(tylko) Konspekt wykładu Algebra I*: Pierścienie

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

v.22.1.2015

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.

1.2 Jedyność jedynki, $a \cdot 0 = 0$

1.3 Pierścień liczb cakowitych $\mathbb{Z}$ i pierścień reszt z dzielenia przez m, $\mathbb{Z}_m$.

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

1.5 Macierze kwadratowe nad ustalonym ciałem. (pierścień nieprzemienny)

1.6 Pierścień grupowy (pólgrupowy). Splot funkcji na grupie. (nieprzemienny jeśli grupa nieprzemienna)

1.7 Funkcje na przestrzeni topologicznej o nośniku zwartym $C_c(X)$. (nie ma 1 jeśli X nie jest zwarta)

1.8 Inne pierścienie bez jedynki: funkcje zbiegające do 0 w nieskończoności $C_0(X)$, fukcje szybko gasnące na $\mathbb{R}$.

1.9 Podpierścień. Podpierścienie $\mathbb{Q}$:
- $\mathbb{Z}[1/p]$,
- $\mathbb{Z}_{(p)}$

1.10 Pierścień wielomianów $k[x]$, pierścień szeregów formalnych $k[[x]]$, pierścień szeregów Laurenta $k((x))$, $k[\epsilon]$, $\epsilon^2 = 0$

1.11 Pierścień funkcji wielomianowych na podzbiorze $V \subset \mathbb{K}^n$ (w przyszłości Nullstellensatz)

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

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

1.13 Pierścienie funkcji (ciągłych, gładkich, ograniczonych)

1.14 Elementy odwracalne, elementy nierozkładalne.

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

Homomorfizmy pierścieni

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

1.17 Jądro homomorfizmu, ideał

1.18 Iloraz przez ideał R/I

1.19 Ideały pierwsze, ideały maksymalne, ideały główne

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

1.21 Twierdzenie: ideał I w A jest pierwszy (odp. maksymalny) $\iff$ A/I jest dziedziną (ciałem).

2 Pieścienie, ideały

– I maksymalny, $[a] \in R/I$ nie jest odwracalny to $(I, a) = I + Ra$ jest włściwym ideałem
– $a \in J \setminus I$, $J \neq R$, to $[a] \in R/I$ jest nieodwracalny, $\neq 0$

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

2.2 Ćwiczenie: przeciwobraz, obraz ideału?

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

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

2.5 Twierdzenie: każdy ideał właściwy jest zawarty w pewnym ideale maksymalnym.

2.6 Ciała mają wyłącznie trywialne ideał

2.7 Ćwiczenie: Każdy homomorfizm ciał do niezererowego pierścienia jest włożeniem.

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

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

2.10 Jeśli R zawiera tylko jeden ideał właściwy, to R jest ciałem.

2.11 $0 = 1 \Leftrightarrow R = \{0\}$.

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

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

2.14 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.

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

2.16 Ideały generowane przez podzbiór

2.17 np $(s+t-2s^2, s-t) \in k[s,t]$ czy tu iloraz jest ciałem? To samo pytanie dla szeregów formalnych?

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

2.19 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 Podzielność

3.1 Typy elementów: odwracalne (jedności), dzielniki zera, nilpotenty, elementy pierwsze, elementy nierozkładalne, idempotenty $a^2 = a$.
– odwracalne elementy nie są dzielnikami zera,
– elementy pierwsze są nierozkładalne.

3.2 Nilradykał pierścienia $\mathfrak{n} \subset R$ to zbiór elementów nilpotentnych. $\mathfrak{n}$ jest ideałem. $R/\mathfrak{n}$ nie ma elementów nilpotentnych.

3.3 Ćwiczenie: R zawiera dokładnie jeden ideał pierwszy wtedy i tylko wtedy, gdy każdy jego element nieodwracalny jest nilpotentny.

3.4 Ćwiczenie: Ideał Jacobsona $= \bigcap$ ideały maksymalne. $x \in J \Leftrightarrow \forall y \in R \ 1 - xy$ jest odwracalny.

3.5 Jeśli a idempotent to $R = aR \bigoplus (1-a)R$ oraz aR i $(1-a)R$ są pierścieniami. (Nie podpierścieniami, bo jedynka w aR nie jest jedynką w R. Za to rzutowanie na aR jest homomorfizmem pierścieni.)

