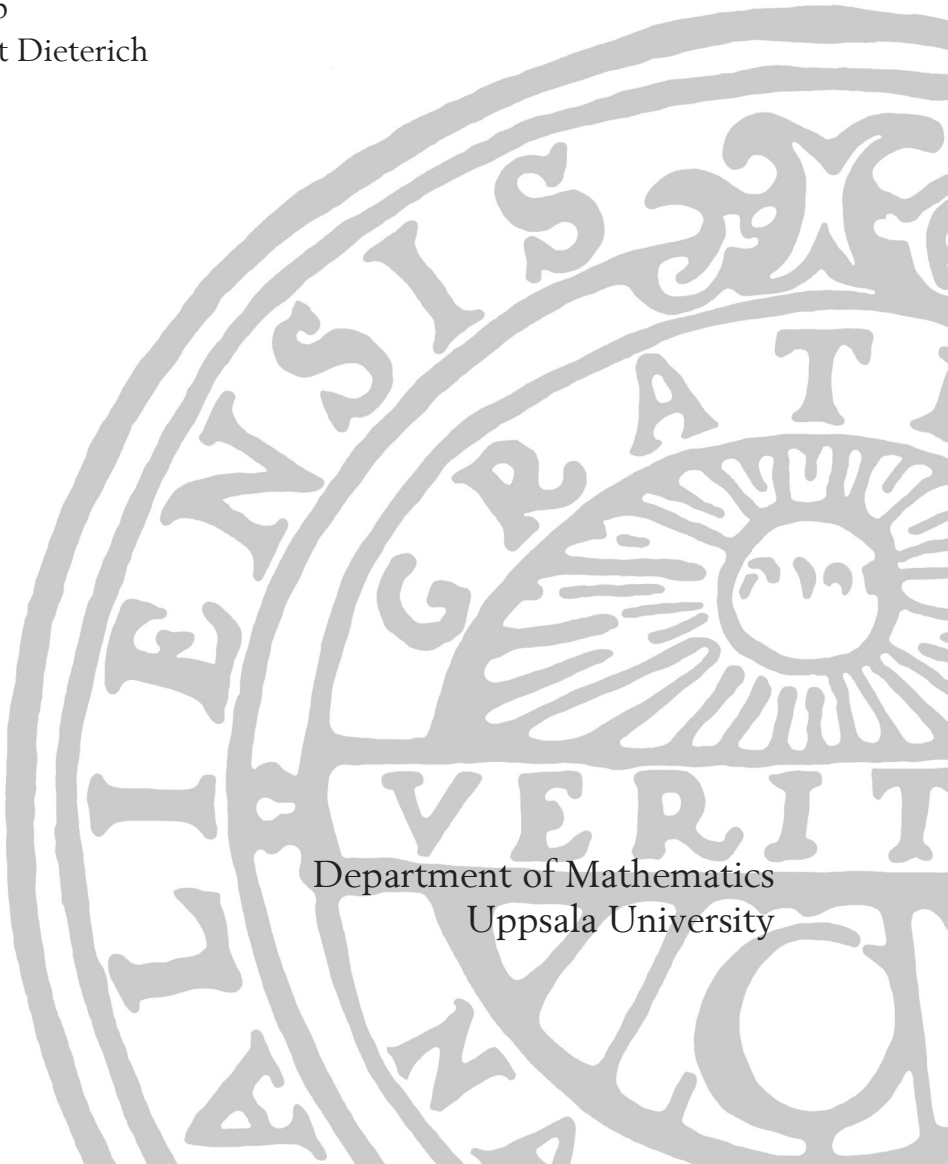
UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2013:15

Ordnade kroppar och Artin-Schreiers teorem

Helena Jonsson

Examensarbete i matematik, 15 hp
Handledare och examinator: Ernst Dieterich
Juni 2013



