3. Pierścień funkcji wielomianowych na krzywej algebraicznej

W tym rozdziale przypominy definicje dziedziny calkowitości; dziedziny z jednoznacznością rozkładu, a następnie zdefiniujemy pojęcia ciła ułamków pierścienia oraz pierścienia lokalnego. W drugiej częsci pokażemy przykłady związane z krzywymi algebraicznymi.

R – pierścień przemienny z jedynką

Definicja:

R jest dziedziną całkowitości: wtt. gdy nie istnieją w nim właściwe dzielniki zera. To znaczy , jeśli $a*b=0$ to $a=0$ lub $b=0$.

Wniosek:

Jeśli $a*b=a*c$ to $a=0$ lub $b=c$.

Definicja:

$a|b$ wtt. gdy $\exists_{c\in R} a*c=b$

W dalszym ciągu R^* będziemy oznaczać grupę elementów odwracalnych (grupa jedności) pierścienia R; tzn.

$R^*=\{a\in R: \exists_{b\in R} a*b=1\}$

Wniosek:

$d\in R^*$ wtt. gdy $a|1$

Definicja:

Element a in R nazywamy pierwszym wtt. gdy zachodzi implikacja $a|b*c\Rightarrow a|b\ lub\ a|c$

Definicja:

Element $a\in R\setminus R^*\cup 0$ nazywamy nierozkładalnym wtt. gdy zachodzi implikacja $a=b*c\Rightarrow b\in R^*\ lub\ c\in R^*$.

Definicja:

Pierścień R nazywamy dziedziną z jednoznacznością rozkładu (DJR) wtt. każdy element $a \in R \setminus (R^* \cup \{0\})$ można przedstawić jednoznacznie z dokładnością do porządku i odwracalności w postaci iloczynu elementów nierozkładalnych.

Twierdzenie 1:

Jeśli R – dziedzina całkowitości to każdy element pierwszy jest nierozkładalny. Jeśli co więcej R jest DJR to zachodzi również odwrotna implikacja, tzn. każdy element nierozkładalny jest pierwszy.

Przykład:

Pierścień wielomianów K[X, Y] nad ciałem K jest DJR

Twierdzenie 2:

Niech R – pierścień (przemienny z jedynka), wtedy zachodzi implikacja:

Jeśli a – pierwszy to pierścień ilorazowy R/(a) jest ciałem.
Jeśli a – nierozkładalny to pierścień ilorazowy R/(a) jest D.C.

Niech R – D.C.
Definiujemy relację (równoważności)

$$\forall r, s, r', s' \in R$$
$$(r, s) \sim (r', s') \Leftrightarrow r * s' - s * r' = 0$$

Klasy abstrakcji tej relacji nazywamy ułamkami w R i oznaczamy:

$\frac{r}{s}; \frac{r'}{s'}$ odpowiednio. Zbiór ułamków z działaniami

$$\frac{r}{s} * \frac{r'}{s'} = \frac{r * r'}{s * s'}$$

$$\frac{r}{s} + \frac{r'}{s'} = \frac{r * s' + s * r'}{s * r'}$$

ma strukturę ciała. Nazywamy go ciałem ułamków pierścienia R.

Ideał I pierścienia nazywamy maksymalnym wtt. gdy zachodzi implikacja

$$I \subset J \subset R \Rightarrow J = I \; lub \; J = R$$

Definicja:

Pierścień R nazywamy lokalnym wtt. gdy posiada dokładnie jeden ideał maksymalny.

Twierdzenie 3:

Następujące warunki są równoważne:

1. R jest pierścieniem lokalnym.
2. Zbiór wszystkich elementów nieodwracalnych jest ideałem pierścienia R.

Dowód Tw 3:

"⇐" tzn. że z (2) wynika (1)

Niech S – zbiór wszystkich elementów nieodwracalnych R. Wiemy, że S jest ideałem. Pokażemy, że S jest jedynym ideałem maksymalnym pierścienia R. W tym celu wystarczy zauważyć, że ideał generowany przez S i dowolny element $a \notin S$ jest całym pierścieniem R a to wynika stąd, że taki element a musi być odwracalny w R.