3.6 Relacja stowarzyszenia $\sim$. Podzielność to relacja porządku na $R/\sim$ (dla pierścieni bez dzielników zera). $NWD(a,b) = c$ w jezyku relacji porządku oznacza $([d] \leq [a] \wedge [d] \leq [b]) \Rightarrow [d] \leq [c]$.

3.7 NWD. Przykład bez NWD: $R = \mathbb{Z}[\sqrt{-3}]$, $a = 4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$, $b = 2 \cdot (1+\sqrt{-3})$

3.8 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.

3.9 Elementy nierozkładalny a spełnia $a = bc$ to b lub c jest odwracalny. Tzn $a \sim c$ lub $a \sim b$.

3.10 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 $k[x^2, x^3] = k[s,t]/(s^3 - t^2)$, $\mathbb{Z}[\sqrt{-3}]$.

3.11 $\mathbb{Z}$ i $k[x]$ są DJR. (Będzie tw Gaussa: A DJR to $A[x]$ DJR.)

3.12 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

3.13 $(\star) \Rightarrow$ każdy element rozkłada się na nierozkładalne.

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

3.15 $(\star)$ i $(\star\star) \Leftrightarrow R$ jest DJR.

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

3.17 DIGi są DJRami:
$(\star)$ jest spełnione, bo $\bigcup(a_i) = (b) \Rightarrow \exists i\ b \in (a_i)$,
$(\star\star)$ $(a) \subset \mathfrak{m} = (b)$, gdy a nierozkładalny, to $a \sim b$. (dodatkowo dostaliśmy, że (a) jest maksymalny.)

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

3.19 Pierścienie Euklidesowe: to pierścienie z dzieleniem z resztą. Dana waluacja $v : R \to \mathbb{N}$, taka, że $v(ab) = v(a)v(b)$ oraz dla każdego $a, b \in R$ istnieją $c, r \in R$ takie, że $a = bc + r$ i $v(r) < v(b)$. Naogół piszemy $|a|$ zamiast $v(a)$.

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

3.21 Wykorzystanie algorytmu Euklidesa do przedstawienia $NWD(a, b)$ jako $ca + bd$. Zastosowanie: liczenie odwrotności w $\mathbb{Z}[\mathbb{Z}_n]$.

3.22 Przykądy: $\mathbb{Z}[\sqrt{d}]$, $v(a + \sqrt{d}b) = |a^2 - db^2|$ dla $d = -2, -1, 2, 3$ (w tym napisie $|x|$ oznacza zwyłą wartość bezwzględną w $\mathbb{Z}$).

4 Ciała, wielomiany i lokalizacja

4.1 Liczby Gaussa $\mathbb{Z}[i]$.
– 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.)

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

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

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

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

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

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

4.8 Przykład $p = 3$, $n = 2$: $f = x^9 - x = (x^3 - x)(1 + x^2 + x^4 + x^6)$. Pierwszy czynnik ma pierwiastki w $\mathbb{F}_3$, drugi w $\mathbb{F}_9 - \mathbb{F}_3$. Rozkładamy dalej

$$f = x^9 - x = (x^3 - x)(x^2 + 1)(x^4 + 1) \equiv_3 (x^3 - x)(x^2 + 1)(x^2 + x - 1)(x^2 - x - 1) = (x^3 - x)f_1 f_2 f_3 \,.$$

Ciało $\mathbb{F}_3[x]/(f_1)$ ma 9 elementów, więc w nim wielomian f rozkłada się na czynniki liniowe. W szczególniości wielomian f_2 ma pierwiastek (nazwijmy go a), więc przekształcenie $\mathbb{F}_3[x] \to \mathbb{F}_3/(f_1)$, $x \mapsto a$ faktoryzuje się przez $\mathbb{F}_3[x] \to \mathbb{F}_3[x]/(f_2) \to \mathbb{F}_3[x]/(f_1)$. Przekształcenia ciał są monomorfizmami, więc licząc ilość elementów wnioskujemy $\mathbb{F}_3[x]/(f_2) \simeq \mathbb{F}_3[x]/(f_1)$.

