $\mathbb{Z}_p^\wedge$

$$\mathbb{Z}_p^\wedge \twoheadrightarrow \ldots \twoheadrightarrow \mathbb{Z}_{p^{n+1}} \twoheadrightarrow \mathbb{Z}_{p^n} \twoheadrightarrow \ldots \twoheadrightarrow \mathbb{Z}_{p^2} \twoheadrightarrow \mathbb{Z}_p \twoheadrightarrow 0$$

1.12 Pierścienie funkcji rzeczywistych (ciągłych, gładkich, ograniczonych) na $U \subset \mathbb{R}^n$.

1.13 Elementy specjalnego typu
– elementy odwracalne, grupa elementów odwracalnych $U(R)$,
– dzielniki zera,
– elementy nilpotentne,
– elementy nierozkładalne,

1.14 Elementy zdefiniowanych wcześniej typów w $\mathbb{Z}$, $\mathbb{K}[x]$, $\mathbb{K}[\epsilon]$
– dzielniki zera w $\mathbb{Z}_n$
– elementy odwracalne w $\mathbb{K}[x]$, $\mathbb{K}[[x]]$
– $U(\mathbb{Z}[i])$

1.15 Dzielniki zera, dziedzina = dziedzina całkowitości = pierścień bez dzielników zera.

1.16 Skończona dziedzina jest ciałem.

Homomorfizmy pierścieni

1.17 Homomorfizm pierścieni (zakładamy, że $1 \mapsto 1$), istnieje tylko jeden homomorfizm z $\mathbb{Z}$ do dowolnego pierścienia.

1.18 Homomorfizmy pierscieni z 1, izomorfizm, homomorfizm $\mathbb{Z}$ w $\mathbb{Z}_m$ oraz ewaluacja wielomianów: $R[x] \to R$, $f \mapsto f(a)$.

1.19 Różnica między $R[x]$ a funkcjami wielomianowymi $R \to R$

1.20 Jądro homomorfizmu: jeśli $a \in \ker(\phi)$ to $ab \in \ker(\phi)$.

1.21 definicja ideału, ideały generowane przez podzbiór, ideały w $\mathbb{Z}$, $\mathbb{Z}_n$ i w $\mathbb{K}[x]$

1.22 Iloraz przez ideał R/I

2 Ideały

2.1 Uniwersalna własność ilorazu. Twierdzenie o izomorfizmie $im(f) = R/kef(f)$.

2.2 A podpierścień R, I ideał w R (piszemy $I \lhd R$), wtedy $I \cap A \lhd A$, $A + I$ podierścień R, oraz $A/(I \cap A) \simeq (A + I)/I$

2.3 Uniwersalna własność pierścienia wielomianów: każdy homomorfizm pierścieni $R \to S$ można jednoznacznie przedłużyć do homomorfizmu $R[x_1, x_2, \ldots, x_n] \to S$ przy zadanych wartościach na x_i.

2.4 Ideały pierwsze, ideały maksymalne, ideały główne

2.5 Twierdzenie: ideałI jest maksymalny $\iff$ R/I jest ciałem.
($[a] \in R/I$ nie jest odwracalny to $(I, a) = I + Ra$ jest właściwym ideałem)

2.6 Twierdzenie: ideał I w R jest pierwszy $\iff$ R/I jest dziedziną.

2.7 Ideał główny $(n) \subset \mathbb{Z}$ dla $n \in \mathbb{N}$, $n > 1$ jest pierwszy wtedy i tylko wtedy gdy n jest liczbą pierwszą.

2.8 W $\mathbb{Z}$, $\mathbb{K}[x]$ każdy ideał jest główny. W tych pierścieniach działa algorytm euklidesa i Każdy element można rozłożyć na elementy nierozkładalne. Rozkład jest jednoznaczny z dokładnością do mnożenia przez elementy odwrotne i przestawianie czynników.

2.9 Plan na przyszłość. Będziemy rozważali trzy klasy pierścieni:
– DJR (ang UFD): pierścienie z jednoznacznoącią rozkładu.
– DIG (ang PID): każdy ideał jest generowany przez jeden element
– Euklidesowe: działa algorytm Euklidesa dla pewnej normy.

$$\text{Eukl.} \quad \subset \quad \text{DIG} \quad \subset \quad \text{DJR}$$

2.10 $\mathbb{Z}[x]$, $\mathbb{K}[x, y]$ DJR, ale nie DIG

2.11 $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ DIG, nie Euklidesowy

2.12 Operacje na ideałach: przecięcie, suma wstępująca, $(I \cup J) = I + J$,

2.13 Ćwiczenie: przeciwobraz, obraz ideału?

2.14 Ideał jest niewłaściwy ($I = R$) wtedy i tylko wtedy gdy $1 \in I$.

2.15 Każdy ideał maksymalny jest pierwszy bo ciało jest bez dzielników zera.

2.16 Ciała mają tylko trywialne ideały $\{0\}$, $\mathbb{K}$. Jeśli R zawiera tylko jeden ideał właściwy, to R jest ciałem.

2.17 R jest ciałem wtedy i tylko wtedy gdy 0 jest ideałem maksymalnym.

2.18 Każdy homomorfizm ciał do niezererowego pierścienia jest włożeniem.

2.19 Twierdzenie: każdy ideał właściwy jest zawarty w pewnym ideale maksymalnym.
Z lematu Kuratowskiego-Zorna: każdy wstępujący ciąg ideałów ma ograniczenie górne (jest nim suma ideałów), zatem istnieje element maksymalny.

2.20 Dla każdego pierścienia R i elementu nieodwracalnego $a \in R$ istnieje epimorfizm do ciała $\pi : R \to \mathbb{K}$ taki, że $\pi(a) = 0$.

2.21 R jest bez dzielników zera wtedy i tylko wtedy gdy 0 jest ideałem pierwszym.

2.22 Dopuszczamy (niechętnie) pierścień zerowy, w którym $0 = 1$. Jeśli w R mamy $0 = 1$ to $R = \{0\}$.

Jeszcze trochę przykładów

2.23 Podpierścienie generowane przez podzbiór np $k[x^2, y^2]$

2.24 Niech $S_{\mathbb{R}} \subset \mathbb{R}^n$ będzie stożkiem wypukłym. Pierścień półgrupowy $k[S]$, dla $S = S_{\mathbb{R}} \cap \mathbb{Z}^n$.