"⇒" tzn. że z (1) wynika (2)

Niech I – ideał maksymalny pierścienia R. Wystarczy pokazać, że suma elementów nieodwracalnych w R jest elementem nieodwracalnym w R. W tym celu rozważmy dwa ideały: $(a) \subset R, (b) \subset R$. Na mocy założenia $(a) \subset I, (b) \subset I$ gdzie I jest jedynym ideałem maksymalnym pierścienia R. Ponieważ I jest grupą addytywna to $a+b \in I$, zatem $a+b$ jest elementem nieodwracalnym w R. CKD

Definicja

K nazywamy ciałem algebraicznie domkniętym wtt. gdy każdy wielomian o współczynnikach w tym ciele posiada w nim także pierwiastki.

Lemat: Jeśli K - ciało algebraiczne domknięte to

$|K| = \infty$

Dowód:

Wystarczy rozważyć wielomiany $x^p - 1$ gdzie p – przebiega liczby pierwsze i zauważyć, że jeśli $x^{p_1} = 1$ oraz $x^{p_2} = 1$ to

$x^{NWD(p_1, p_2)} = x^1 = 1$.

Definicja:

$A^2(K)$ – przestrzeń afiniczna dwuwymiarowa $(A^2(K)=K\times K)$

Niech C – krzywa algebraiczna płaska, tj. zbiór rozwiązań równania $C(X,Y)=0$

gdzie $C\in K[X,Y]$

tzn. $C=\{(x,y)\in A^2(K): C(x,y)=0\}$

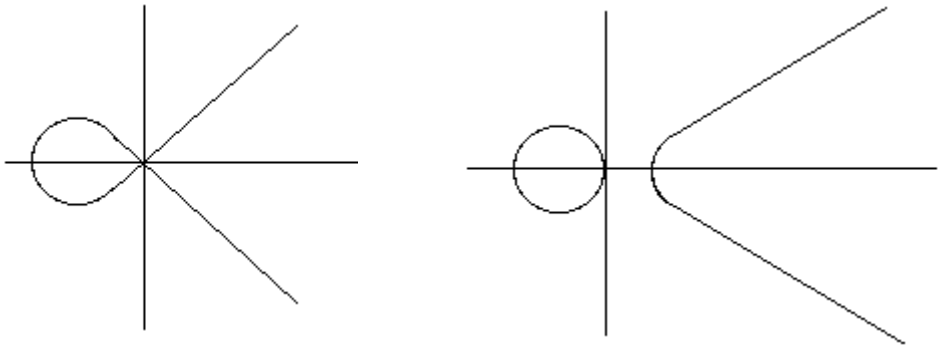
Przykład:

$K=\mathbb{R}$

$D=Y^2-(X^3+X^2)$

$E=Y^2-(X^3-X)$

D E



Wniosek 2:

Jeśli K – ciało algebraicznie domknięte, to krzywa algebraiczna płaska $C\in K[X,Y]$ zawiera nieskończenie wiele punktów.

Dowód:

$\forall_{x\in K}\ C(X,Y)=0$ ma rozwiązanie Y = y na mocy algebraicznej domkniętości K.

$|\{(x,y): C(x,y)=0\}|\geq \sum_{x\in K} 1 = \infty$ na mocy wniosku 1.

Definicja:

$C\subset A^2(K)$, $P=(x,y)$ punkt leżący na krzywej $C, (P\in C)$ powiemy, że P jest punktem osobliwym wtt gdy

$$\frac{\partial C}{\partial x}(P)=\frac{\partial C}{\partial Y}(P)=0$$

Krzywa C jest osobliwa wtt gdy posiada co najmniej jeden punkt osobliwy.