4.9 Przykład: wielomian $x^{16} - x$ w $\mathbb{F}_2$ faktoryzuje się

$$x^{16} - x = x(1 + x)(1 + x + x^2)(1 + x + x^4)(1 + x^3 + x^4)(1 + x + x^2 + x^3 + x^4)$$

– 2 czynniki liniowe mają pierwiastki w $\mathbb{F}_2$ (dwa pierwiastki),
– czynnik kwadratowy ma pierwiastki w $\mathbb{F}_4 \setminus \mathbb{F}_2$ (4–2=2 pierwiastki),
– 3 czynniki stopnia 4 mają pierwiastki w $\mathbb{F}_8 \setminus \mathbb{F}_4$, jest ich $2^4 - 2^2 = 12 = 3 \cdot 4$
Tak jak poprzednio wykazujemy, że $\mathbb{F}_2[x]/(f_1) \simeq \mathbb{F}_2[x]/(f_2)$ dla f_1 i f_2 różnych czynników stopnia 4.

Lokalizacja

4.10 $S \subset R$ 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.

4.11 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 $\frac{a}{s}$

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

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

4.14 $k(x) := (k[x])$ ciało funkcji wymiernych o współczynnikach w k.

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

4.16 Przekształcenie $\iota : R \to R_S$ ma jądro $Z(S) = \{a \mid \exists s \in S\ sa = 0\}$. (Lokalizację można zrobić w dwóch krokach: najpierw podzielić przez $Z(S)$, a potem użyć prostszej relacjii 4.12.

4.17 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 $f = \bar{f}\iota$.

5 Wielomiany o współczynnikach w pierścieniu DJR, podzielność

5.1 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 $= C(X, \mathbb{R})/\mathfrak{m}_x$

5.2 Pierścienie lokalne i lokalizacja w ideale maksymalnym zbioru domkniętego istnieje fun

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

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

5.5 Tw Bezout $f(a) = 0$ to f dzieli się przez $x - a$.

5.6 Wniosek: Jeśli R jest nieskończonym pierścieniem bez dzielników zera, to przekształcenie $R[x] \to R^R$ (wielomian $f \mapsto$ funkcja wielomianowa

Założenie: od tej pory do kryterium Eisensteina R DJR

5.7 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 $f = a \cdot prymitywny$. (a nazywane jest zawartość f.)

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

5.9 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).

5.10 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 $c \in R$, $h \in R[x]$, załóżmy, że c ma minimalną ilość czynników pierwszych. Przypuśćmy, że $p|c$, wtedy $p|h$ (bo $p \not| f$). †

5.11 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.)

5.12 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 $R[x]$.

5.13 Wniosek: $f = x^n + \cdots + a_0$ ma pierwiastek w $F[x]$, to ma pierwiastek w $R[x]$.

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

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

5.16 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.

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

5.17 Pierścienie noetherowskie z definicji: każdy rosnący ciąg ideałów stabilizuje się. (ACC, nie tylko dla ideałów głównych.)

5.18 Równoważny warunek: każdy ideał jest skończenie generowany.

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

5.20 Twierdzenie Hilberta o bazie: R noetherowski, to $R[x]$ noetherowski.
Dow. Skonstruujemy zbiór elementów, które generują dany I. Wybieramy ciaąg $f_n \in I$ i pokazujemy, że dla pewnego n ideał $I_n = (f_1, f_2, \dots, f_n) = I$. Wielomian f_n dobieramy tak: to wielomian o najmniejszym stopniu należący do $I \setminus I_{n-1}$. Ideał wiodących współczynników $J = (a_1, a_2, \dots) = (a_1, a_2, \dots, a_m)$. Wielomian $f_{m+1} \in I \setminus I_m$ ma wiodący współczynnik $a_{m+1} = \sum_{k \leq m} b_k a_k$. Biorąc kombinację wielomianów $\sum_{k \leq m} b_k f_k x^{\deg f_{m+1} - \deg f_m}$ dostajemy wielomian g z wiodącym współczynnikiem a_{m+1}. Wielomian $f_{m+1} - g$ ma niższy stopień niż f_{m+1} co przeczy wyborowi f_{m+1}.