2.25 Przykład: $S_{\mathbb{R}} = \{a(1,1) + b(-1,1) \in \mathbb{R}^2 \ : \ a, b \geq 0\}$.
$k[S] \simeq k[u, v, w]/(uv - w^2)$

3 Teoria podzielności

3.1 Niech R pierścień bez dzielników zera. Podzielność to relacja porządku na $R/\sim$, gdzie $\sim$ to relacja stowarzyszenia:

$$a \sim b \iff a = ub \qquad \text{gdzie } u \text{ jest elementem odwracalnym.}$$

3.2 NWD nie zawsze musi istnieć $NWD(a, b) = c$ w jezyku relacji porządku oznacza $([d] \leq [a] \wedge [d] \leq [b]) \Rightarrow [d] \leq [c]$. Przykład bez NWD: $R = \mathbb{Z}[\sqrt{-3}]$, $a = 4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$, $b = 2 \cdot (1+\sqrt{-3})$

3.3 Element $p \in R$ jest pierwszy gdy ideał (p) jest pierwszy tzn $p|ab \implies p|a \ \vee \ p|b$.

3.4 W pierścieniu bez dzielników zera jeśli p jest pierwszy i $a|p$ to albo $a \sim p$, albo a jest odwracalny. Dw: $p = ab$ to $p|a$ lub $p|b$. W pierwszym przypadku $pc = a$, więc $p = pcb$, stąd $1 = bc$, czyli b odwracalny.

3.5 W $\mathbb{Z}[\sqrt{-3}]$ liczba 2 jest nierozkładalna, ale nie jest pierwsza: $2|4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ i nie dzieli czynników.

3.6 Element nierozkładalny a spełnia $a = bc$ to b lub c jest odwracalny. Tzn

$$a = bc \iff (a \sim c \ \vee \ a \sim b)\,.$$

3.7 Pierścienie bez dzielników zera i z jednoznacznością rozkładu, w skrócie DJR, ang UFD. Np $\mathbb{Z}$, $k[x_1, x_2, \ldots x_n]$. Konrtprzykład $k[x^2, x^3] = k[s, t]/(s^3 - t^2)$, $\mathbb{Z}[\sqrt{-3}]$.

3.8 $\mathbb{Z}$ i $k[x]$ są DJR. (Będzie tw Gaussa: R DJR to $R[x]$ DJR.)

3.9 R jest DJR $\Rightarrow$ $(\star)$ każdy ciąg ideałów głównych $(a_1) \subset (a_2) \subset (a_3) \subset (a_4) \subset \ldots$ stabilizuje się.
$(\star)$=ACC=ascending chain condition

3.10 $(\star) \Rightarrow$ każdy element rozkłada się na nierozkładalne. (Jednak rozkład nie musi być jednoznaczny.)

3.11 W DJR spełniony jest warunek
$(\star\star)$ każdy nierozkładalny element jest pierwszy ($a|bc$ to a występuje w rozkładzie bc, więc $a|b$ lub $a|c$).

3.12 $(\star)$ i $(\star\star) \iff R$ jest DJR.
Bo z $(\star)$ rozkład istnieje. Czynniki są pierwsze. Gdy $x_1x_2\dots x_n = y_1y_2\dots y_m$ to x_1 musi dzielić któryś y_k, więc być z nim stowarzyszony. Dalej indukcja ze względu na długość.

3.13 DIG = Dziedzina ideałów głównych. Przykład $\mathbb{Z}$, $k[x]$. Kontrprzykład: $(x, y) \subset k[x, y]$ nie jest główny.

3.14 DIGi są DJRami:
$(\star)$ jest spełnione, bo $\bigcup(a_i) = (b) \Rightarrow \exists i\ b \in (a_{i_0})$, on dzieli wszystkie a_i.
$(\star\star)$ (a) jest zawarty w pewnym ideale maksymalnym $\mathfrak{m} = (b)$, tzn $a = bc$. Gdy a nierozkładalny, b nieodwracalny, więc $a \sim b$ z (3.4).

3.15 Dodatkowo dostaliśmy: w DIG ideał generowany przez element nierozkładalny jest maksymalny.

3.16 Największy wspólny dzielnik podzbioru $A \subset R$ w DIGu to taki element b, że $(A) = (b)$.

3.17 Pierścienie Euklidesowe: to pierścienie z dzieleniem z resztą. Dana norma (waluacja) $v : R \setminus \{0\} \to \mathbb{N}$, taka, że dla każdego $a, b \in R$ albo $b|a$ albo istnieją $c, r \in R$ takie, że $a = bc + r$ i $v(r) < v(b)$.

3.18 Przykłady $\mathbb{Z}$, $\mathbb{Z}[i]$, $k[x]$
– $\mathbb{Z}[\sqrt{-2}]$, $v(a + b\sqrt{-2}) := a^2 + 2b^2$, ogólniej $\mathbb{Z}[\sqrt{d}]$, $v(a + \sqrt{d}b) = |a^2 - db^2|$ dla $d = -2, -1, 2, 3$ (w tym napisie $|x|$ oznacza zwykłą wartość bezwzględną w $\mathbb{Z}$).
– $\mathbb{Z}[\xi]$ gdzie ξ pierwiastek prymitywny z 1 stopnia 3, $v(a + b\xi) := a^2 - ab + b^2$

3.19 Algorytm Euklidesa tak jak w $\mathbb{Z}$. Największy wspólny dzielnik, jako wynik algorytmu.

3.20 Wykorzystanie algorytmu Euklidesa do przedstawienia $NWD(a, b)$ jako $ca + bd$. Zastosowanie: liczenie odwrotności w $R/(a)$.
(17,7)=(7,3)=(3,1)=(1)
17=2*7+3 więc 3=17-2*7
7=2*3+1 więc 1=7-2*3=7-2*(17-2*7)=5*7-2*17
stąd $7^{-1} = 5$ w $\mathbb{Z}_{17}$

3.21 Liczby Gaussa $\mathbb{Z}[i]$ (było na ćwiczeniach)
– Elementy pierwsze w $\mathbb{Z}[i]$ to dzielniki liczby pierwszej $p \in \mathbb{Z}$.
– Ponadto p jest rozkładalna w $\mathbb{Z}[i]$ wtedy i tylko wtedy gdy $p = a^2 + b^2$.
– Jeśli $p = 4k + 1$ to p rozkładalna (dow. $(p-1)! \equiv_p -1$, $p|((2k)!)^2 + 1 = ((2k)! + i)((2k)! - i)$, ale $p \not| (2k)! + i$ więc p nie jest elementem pierwszym.)