Przykład:

$$\frac{\partial D}{\partial x}(0,0)=-(3x^2+2x)=0$$
$$\frac{\partial D}{\partial y}(0,0)=2y=0$$
$$\frac{\partial E}{\partial x}(0,0)=-(3x^2-1)=1$$
$$\frac{\partial E}{\partial y}(0,0)=2y=0$$

Zatem punkt P = (0, 0) jest punktem osobliwym krzywej D ale nie jest punktem osobliwym krzywej E.

3.1 Funkcje wielomianowe i wymierne na krzywej C

Definicja:

Pierścieniem współrzędnych krzywej C nazywamy pierścień ilorazowy K[C] = K[X, Y] / (C), w dalszym ciągu będziemy zakładać, że C[X, Y] jest wielomianem nierozkładalnym nad ciałem K.

Wniosek:

Na mocy twierdzeń 1 i 2 mamy, że:

K[C] jest dziedziną całkowitości

Uwaga:

Elementy pierścienia współrzędnych K[C] są klasami abstrakcji relacji równoważności określonej następująco:

[f] = f + (C), gdzie (C) oznacza ideał generowany przez wielomian C(X, Y)

Definicja:

Ciałem funkcji wymiernych na krzywej C nazywamy ciało ułamków pierścienia K[C], i oznaczamy je przez K(C).

Wniosek:

Elementy ciała funkcji wymiernych są postaci $r=\frac{f}{g}\ gdzie\ f,g\in K[C]$

3.2 Pierścień lokalny

Niech $P\in C$ – krzywa eliptyczna płaska
K(C) - ciało funkcji wymiernych

Definicja:

$r\in K(C)$ jest regularna w punkcie P jeśli istnieje reprezentacja :
$r=\frac{f}{g}, f, g\in k[C]$ oraz $g(P)\neq 0$

Definicja:

Pierścień funkcji wymiernych regularnych w punkcie P nazywamy pierścieniem lokalnym krzywej C i oznaczamy $O_P(C)$

Krzywe eliptyczne afiniczne

Definicja

Równaniem Weierstrassa nad ciałem *K* nazywamy równanie:
$E: Y^2+a_1XY+a_3Y=X^3+a_2X^2+a_4X+a_6$
$gdzie\ a\in K, i=1,2\ldots 6$

Równanie to nazywamy osobliwym wtt. gdy układ
$\frac{\partial E}{\partial X}=\frac{\partial E}{\partial Y}=0$ nie ma rozwiązań dla żadnego *P = (x, y)* należącego do *E*

Definicja

Krzywą ***E*** zadaną przez powyższe równanie Weierstrassa, która jest nieosobliwą nazywamy krzywą eliptyczną afiniczna

Uwaga

W dalszym ciągu będziemy identyfikować krzywą ***E*** z jej równaniem Weiestrassa a także wielomianem $E(X,Y)\in K[X,Y]$

$E(X,Y)=Y^2+a_1XY+a_3Y-(X^3+a_2X^2+a_4X+a_6)$

Definicja

Stopniem funkcji wymiernej $r=\frac{f}{g}$

$r\in K(X)$, nazywamy liczbę $st(r)=st(f)-st(g)$

Zachodzą równości:

$st(rs)=st(r)+st(s)$

$st(\frac{1}{r})=-st(r)$

$st(r+s)\leqslant min(st(r),st(s))$

Równość zachodzi wtt. gdy $st(r)\neq st(s)$

Twierdzenie 1

Niech R – dziedzina z jednoznacznością rozkładu, L – ciało ułamków pierścienia R i niech $a\in R[Y]$ będzie elementem nierozkładalnym w *R[Y]*. Wtedy $a\in R$ lub a jest nierozkładalny w $L[Y]$.

Dowód

Załóżmy niewprost, że a in R[Y] niestały i że a ma rozkład w L[Y].

Wtedy $a=\frac{f_1}{g_1}*\frac{f_2}{g_2}$ gdzie $f_i,g_i\in R[Y]$

Gdyby istotnie p-element pierwszy dzielił g_1g_2 , wtedy $p|f_1f_2\Rightarrow p|f_1$ lub $p|f_2$ a to niemożliwe bo $f_1f_2\perp g_1g_2$ zatem g_1g_2 jest elementem odwracalnym w $R[Y]$ i wtedy $a=f_1f_2$ gdzie $f_{1,}f_2\in R[Y]$ co przeczy nierozkładalności a w $R[Y]$.