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

6 Związki z geometrią

6.1 Pierścień ilorazowy noetherowskiego są noetheowskie.

6.2 Pierścienie skończenie generowane nad noetherowskim są noetherowskie.

6.3 k dowolne ciało, $k \subset A$ pierścień zawierający $k = k$-algebra. Jeśli A jest skończenie generowany, to dla każdego ideału maksymalnego $\mathfrak{m}$ iloraz $A/\mathfrak{m}$ jest ciałem zawierającym k i skończenie geberowaną k-algebrą. (Bardzo ważna uwaga bez dowodu: Wtedy $A/\mathfrak{m}$ jest algebraicznym rozszerzeniem k.)

6.4 Tw 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 $(a_1, a_2, \dots, a_n) \in k^n$

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

Oznaczenie: zbiór idałów maksymalnych $SpecMax\, A$.

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

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

gdzie

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

6.6 Uwaga: do definicji zbioru X nie są potrzebne generatory algebry A. Za chwilę zdefiniujemy topologię w X.

6.7 Topologia Zariskiego w k^n: zbiory domknięte = zbiory algebraiczne (tzn opisane skończonymi układami równań wielomianowych). Zbiory otwarte w języku ideałów

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

gdzie I ideał. Baza topologii

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

gdzie $f \in A$.

6.8 Twierdzenie Hilberta o zerach *Nullstellensatz*: Dla $X \subset k^n$ niech

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

(to jest ideał) oraz dla $E \subset k[x_1, x_2, \ldots, x_n]$ niech $V(E)$ zbiór zer:

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

Mamy

$$I(V(E)) = \sqrt{(E)}, \qquad \overline{X} = V(I(X))\,,$$

gdzie $\overline{X}$ oznacza domknięcie w topologi Zariskiego.

6.9 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 $(x^2y, x^2z) = (x^2) \cap (y, z)$
– $V(xy, x^2) = V(x) \cup V(x^2, xy, y^2)$ suma osi i wielokrotnego punktu (ukryta składowa),
bo $(xy, x^2) = (x) \cap (x^2, xy, y^2)$
– $V(xy, x^2) = V(x) \cup V(x^2, xy, y^3)$ inny rozkład poprzedniego ideału.
Tez mamy $(xy, x^2) = (x) \cap (x^2, xy, y^3)$

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

6.11 I prymarny, wtedy $\sqrt{I}$ pierwszy

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

6.12 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).

6.13 Twierdzenie: R noetherowski, każdy Q nierozkładalny ideał jest prymarny. (tbc)

Tu są pliki z książkami: `...aweber/zadania/algebra/pdf/`

7 Rozkład prymarny, ciała

7.1 $V(I) \cup V(J) = V(I \cdot J) = V(I \cap J)$, 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.

7.2 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 $b \in I$

7.3 Twierdzenie: R noetherowski, każdy nierozkładalny ideał Q jest prymarny. Dow: 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 $a^n \in Q$.

7.4 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.

7.5 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.

7.6 Twierdzenie: jeśli $I = \bigcap Q_i$ będzie nieskracalnym rozkładem na ideały prymarne, to zbiór ideałów pierwszych $\sqrt{Q_i}$ jest jednoznacznie wyznaczony: $P = \sqrt{Q_i}$ dla pewnego i wtedy i tylko wtedy, gdy istnieje $b \in R$ taki, że $P = \sqrt{(Q_i : b)}$.

7.7 (bez dowodu) Niech $P_i \subset ass(I)$ będzie minimalnym stowarzyszonym ideałem, wtedy Q_i w rozkładzie minimalnym nie zależy od rozkładu.

Ciała

7.8 Dla każdego wielomianu $f \in K[x]$ istnieje ciało L oraz włożenie $K \hookrightarrow L$, takie, że f ma pierwiastek w L. W być może większym ciele f rozkłada się w L na czynniki liniowe.

7.9 Dane rozszerzenie ciała $K \subset L$. Następujące warunki są równoważne:
1) istnieje $0 \neq f \in K[x]$ taki, że $f(a) = 0$ (element a jest algebraiczny nad K)
2) $\dim_K K[a] < \infty$
3) $K[a] = K(a)$ (tzn podpierścień $K[a]$ jest ciałem).