3.22 Jeśli $f \in k[x]$ nierozkładalny, to $k[x]/(f)$ jest ciałem. (Bo $k[x]$ jest DIGiem, więc element nierozkładalny generuje ideał maksymalny.)

3.23 Twierdzenie: f w $k[x]$ jest nierozkładalny $\Rightarrow k[x]/(f)$ jest ciałem.

3.24 Wniosek: pierścień ilorazowy $k[x]/(f)$ jest nadciałem k, w którym f ma pierwiastek.

3.25 Przykłady: $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$, $\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2+x+1)$, $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$, $\mathbb{F}_{27} = \mathbb{Z}_3[x]/(x^3 - x+1)$.

3.26 Jeśli $f \in k[x]$ jest nierozkładalny stopnia n, to ciało $k[x]/(f)$ jako przestrzeń liniowa nad k ma wymiar n.

3.27 W ciele p^n-elementowym każdy element $\neq 0$ spełnia tożsamość $x^{p^n-1} = 1$ (bo grupa multiplikatywna jest rzędu $p^n - 1$), zatem wielomian $x^{p^n} - x$ rozkłada się na p^n **różnych** czynników liniowych (z tw Bezout).

3.28 Przykład $p = 3$, $n = 2$: $f = x^9 - x = (x^3 - x)(1 + x^2 + x^4 + x^6)$. Pierwszy czynnik ma pierwiastki w $\mathbb{F}_3$

$$x^3 - x = (x-1)(x+1)x\,,$$

drugi czynnik ma pierwiastki w $\mathbb{F}_9 \setminus \mathbb{F}_3$. Rozkładamy dalej

$$(1 + x^2 + x^4 + x^6) = (x^2+1)(x^4+1) \equiv_3 \underbrace{(x^2+1)}_{f_1}\underbrace{(x^2+x-1)}_{f_2}\underbrace{(x^2-x-1)}_{f_3}\,.$$

Ciało $\mathbb{F}_3[x]/(f_k)$ ma 9 elementów (dla $k = 1, 2, 3$) i w nim wielomian f rozkłada się na czynniki liniowe.

Ćwiczenie: rozłożyć wielomian $x^2 + x - 1$ na czynniki liniowe w $\mathbb{F}_3[y]/(y^2+1)$.
(Dla uproszczenia nazwijmy obraz y w $\mathbb{F}_3[y]/(y^2+1)$ przez „i".)

4

Lokalizacja

4.1 $S \subset R$ system multiplikatywny $a, b \in S \Rightarrow ab \in S$. Gdyby $0 \in S$, to dalsza konstrukcja byłaby poprawna ale trywialna. Więc zakładamy, że $0 \notin S$. Np:
– $S = R \setminus I$, gdzie I jest ideałem pierwszym
– w szczegolności $S = R - 0$ gdy R jest bez dzielników zera
– $S = \{a^n \mid n \in \mathbb{N}\}$, gdzie a nie jest nilpotentny.

4.2 Pierścień $R_S = S^{-1}R$ to zbór ilorazowy $R \times S/\sim$, $(a, s) \sim (b, t)$, gdy istnieje $u \in S$ taki, że $uat = ubs$. Klasa $[(a, s)]$ oznaczana przez $\frac{a}{s}$

4.3 Jesli R bez dzielników zera, to mozna: $(a, s) \sim (b, t)$ gdy $at = bs$.

4.4 Dla R bez dzielników zera $S = R - 0$ ciało R_S oznaczane jest przez (R).

4.5 $k(x) := (k[x])$ ciało funkcji wymiernych o współczynnikach w k.

4.6 Przykłady lokalizacji $\mathbb{Z}$: $\mathbb{Z}_{(p)}$, $\mathbb{Q}$, $\mathbb{Z}[1/p]$.

4.7 Przekształcenie $\iota : R \to R_S$ ma jądro $Ann(S) = \{a \mid \exists s \in S\ sa = 0\}$. (Lokalizację można zrobić w dwóch krokach: najpierw podzielić przez $Ann(S)$, a potem użyć prostszej relacjii 4.3.

4.8 Uniwersalna własność: dane przekształcenie $f : R \to R'$, takie że $f(s)$ jest odwracalne. Wtedy istnieje dokładnie jedno $\bar{f} : R_S \to R'$ takie, że $f = \bar{f}\iota$.

4.9 Pierścienie lokalne i lokalizacja w ideale maksymalnym: $S = R \setminus \mathfrak{m}$.

4.10 Motywacja nazwy ,,pierścień lokalny,,: Niech X przestrzeń topologiczna $T_{3\frac{1}{2}}$ (tzn przestrzeń Tichonowa, tzn dla dowolnego zbioru domknietego i punktu poza nim istnieje funkcja zerująca się na tym zbiorze i nie zerująca się w danym punkcie), pierścień kiełków w x jest izomorficzny z $= C(X, \mathbb{R})/\mathfrak{m}_x$.

4.11 Dla $X = \mathbb{C}^n$ lub $\mathbb{R}^n$ zamiast funkcji ciągłych można brać funkcje C^∞, analityczne (tzn rozwijalne w szereg), algebraiczne (zadane wielomianem) itp.