Twierdzenie 2

Wielomian $E(X,Y)$ występujący w równaniu Weierstrassa jest nierozkładalny w $K[X,Y]$.

Dowód

Niech $R=K[X]$ – dziedzina z jednoznacznością rozkładu.

Gdyby E był rozkładalny w $K[X,Y]$ to także nie mamy powyższego twierdzenia w $K(x)[Y]=L[K]$ wtedy $E=(Y+r)(Y+s)$ gdzie $r,s\subset K(x)$

Porównując współczynniki dostajemy:

$r+s=a_1X+a_3$
$rs=-(X^3+a_2X^2+a_4+a_6)$
$st(r+s)\leqslant 1$
$1\geqslant st(r+s)=max(str,sts)\geqslant\frac{3}{2}$ - sprzeczność

Dla dowolnego $f\in K[E] oraz (x,y)=P\in E$ definiujemy wartość $f(P)=f(X,Y)(x,y)=f(x,y)$ która nie zależy od wyboru reprezentacji wielomianu f gdyż biorąc $g=f+cE$ otrzymujemy
$g(P)=f(P)+cE(P)=f(P)+c*0=f(P)$

Uwaga

Ciało K(E) jest rozszerzeniem stopnia dwa ciała K(X). Automorfizm ciała K(E) na K(X) jest zadany przez odwzorowanie:
$\tau: Y\to\bar{Y}=-Y-a_1X-a_3$
Dla dowolnego $f\in K(E)$ definiujemy:
$\bar{f}(X,Y)=f(X,\bar{Y})$
gdzie $\bar{Y}$ jak wyżej

Podobnie jeśli $P=(x,y)\in E$ to $(\bar{P})=(x,\bar{y})$ tez należy do E gdzie $\bar{y}=-y-a_1X-a_3$
Wynika to z podstawienia $y\to\bar{y}$ w równaniu Weiestrassa
$Y+a_1XY+a_3Y=Y(+a_1X+a_3)=(-Y-a_1X-a_3)(-Y)=Y(Y+a_1X+a_3)$

Definiujemy funkcję normy i śladu:
$N: K(E)\to K(X)$
$Tr: K(E)\to K(X)$
$N(f): f\to f\bar{f}$
$Tr(f): f+\bar{f}$
Norma jest pożytecznym narzędziem przy redukcji wielomianów dwu zmiennych do jednej zmiennej. W szczególności pozwala udowodnić, że:

Stwierdzenie

K[E] jest pierścieniem funkcji wielomianowych na E tzn. zachodzi równoważność $\forall P\in E \quad f(P)=0$ wtt. gdy $f=0\, w\, K[E]$

Izomorfizm krzywych eliptycznych

Krzywa E i E' zadane równaniami Weierstrassa

$E: Y^2 a_1 XY + a_3 Y = X^3 a_2 X^2 + a_4 X + a_6$

$E': Y^2 + a'_1 XY + a'_3 Y = X^3 + a'_2 X^2 + a'_4 X + a'_6$

nazywamy izomorficznymi wtt. gdy istnieje zamiana zmiennych

$$\psi: \begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} u^2 & 0 \\ u^2 s & u^3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} r \\ t \end{pmatrix}$$

gdzie $u \neq 0,$ r, s, t dowolne elementy ciała K

Przekształcenie ψ nazywamy dopuszczalną zamianą zmiennych lub izomorfizmem.