7.10 Niech a algebraiczny nad K. Następujące liczby są równe:
1) stopień wielomianu minimalnego dla a: (f jest minimalny jeśli $(f) = \{g \in K[x] \mid g(a) = 0\}$)
2) $\dim_K K[a]$

7.11 Ćwiczenie: Niech $a, b \in L \supset K$ będą algebraiczne nad K. Wtedy ich suma i iloczyn są algebraiczne nad K.

7.12 Rozszerzenie algebraiczne $K \subset L$. Def: każdy element $a \in L$ jest algebraiczny.

7.13 Twierdzenie: Rozszerzenie algebraiczne rozszerenia algebraicznego jest algebraiczne.
Dw: $K \subset L \subset M$ wystarczy założyć, że $L = K[a_0, a_1, \ldots a_n]$, $M = L[b]$. Wtedy $\dim_K M = \dim_L M \cdot \dim_K L < \infty$.

8 Algebraiczne domknięcie ciała, moduły

8.1 Niech $K \subset L$. Grupa automorfizmów L stałych na K oznaczana jest $Gal(L, K)$. Permutuje pierwiastki wielomianów $f \in K[x]$.

8.2 Przykłady: - $K = \mathbb{Q}$, $L = Q(\sqrt{2})$, $Gal(L, K) = \mathbb{Z}_2$
- $K = \mathbb{Q}$, $L = Q(\xi)$, $\xi^n = 1$, pierwiastek pierwotny $Gal(L, K) = \mathbb{Z}_n^*$
- $K = k(\sigma_1, \sigma_2, \ldots, \sigma_n)$, $L = k(x_1, x_2, \ldots, x_n)$, gdzie σ_i to elementarna funkcja symetryczna od x_i (ze wzorów Viete'a), $Gal(L, K) = \Sigma_n$.
- $Gal(\mathbb{Q}(i, \sqrt[4]{2})) = D_8$
- $Gal(\mathbb{F}_{p^n}, \mathbb{F}_p) = \mathbb{Z}_n$
- $Gal(\overline{\mathbb{F}}_p, \mathbb{F}_p) = \mathbb{Z}^\wedge$

8.3 $K \subset L \subset M$. Dla podgrupy $H < Gal(M, K)$ zbiór punktów stałych M^H jest ciałem. Dla podciała $L \subset M$ zbiór elementów grupy G_L stałych na L jest podgrupą.
– $L \subset M^{G_L}$
– $H \subset G_{M^H}$
Patrz teoria Galois.

8.4 Konstrukcja ciała algebraicznie domkniętego zawierającego dane: ([B-B, Elementy algebry roz 4]): bierzemy jakikolwiek ciąg ciał $K \subset K_1 \subset K_2 \subset \ldots$, taki, że każdy wielomian z $K_i[x]$ ma pierwiastek w K_{i+1}. Wtedy $\bigcup K_i$ jest algebraicznie domknięte.

8.5 Konstrukcja oszczędniejsza: jeśli $K \subset L$ jest rozszerzenim algebraicznym i każdy wielomian $f \in K[x]$ dodatniego stopnia rozkłada się na czynniki liniowe w $L[x]$, to L jest algebraicznie domknięte. Dow: Niech $f \in L[x]$ będzie wielomianiem dodatniego stopnia. Istnieje większe ciało $M \supset L$, w którym f ma pierwiastek b. Niech $L(b) \subset M$ będzie podciałem M generowanym przez L i b. Wtedy

$K \subset L(b)$ jest rozszerzeniem algebraicznym (bo jest złożeniem rozszerzeń algebraicznych). Zatem istnieje wielomian $g \in K[x]$, taki, że $g(b) = 0$. Ale w każdy wielomian z $K[x]$ rozkłada się w $L[x]$ na czynniki liniowe. Zatem $b \in L$.

8.6 Dane $K \subset \widetilde{K}$, gdzie $\widetilde{K}$ jest algebraicznie domknięte. Wtedy zbiór elementów algebraicznych nad K jest ciałem algebraicznie domkniętym i algebraicznym rozszerzeniem K. To jest domknięcie algebraiczne K. Jest wyznaczone jednoznacznie z dokładnością do izomorfizmu.

8.7 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.

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

8.9 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.)

8.10 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.

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