Wielomiany o współczynnikach w pierścieniu DJR, podzielność

4.12 Każdy wielomian dzieli się z resztą przez $(x - a)$.

4.13 Ogólniej, jeśli wielomain g ma odwracalny wiodący współczynnik, to można dzielić z resztą przez g.

4.14 Tw Bezout $f(a) = 0$ to f dzieli się przez $x - a$ w $R[x]$. (Reszta z dzielenia f przez $x - a$ jest równa $f(a)$.)

4.15 Wniosek: Jeśli R jest nieskończonym pierścieniem bez dzielników zera, to przekształcenie $R[x] \to R^R$ (wielomian $f \mapsto$ funkcja wielomianowa $\bar{f}$) jest różnowartościowe.

Założenie: od tej pory do kryterium Eisensteina R DJR

4.16 Mówimy, że $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ jest prymitywny, jeśli a_i nie mają wspólnych czynników, tzn $NWD(a_0, a_1, \ldots, a_n) = 1$. Każdy wielomian można przedstawić jako $f = a \cdot prymitywny$.

4.17 Element $a = cont(f) = NWD($współczynniki$)$ z powyższego rozkładu nazywane jest zawartością wielomianu f.

4.18 Lemat: $cont(fg) = cont(f)cont(g)$.
Dowód: zakładamy, że f, g prymitywne. Niech $p|cont(fg)$. Redukujemy iloczyn fg modulo p. ↯

4.19 Każdy wielomian można przedstawić jako produkt nierozkładalnych: elementów pierwszych z R i nierozkładalnych wielomianów prymitywnych. Pokażemy, że to rozkład na elementy pierwsze w $R[x]$.

4.20 Jeśli $p \in R$ jest pierwszy w R, to jest pierwszy w $R[x]$ (redukujemy $R[x]/(p) = (R/(p))[x]$ nie ma dzielników zera).

4.21 Jeśli $f, g \in R[x]$, f prymitywny. Niech $F = (R)$, $f|g$ w $F[x]$. Wtedy $f|g$ w $R[x]$
Dow: $cg = fh$ dla $c \in R$, $h \in R[x]$ i załóżmy, że c ma minimalną ilość czynników pierwszych. Przypuśćmy, że $p|c$, wtedy $p|h$ (bo $p \not| f$). ↯

4.22 Lemat Gaussa: $0 \neq f \in R[x]$ i $f = gh$ w $F[x]$, to $f = g_0 h_0$ w $R[x]$, oraz $ag = g_0$, $bh = h_0$. (Wystarczy dla $g = g_0$ prymitywnego; z poprzedniego punktu.)

4.23 Jeśli $f \in R[x]$ prymitywny i nierozkładalny w $R[x]$, to pierwszy.
– f nierozkładalny w $F[x]$ (z Gaussa)
– $F[x]$ jest DIG, więc tam f jest pierwszy: $f|gh \Rightarrow f|g$ lub $f|h$. Podzielnośś w $F[x]$ implikuje podzielność w $R[x]$.

4.24 Wniosek: $f = x^n + \cdots + a_0$ ma pierwiastek w $F[x]$, to ma pierwiastek w $R[x]$.
Dw. Przypuśćmy, że $a \in F$ jest pierwiastkiem f, tzn $f = (x-a)g$ dla $g \in F[x]$. Piszemy $a = \frac{b}{c}$ dla $b, c \in R$, $(b,c) = 1$. Wtedy $(bx-c)|f$, $bx - c \in R[x]$. Zatem $f = (bx-c)h$ dla pewnego $h \in R[x]$, $h = dx^{n-1} + \ldots$. Współczynnik przy x^n w $(bx-c)h$ jest równy $bd = 1$. Zatem b jest odwracalny.

4.25 Wniosek: $R[x]$ jest DJR ($\star$ ACC i $\star\star$ nierozkładalne są pierwsze)

4.26 Wniosek: $R[x_1, x_2, \ldots, x_n]$ jest DJR.

5

5.1 Kryterium Eisensteina: założenia $f \in R[x]$, $p \not| a_n$, p dzieli pozostałe współczynniki wielomianu, ale $p^2 \not| a_0$. Wtedy f nierozkładalny w $F[x]$.
– po redukcji mod (p) $\bar{f} = \bar{a}_n x^n \neq 0$ w $R/(p)[x]$. Czynniki $\bar{f} = \bar{g}\bar{h}$, mają zerowe wyrazy wolne. Stąd wyraz wolny f podzielny przez p^2.

Ciała

5.2 Dla pary ciał $K \subset L$ definiujemy stopień rozszczerzenia $(L:K) = \dim_K L$.

5.3 Gdy $K \subset M \subset L$ to $(L:K) = (L:M)(M:K)$.

5.4 Niech $K \subset L$. Element $a \in L$ jest algebraiczny nad K gdy istnieje $f \in K[x]$ t.ż. $f(a) = 0$.

5.5 Załóżmy, że a jest algebraiczny nad K. Ideał $\{g \in K[x] \mid g(a) = 0\} = \ker(ev_a : K[x] \to L)$ jest główny, generowany przez pewien f o minimalnym stopniu. Ten wieleomian nazywa się wielomianem minimalnym, $K[x]/(f)$ jest ciałem. Obraz $K[x]$ w L jest podciałem, oznaczanym przez $K(a)$.

5.6 Element $a \in L$ jest algebraiczny nad K wtedy i tylko wtedy, gdy $(K(a):K) < \infty$. Ponadto $(K(a):K) = deg(f)$ jeśli f jest wielomioanem minimalnym.

5.7 Jeśl $a_1, a_2, \ldots, a_n \in L$ są algebraiczne nad K, to podpierścień

$$M = im(K[x_1, x_2, \ldots, x_n] \xrightarrow{ev_a} L$$

jest podciałem i $(M:K) < \infty$.
Wniosek: jeśli a i b algebraiczne, to $a+b$ i ab są algebraiczne.

5.8 Różne typy rozszerzeń:
– rozszerzenia pojedyńcze $K(a)$ (każde rozszerzenie skończone nad ciałem charakterystyki 0 jest pojedyńcze – patrz [Browkin str 84, Tw. 22], np $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, ogólnie trzeba bracć $K(a,b) = K(a+tb)$ dla pewnego $t \in K$.)