Przykład

$\psi: (X, Y) \to (X, \bar{Y}) = (X, -Y - a_1 X - a_3)$

Wniosek

Relacje izomorfizmu są relacją równoważności

Przekształcenie odwrotne do ψ zadane jest wzorem

$$\psi^{-1}: \begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} u^{-2} & 0 \\ -u^{-2} s & u^{-3} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} u^{-2} r \\ u^{-3}(t - rs) \end{pmatrix}$$

Wniosek

Ściślej mówiąc przekształcenie ψ zamienia układ współrzednych (X, Y) w którym zadana jest krzywa E = E(X, Y) na układ (X', Y') w którym krzywa E ma postać E' tj. $\begin{pmatrix} X \\ Y \end{pmatrix} = \psi \begin{pmatrix} X' \\ Y' \end{pmatrix}$

i macierz ψ jest dana powyżej. Zatem $E' = E \circ \psi$ i $E'(P') = E(P)$, gdzie $P' = \phi(P) \in E'$ i ϕ jest równe ψ^{-1}. Naturalnym rozszerzeniem ψ jest:

$\psi: K(E) \to K(E')$

$\psi(f) = f \circ \psi$

Wniosek

Izomorfizm krzywych E i E' jest jedynym w klasie transformacji afinicznych postaci:

$$\begin{pmatrix} X \\ Y \end{pmatrix} \to \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} r \\ t \end{pmatrix}$$

Postacie normalnie krzywych eliptycznych

Niech K - dowolne ciało. Jeśli istnieje p>0 takie że $1 + 1 + \ldots + 1 = 0$ to ciało ma charakterystykę dodatnią.
Najmniejsza taka liczba p jest nazywana charakterystyką ciała i oznaczana przez char(K).
W przeciwnym przypadku ciało K ma charakterystykę zero i piszemy char(K)=0

Przykład

$char(Z_2) = 2 \quad , char(Z_3) = 3$

Niech ψ - dopuszczalna zamiana zmiennych $\psi : (X', Y') \to (X, Y)$.

Wtedy:

$\psi : K(E) \to K(E')$ takie, że
$\psi(f) = f \circ \psi$ (złożenie zadaje izomorfizm odpowiednich ciał)
Wtedy odbicie (ψ do pierścienia lokalnego) $O_P(E)$ indukuje odpowiednie przekształcenie $\tilde{\psi} | O_P(E) : O_P(E) \to O_{P'}(E')$

Uwaga

Operacje sprzężenia „-„ zadaje izomorfizm krzywej E w krzywą E'=E (automorfizm krzywej E), gdyż $\tau : E \to E \quad P \in E \to P' \in E$, a macierz τ wygląda następująco: $\tau : \begin{pmatrix} X \\ Y \end{pmatrix} \to \begin{pmatrix} X \\ -Y - a_1 X - a_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -a_1 & -1 \end{pmatrix} \begin{pmatrix} Y \\ Y \end{pmatrix} + \begin{pmatrix} 0 \\ -a_3 \end{pmatrix}$

Automorfizm τ jest stały na ciele funkcji wymiernych $K(X)$, Ponieważ $\psi^{-1} K(E') \to K(E)$ wiec $\psi \circ \tau \circ \psi^{-1} : K(E') \to K(E')$ jest to automorfizm stałym na $K(X)$. Zatem $\psi \circ \tau \circ \psi^{-1}$ musi być sprzężeniem na ciele $K(E')$ oznaczanym symbolem τ'.

Wniosek 1

Izomorfizm ψ komutuje a automorfizmem sprzężenia tzn. $\tau \circ \psi = \psi \circ \tau'$

Wniosek 2

Dla dowolnej funkcji wymiernej zachodzi równość $r \in K(E)$

$\psi(\bar{r}) = (\psi \circ \tau)(r) = (\tau \circ \psi)(r) = \psi(r) = \overline{\psi(r)}$

Wniosek 3

ψ komutuje z operatorami normy N i śłady Tr tzn. $\psi \circ N = N \circ \psi$,

$\psi \circ Tr = Tr \circ \psi$

Dowód

Dla normy:

$N(\psi(f)) = (f \circ \psi)(\overline{f \circ \psi})$

$\psi \circ N(f) = \psi(Nf) = \psi(f\bar{f}) = f\bar{f} \circ (\psi) = (f \circ \psi)(\bar{f} \circ \psi) = (f \circ \psi)(\overline{f \circ \psi})$

Dla śladu:

$Tr \circ \psi(f) = Tr(\psi f) = Tr(f \circ \psi) = (f \circ \psi) + \overline{(f \circ \psi)}$

$\psi \circ Tr(f) = \psi(Trf) = \psi \circ (f + \bar{f}) = (f + \bar{f}) \circ \psi = f \circ \psi + \bar{f} \circ \psi = (f \circ \psi) + \overline{(f \circ \psi)}$

Ostatnie przekształcenie zachodzi na mocy wniosku 2.