– rozdzielcze: każdy $a \in L$ jest jednokrotnym pierwiastkem swojego wielomianu minimalnego. Tak jest zawsze dla ciał charakterystyki 0 i dla ciał skończonych. Kontrprzykładem jest $\mathbb{F}_p(x^p) \subset \mathbb{F}_p(x)$ (ciało funkcji wymiernych).
– rozszerzenie normalne: jeśli wielomian nierozkładalny $f \in K[x]$ ma pierwiastek w L, to rozkłada się na czynniki liniowe. Kontrprzykład $\mathbb{Q}(\sqrt[4]{2})$.

5.9 Ciało K jest algebraicznie domknięte, gdy każdy wielomioan ma pierwiastek. Równoważnie, każdy wielomian rozkłada się na czynniki liniowe.

5.10 Jeśli $K \subset L$ jest algebraicznym rozszerzeniem oraz każdy $f \in K[x]$ rozkłada się na czynniki liniowe w L, to L jest algebraicznie domknięte.
Dowód, przypuśćmy, że nierozkładalny $f \in L[x]$ nie ma pierwiastka. Niech L_0 będzie ciałem generowanym przez współczynniki f. Niech $M = L_0[x]/(f)$, $a := x \mod (f)$. Ciało M jest skończonym rozszerzeniem ciała K. Zatem a jest algebraiczny nad K i ma swój wielomian minimalny g. Z założenia g rozkłada się na czynniki liniowe w L, zatem $a \in L$. ↯

5.11 Dla każdego wielomianu $f \in K[x]$ istnieje rozszerzenie algebraiczne L takie, że L rozkłada się na czynniki linowe w $L[x]$.

5.12 Konstrukcja algebraicznego domknięcia. Konstruujemy ciało L takie, że każdy $f \in K[x]$ rozkłada się na czynniki linowe w $L[x]$.

5.13 Przykład rozszerzeń niealgebraicznych: $\mathbb{Q}(\pi) \subset \mathbb{R}$, $\mathbb{Q}(\pi) \simeq \mathbb{Q}(x)$.

5.14 Każde dwa ciała charakterystyki 0, które s'a algebraicznie domknięte i mocy continnuum są izomorficzne:

$$\mathbb{Q}_p^\wedge\,, \qquad \mathbb{Q}(\{x_i\}_{i\in I})\,,$$

gdzie $\mathbb{Q}_p^\wedge$ jest ciałem ułamków $\mathbb{Z}_p^\wedge$ oraz $|I| = \mathfrak{c}$ mają algebraiczne domknięcia izomorficzne z $\mathbb{C}$.

5.15 Jeśli rozszerzenie L jest rozdzielcze i normalne bada się automorfizmy L, które są stałe na K. Jest to tzw grupa Galois $Aut_K(L) = G(L/K)$. Grupa Galois permutuje pierwiatki każdego nierozkładalnego wielomianu.

5.16 Przykład $G(\mathbb{Q}(\xi_n)/\mathbb{Q}) \simeq \mathbb{Z}_n^*$, gdzie ξ_n jest pierwiastkiem pierwotnym z 1 stopnia n.

5.17 Dla $L = \mathbb{Q}(\sqrt[4]{2}, i)$ mamy $G(L/K) = D_8$.

5.18 Niech $\sigma_i(x_1, \ldots, x_n)$ będzie elementarną funkcją symetryczną. Niech $K = \mathbb{Q}(\sigma_1, \ldots, \sigma_m) \subset \mathbb{Q}(x_1, \ldots, x_m)$. Wtedy $GL/K) = \Sigma_n$.

5.19 $G(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \mathbb{Z}^\wedge$

5.20 $K \subset M \subset L$. Dla podgrupy $H < Gal(L, K)$ zbiór punktów stałych L^H jest ciałem. Dla podciała $M \subset L$ zbiór elementów grupy $G(L/K)$ stałych na L jest podgrupą.

5.21 Jeśli $K \subset L$ jest rozdzielcze i normalne to wyżej opisana odpowiedniość jest bijekcją pomiędzy podgrupami $G(L/K)$ a podciałami M zawierającymi K. W tej odpowiedniości podgrupy normalne odpowiadają rozszerzeniom normalnym.
Patrz teoria Galois.

6 Pierścienie Noetherowskie: odsyłacz [Eisenbud: Commutative Algebra with a View Toward Algebraic Geometry]

6.1 Pierścienie noetherowskie (definicja): każdy rosnący ciąg ideałów stabilizuje się. (Tzn. ACC, nie tylko dla ideałów głównych.)

6.2 Równoważny warunek: każdy ideał jest skończenie generowany.

6.3 W pierścieniu noetherowskim każdy element można przedstawić jako iloczyn elemntów nierozkładalnych (niekoniecznie pierwzych, np $k[x^2, x^3]$

6.4 Twierdzenie Hilberta o bazie: R noetherowski, to $R[x]$ noetherowski.
Dow. Skonstruujemy zbiór elementów f_m oraz ideał $I_m = (f_1, f_2, \dots, f_m) \subset I$. Pokarzemy, że dla pewnego n mamy $I_n = I$. Wielomian f_m dobieramy tak: to wielomian o najmniejszym stopniu należący do $I \setminus I_{m-1}$ jeśli $I_m \subsetneq I$. (W przeciwnym przypadku kończymy konstrukcję $\ddot\smile$.) Zauważmy $\deg f_\ell \geq \deg f_k$ dla $\ell > k$. Niech J będzie ideałem wiodących współczynników $J = (a_1, a_2, \dots)$ wielomianów f_m. Skoro R jest noetherowski, to $J = (a_1, a_2, \dots, a_n)$: wielomian $f_{n+1} \in I \setminus I_n$ ma wiodący współczynnik $a_{n+1} = \sum_{k \leq n} b_k a_k$. Biorąc kombinację wielomianów $\sum_{k \leq n} b_k f_k x^{\deg f_{n+1} - \deg f_k}$ dostajemy wielomian g z wiodącym współczynnikiem a_{n+1} i o tym samym stopniu, co f_{n+1}. Wielomian $f_{n+1} - g$ ma niższy stopień niż f_{n+1} co przeczy wyborowi f_{n+1}.

6.5 Wniosek $k[x_1, x_2, \dots, x_n]$ jest noetherowski.

6.6 Pierścień ilorazowy noetherowskiego są noetheowskie.

6.7 Pierścienie skończenie generowane nad noetherowskim są noetherowskie.

Związki z geometrią

6.8 Topologia Zariskiego w k^n: zbiory domknięte, to zbiory algebraiczne (tzn opisane skończonymi układami równań wielomianowych).
– jeśli $F_1, F_2 \in \mathfrak{F}$, to $F_1 \cup F_2 \in \mathfrak{F}$
– jeśli $A \subset \mathfrak{F}$, to $\bigcap_{F \in A} F \in \mathfrak{F}$
– $\emptyset, k^n \in \mathfrak{F}$

6.9 Indukowana topologia w podzbiorach algebraicznych.

6.10 Twierdzenie Hilberta o zerach *Nullstellensatz* (cz I). Gdy $k = \overline{k}$ to ideały maksymalne w $A = k[x_1, x_2, \dots x_n]$ są postaci $(x_n - a_n, x_1 - a_n, \dots, x_n - a_n)$ dla $(a_1, a_2, \dots, a_n) \in k^n$

$$\{\text{Ideały maksymalne w } A\} \;=\; k^n$$

(Równoważnie: każdy właściwy ideał ma wspólne zero.)
Oznaczenie: zbiór idałów maksymalnych $SpecMax\, A$.

6.11 Dowód wynika z tw Zariskiego: Jeśli $K \subset L$ jest rozszerzeniem ciał oraz L jest skończenie generowane jako pierścień nad K, to L jest roszerzeniem algebraicznym.
(złożenie $\phi : k \hookrightarrow k[x_1, x_2, \dots, x_n] \twoheadrightarrow k[x_1, x_2, \dots, x_n]/\mathfrak{m}$ jest izomorfizmem, $a_i := \phi^{-1}(x_1 + \mathfrak{m})$)

6.12 Jeśli $A = k[x_1, x_2, \ldots x_n]/I$, $I = (f_1, f_2, \ldots, f_m)$, to

$$\{\text{Ideały maksymalne w } A\} \;=\; X,$$

gdzie

$$X = \{(a_1, a_2, \ldots, a_n) \in k^n \mid \forall j = 1, 2, \ldots, m \quad f_j(a_1, a_2, \ldots, a_n) = 0\}.$$

6.13 Dla $X \subset k^n$ niech

$$\mathfrak{I}(X) = \{f \in k[x_1, x_2, \ldots, x_n] \,:\, \forall a \in X \;\; f(a) = 0\}.$$

To jest ideał.

6.14 Dla $E \subset k[x_1, x_2, \ldots, x_n]$ niech $V(E)$ zbiór zer:

$$V(E) = \{(a_1, a_2, \ldots, a_n) \in k^n \mid \forall f \in E \; f(a_1, a_2, \ldots, a_n) = 0\}.$$

Jeśli I jest ideałem generowanym przez E, to $V(E) = V(I)$.

6.15 Z THoZ(cz I): jeśli $k = \bar{k}$ i $V(I) = \emptyset$ to $1 \in I$.

6.16 Twierdzenie Hilberta o zerach *Nullstellensatz* (cz II): Niech $I \subset k[x_1, x_2, \ldots, x_n]$ będzie ideałem. Mamy

$$\mathfrak{I}(V(I)) = \sqrt{(I)}.$$

(Dow: Dla $f \in \mathfrak{I}(V(I)) = (f_1, f_2, \ldots, f_k)$ niech $J = (I, 1 - fy) \subset k[x_1, x_2, \ldots, x_n, y]$. Mamy

$$V(J) = (V(I) \times k) \cap V(1 - fy) \subset (V(f) \times k) \cap V(1 - fy) = \emptyset \subset k^{n+1}\,,$$

więc $1 \in J$

$$1 = \sum g_i f_i + h(1 - fy).$$

Bierzemy obraz w

$$k[x_1, x_2, \ldots, x_n, 1/f] = k[x_1, x_2, \ldots, x_n, y]/(1 - fy)\,.$$

mamy tożsamość $1 = \sum g_i f_i$, gdzie g_i zależą od $1/f$. Mnożąc przez f^N dostajemy tezę.)

6.17 Wniosek: Jeśli $X = V(I)$ jest zbiorem algebraicznym, to $V(\mathfrak{I}(X)) = X$. Ogólnie $V(\mathfrak{I}(X)) = \overline{X}$ jest domknięciem w topologi Zariskiego.

6.18 Abstrakcyjna definicja topologii Zariskiego w $SpecMax(A)$ nie odwołująca się do przedstawienia $A = k[x_1, x_x, \ldots, x_n]/(f_1, f_2, \ldots, f_k)$. Każdy ideał $I \subset A$ definiuje zbiór domknięty w $SpecMax(A) =$ {zbiór ideałów maksymalnych }. Zbiory otwarte w języku ideałów

$$V(I) = \{\mathfrak{m} \in SpecMax(A) \,|\, I \subset \mathfrak{m}\}.$$

6.19 Zbiory otwarte w języku ideałów

$$U(I) = \{\mathfrak{m} \in SpecMax(A) \,|\, I \not\subset \mathfrak{m}\}.$$

Baza topologii

$$U(f) = \{\mathfrak{m} \in SpecMax(A) \,|\, f \notin \mathfrak{m}\},$$

gdzie $f \in A$.