Postacie normalne

Dopuszczalna zamiana zmiennych ψ przeprowadza krzywą E na krzywą E’

$E: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$

$E': Y^2 + a'_1 XY + a'_3 Y = X^3 + a'_2 X^2 + a'_4 X + a_6$

gdzie :

$a_i, a'_i \in K, i = 1,\ldots,6$ są powiązane równościami

$$a'_1 = u^{-1}(a_1 + 2s)$$
$$a'_3 = u^{-3}(a_3 + ra_1 + 2t)$$
$$a'_2 = u^{-2}(a_2 + sa_1 + 3r - s^2)$$
$$a'_4 = u^{-4}(a_4 + 2ra_2 - (rs + t)a_1 - sa_3 + 3r^2 - 2st)$$
$$a'_6 = u^{-6}(a_6 + r^2a_2 + ra_2 - rta_1 - ta_3 + r^3 - t^2)$$
$$b'_2 = u^{-2}(b_1 + 12r)$$
$$b'_4 = u^{-4}(b_4 + rb_2 + 6r^2)$$
$$b'_6 = u^{-6}(b_6 + 2rb_4 + r^2b_2 + 4r^3)$$
$$b'_8 = u^{-8}(b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4)$$
$$c'_4 = u^{-4}c_4$$
$$\Delta' = u^{-12}\Delta$$
$$j' = j$$

Wniosek

Krzywe izomorficzne mają ten sam j - niezmiennik. Ponieważ $u \neq 0$ więc krzywe izomorficzne mają jednocześnie wyróżnik niezerowy lub zerowy. Klasyfikacja postaci normalnej wyróżnia dwa przypadki:

Przypadek 1

Podstawiając $(X,Y) \to \left(X, Y - \frac{1}{2}(a_1X + a_3)\right)$ przeprowadzamy krzywą E na $E': Y^2 = X^3 + a'_2X^2 + a'_4X + a'_6$

Dalej jeśli dodatkowo $char(K) \neq 3$ to podstawiając $(X,Y) \to \left(X - \frac{1}{3}a'_2, Y\right)$ przeprowadzamy krzywą E' na $E'': Y^2 = X^3 + a''_4X + a''_6$

Jeżeli $char(K) = 3$ to

1) Jeżeli $a'_2 = 0 \left(tj.\ j' = \frac{a'^6_2}{\Delta}\right)$ to E ma żądaną postać : $Y^2 = X^3 + a''_4X + a''_6$

2) W przeciwnym przypadku podstawienie $(X,Y) \to \left(X + \frac{a'_4}{a'_2}, Y\right)$ przeprowadza krzywą E' na $E'': Y^2 = X^3 + a''_2X^2 + a''_6$

Przypadek 2 (char(K) = 2)

1) Jeżeli $a_1 = 0 \left(tj.\ j' = \frac{a_1^{12}}{\Delta}, \Delta \neq 0\right)$ to podstawienie $(X,Y) \to (X + a_2, Y)$ przeprowadza E na postać : $E': Y^2 + a'_3Y = X^2 + a'_4X + a'_6$

2) Jeżeli $a_1 \neq 0$ to podstawienie $(X,Y) \to \left(a_1^2 X + \frac{a_3}{a_1}, Y + \frac{a_1^2 a_4 + a_3^2}{a_1^3} \right)$ przeprowadza krzywą E na $E': Y^2 + XY = X^3 + a'_2 X^2 + a'_6$