6.20 Zbiory algebraiczne można rozkładać na składowe:
– $V(xy) = V(x) \cup V(y)$ suma osi, bo $(xy) = (x) \cap (y)$
– $V(x^2y, x^2z) = V(x^2) \cup V(y, z)$ suma prostej $y = z = 0$ i podwójnej płaszczyzny,
bo $(x^2y, x^2z) = (x^2) \cap (y, z)$
– $V(xy, x^2) = V(x)$ ale $(xy, x^2) = (x) \cap (x^2, xy, y^2)$

6.21 Ideał prymarny: $ab \in I$, $b \notin I$ to $a^n \in I$ dla penego n (jedyne dzielniki zera w R/I to nilpotenty).

Rozkład ideału w pierścieniach noetherowskich - Rozkład prymarny [np R. Sharp: Steps in Commutative Algebra, roz. 4, Atiyah-MacDonald, roz 4]

6.22 R noetherowski, to każdy ideał dopuszcza przedstawienie $I = \bigcap Q_i$, gdzie Q_i nierozkładalny (Q_i nie da się przedstawić jako przecięcie większych ideałów).

6.23 Twierdzenie: R noetherowski, każdy Q nierozkładalny ideał jest prymarny.

7 Rozkład prymarny

7.1 Ex1 $R = K[x, y, z]/(xz - y^2)$, $P = (x, y)$ prymarny (a nawet pierwszy), ale P^2 nie.

7.2 Ex2 $R = K[x, y, z]$, $I = (x^2z^2, x(x + y^2), z(z - y^2))$.
Np w programie sage (`http://sage2.mimuw.edu.pl/`) trzeba napisać:

```
R.<x,y,z> = PolynomialRing(QQ)
I=(x^2*z^2,x*(x+y^2),z*(z-y^2))*R;
I.primary_decomposition()
```

A potem:

```
I.associated_primes()
```

7.3 Jeśli R jest noetherowski, to każdy ideał dopuszcza przedstawienie jako przecięcie ideałów nierozkładalnych.
[Dowód taki jak: (ACC) $\Rightarrow$ każdy element jest iloczynem elementów nierozkładalnych.]

7.4 $V(I) \cup V(J) = V(I \cdot J) = V(I \cap J)$, zatem mając przedstawienie ideału

$$I = \bigcap Q_i$$

otrzymujemy rozkład

$$V(I) = \bigcup V(Q_i).$$

Jeśli ideały Q_i są nierozkładalne, to $V(Q_i)$ są zbiorami nierozkładalnymi. Udowodnimy, że ideały Q_i są prymarne, zatem $P_i = \sqrt{Q_i}$ są ideałami pierwszymi. Te ideały są nazywane stowarzyszonymi ideałami pierwszymi (pokażemy, że dla nieskracalnych rozkładów $ass(I)$ nie zależy od rozkładu). Mamy

$$V(I) = \bigcup_{P \in ass(I)} V(P).$$

W tym rozkładzie mogą się pojawić $P \subset P'$ (tzn $V(P) \supset V(P')$) więc wystarczy brać w rozkładzie $V(I)$ tylko minimalne ideały stowarzyszone.

7.5 Zbiór $(I : b) = \{x \in R \mid bx \in I\}$ jest idałem. Dla I prymarnego
– $\sqrt{(I : b)} = \sqrt{I}$ gdy $b \notin I$
– $(I : b) = R$ gdy $b \in I$

7.6 Twierdzenie: R noetherowski, każdy nierozkładalny ideał Q jest prymarny.
Dow: Niech $ab \in Q$, $b \notin Q$. Ciąg $\cdots \subset (Q : a^n) \subset (Q : a^{n+1}) \subset \ldots$ stabilizuje się. Załóżmy, że $(Q : a^n) = (Q : a^{n+1})$. Dowodzimy (*) $Q = (Q + (a^n)) \cap (Q + (b))$. Wtedy skoro $b \notin Q$, to $Q + (b) \neq Q$, więc $Q = Q + (a^n)$, czyli $a^n \in Q$.
(*) $r = g + ca^n = h + db \Rightarrow ca^{n+1} = ha + dab - ga \in Q \Rightarrow c \in (I : a^{n+1}) = (I : a^n) \Rightarrow r \in Q$.

7.7 Niech P będzie ideałem pierwszym. Mówimy, że Q jest ideałem P-prymarnym, jeśli $\sqrt{P} = Q$.
Lemat: Przecięcie ideałów P-prymarnych jest ideałem P-prymarnym.
Dowód: $ab \in Q_1 \cap Q_2$, $b \notin Q_1 \Rightarrow a^n \in Q_1 \Rightarrow a \in P = \sqrt{Q_1} = \sqrt{Q_1 \cap Q_2} = \sqrt{Q_2}$.

7.8 Mówimy, że rozkład $I = \bigcap Q_i$ jest minimalny, jeśli
1) wszystkie $P_i = \sqrt{Q_i}$ są różne,
2) dla każdego i mamy $\bigcap_{j \neq i} Q_j \not\subset Q_i$ (rozkład nieskracalny)
Każdy rozkład I na ideały prymarne można przerobić na rozkład minimalny.

7.9 Twierdzenie (bez dowodu): jeśli $I = \bigcap Q_i$ będzie nieskracalnym rozkładem na ideały prymarne, to zbiór ideałów pierwszych $\sqrt{Q_i}$ jest jednoznacznie wyznaczony.

8 Różne

8.1 Lemat: Jeśli $\sqrt{I} + \sqrt{J} = (1)$ to $I + J = 1$.
Dw: $a + b = 1$, $a^n \in I$, $b^m \in J$ to $1 = (a + b)^{m+n} \in I + J$.

8.2 Jeśli $\sqrt{I} = \mathfrak{m}$ jest ideałem maksymalnym, to I jest prymarny.
Dw: Niech $ab \in I$, $a \notin \sqrt{I}$, wtedy $(a) + \sqrt{I} = (1)$. Z lematu $(a) + I = (1)$, czyli $1 = ax + y$, $y \in I$. Stąd $b = abx + by \in I$.

Rozszerzenia przestępne ciał

8.3 Ciało funkcji wymiernych $k(x)$. Jeśli $\alpha \in k(x) \setminus k$, to rozszerzenie $k(\alpha) \subset k(x)$ jest algebraiczne.
Dow. $\alpha = f(x)/g(x)$, więc x spełnia równanie wielomianowe

$$\alpha g(x) = f(x)\,.$$

8.4 Twierdzenie Lürotha: Każde podciało $k \subsetneq L \subset k(x)$ jest izomrficzne z cia'lem funkcji wymiernych jednej zmiennej.
Dowód [Van der Waerden: Modern Algebra, Vol I (1949), §63 str. 198] korzysta z lematu Gaussa 4.21 oraz z następującego faktu:

8.5 Jeśli $g, h \in k[x]$ są względnie pierwsze to jeśli $f[z]$ dzieli $g[x]h[z] - h[x]g[z] \in k[x, z]$ to f jest stałą.
Dow: założyć, że k jest algebraicznie domknięte.

8.6 Niech L będzie skończenie generowanym rozszerzeniem ciała k. Mówimy, że układ elementów $a_1, a_2, \ldots, a_n$ jest algebraicznie zależny (nad k), jeśli istnieje nietrywialny wielomian $f(x_1, x_2, \ldots, x_n) \in k[x_1, x_2, \ldots, x_n]$, taki, że $f(a_1, a_2, \ldots, a_n) = 0$.
Uwaga: Możemy też rpzważać układy nieskończone.

8.7 Jeśli układ elementów $a_1, a_2, \ldots, a_n$ jest algebraicznie zależny, to $k(a_1, a_2, \ldots, a_n)$ jest izomorficzny z ciałem ułamków pierścienia wielomianów $k[x_1, x_2, \ldots, x_n]$.

8.8 Załóżmy, że $\{a_1, a_2, \ldots, a_n\} \subset L$ jest układem algebraicznie niezależnym. Element $b \in L$ jest algebraicznie zależny, jeśli istnieje nietrywialny wielomian o współczynnikach w $k(a_1, a_2, \ldots, a_n)$, którego pierwiastkiem jest b.

8.9 Fundamentalny lemat (analog lematu o wymianie z algebry liniowej):
1) Załóżmy, że $\{a_1, a_2, \ldots, a_n\} \subset L$ jest układem algebraicznie niezależnym.
2) Załóżmy, że $\{a_1, a_2, \ldots, a_{n-1}, b\} \subset L$ jest układem algebraicznie nie zależnym.
3) Załóżmy, że $\{a_1, a_2, \ldots, a_n, b\} \subset L$ jest układem algebraicznie zależnym.
Wtedy a_n jest algebraiczne nad $k(a_1, a_2, \ldots, a_{n-1}, b)$.
Dw: Przyjmijmy $K = k(a_1, a_2, \ldots, a_{n-1})$. Z 3) istnieje wielomian $f[x, y] \in K[x, y]$, taki, że $f(a_n, b) = 0$. Wielomian musi zawieać zarówno x jak i y, bo inaczej 1) i 2) nie byłyby spełnione.

8.10 Dla każdego rozszerzenia $k \subset L$ istnieje maksymalny układ elementów algebraicznie niezależnych. Takie układy nazywają się bazami przestępnymi. Bazy przestępne są równoliczne. Liczebnośc bazy przest:epnej nazywa się stopniem przestępnym $degtr_k(L)$.

8.11 Każde rozszerzenie ciąła k można przedstawić jako złożenie

$$k \subset M = k(a_1, a_2, \ldots, a_n) \subset L = M/(f_1, f_2, \ldots f_r),$$

gdzie L jest rozszerzeniem algebraicznym, $f_i \in M[y_1, y_2, \ldots, y_m]$. Jeśli $char(k) = 0$, to można przyjąć, że rozszerzenie $M \subset L$ jest pojedyńcze i wtedy $m = 1$.

8.12 Geometryczna interpretacja M można traktować jako funkcje wymiernie na k^n, a L jako funkcje wymierne na podzbiorze $X \subset k^{n+m}$ opisanym przez funkcje wymierne f_i (zależące wielomianowo od y_j).

8.13 Ciała stopnia przestępnego 1 są izomorficzne z ciałami funkcji wymiernych na krzywych algebraicznych zdefiniowanych nad k.

8.14 Gdy $k = \mathbb{C}$ krzywe algebraiczne są powierzchniami Riemanna. Np krzywe eliptyczne opisane równaniem stopnia 3 w $\mathbb{C}^2$, można przyjąć, że równanie jest w postaci Weierstrassa $y^2 = x^3 + px + q$. Wtedy $L = \mathbb{C}(x)[y]/(y^2 - (x^3 + px + q))$.

Moduły

8.15 Moduły nad pierścieniem: przykłady
– wolny R^n

– ideał (to są dokładnie podmoduły R^1)
– R/I
– dla $R = k$: przestrzeń liniowa nad k
– dla $R = \mathbb{Z}$-moduł to grupa abelowa
– dla $R = k$, $k[x]$-moduł to przestrzeń liniowa nad k wraz z endomorfizmem.

8.16 Operacje na modułach
– suma prosta skończona = produkt skończony
– suma prosta nieskończona $\neq$ produkt nieskończony
– moduł ilorazowy
– jądro, kojądro
– iloczyn tensorowy
– operacje zmiany pierścienia bazowego

8.17 Klasyfikacja skończenie generowanych modułów nad pierścieniem DIG

$$M \simeq R^r \oplus \bigoplus_{i=1}^{N} R/(p_i^{k_i})$$

gdzie $p_i \in R$ element pierwszy, $k_i \in \mathbb{N}$.
(W przypadku gdy $M = R/I$, $I = \bigcap(a)$, $\prod p_i^{k_i}$ z tw chińskiego o resztach mamy tezę.)

8.18 Wnioski:
– Tw Jordana (dla $R = k[x]$), bo $p_i = (x - a_i)$, składnik wolny odpada, bo zakładamy $\dim M < \infty$
– Tw o klasyfikacji skończenie generowanych grup abelowych (dla $R = \mathbb{Z}$), bo p_i to liczby pierwsze.

8.19 Dla pierścieni noetherowskich mamy rozkład prymarny podmodułu w module skończenie generowanym. Jest to uogólnienie przypadku $I \subset M = R$.