Department of Mathematics
Uppsala University

Sammanfattning

För varje kropp K kan mängden $\deg(\mathrm{irr}(K[X])) \subset \mathbb{N}$ definieras. För denna mängd finns tre alternativ: den kan vara $\{1\}$, $\{1, 2\}$ eller obegränsad. Denna trikotomi av kroppar följer från Artin-Schreiers teorem från 1926, vilket är en höjdpunkt i teorin om ordnade kroppar. I den här uppsatsen utforskas ordnade kroppar - när kan en kropp ordnas, och vilka kroppsutvidgningar kan i så fall ordnas? Slutligen bevisas Artin-Schreiers teorem och nämnda trikotomi.

Tack
Jag vill tacka min handledare Ernst Dieterich för att ha föreslagit ett fascinerande ämne,
och med stort tålamod ha väglett mig i mitt arbete.

Innehåll

1 Inledning

Att de reella talen utgör en kropp på vilken det finns en total ordning som respekterar både additionen och multiplikationen är ett vedertaget faktum. Det finns dock många kroppar som inte kan ordnas - men också många som kan ordnas. I den här uppsatsen visas vilka kriterier en kropp måste uppfylla för att kunna ordnas, och några klasser av kroppsutvidgningar av ordnade kroppar som kan eller inte kan ordnas bestäms. Merparten av denna teori härör från Artin och Schreier, såsom uppsatsens viktigaste resultat, det teorem från 1926 som bär deras namn.

Läsaren antas vara bekant med grundläggande begrepp från abstrakt algebra. Framför allt används resonemang från galoisteori utan närmare förklaring. Den som vill läsa mer om detta hänvisas till exempelvis [1]. Vissa resultat som utnyttjas men inte bevisas i uppsatsen finns i ett appendix - för bevis och bakomliggande teori, se [1].

2 Ordnade kroppar

Definition. En *partiell ordning* på en mängd M är en delmängd $R \subset M \times M$, där $(x, y) \in R$ skrivs $x \leq y$, så att

(o1) $x \leq x \quad \forall x \in M$.

(o2) $x \leq y \ \wedge \ y \leq x \Rightarrow x = y \quad \forall x, y \in M$.

(o3) $x \leq y \ \wedge \ y \leq z \Rightarrow x \leq z \quad \forall x, y, z \in M$.

Definition. En *total ordning* på en mängd M är en partiell ordning på M så att
$x \leq y$ eller $x \geq y \quad \forall x, y \in M$.

Definition. En *kropp* är en mängd K med två binära operationer,
en addition $K \times K \to K, (x, y) \mapsto x + y$ och en multiplikation $K \times K \to K, (x, y) \mapsto x \cdot y$, så att

(a1) $x + y = y + x \quad \forall x, y \in K$.

(a2) $(x + y) + z = x + (y + z) \quad \forall x, y, z \in K$.

(a3) $\exists 0 \in K : x + 0 = x \quad \forall x \in K$.

(a4) $\forall x \in K \ \exists (-x) \in K : x + (-x) = 0$.

(m1) $xy = yx \quad \forall x, y \in K$.

(m2) $(xy)z = x(yz) \quad \forall x, y, z \in K$.

(m3) $\exists 1 \in K : x \cdot 1 = x \quad \forall x \in K$.

(m4) $\forall x \in K \setminus \{0\} \ \exists x^{-1} \in K \setminus \{0\} : xx^{-1} = 1$.

(d) $x(y + z) = xy + xz \quad \forall x, y, z \in K$.

Definition. En *totalt ordnad kropp* är en kropp K med en total ordning $\leq$ på K så att

(ok1) $x < y \Rightarrow x + z < y + z \quad \forall x, y, z \in K$.

(ok2) Om $z > 0$ så gäller $x < y \Rightarrow xz < yz \quad \forall x, y, z \in K$.

Med *ordnad kropp* åsyftas hädanefter en totalt ordnad kropp.

Vi visar nu några allmänna egenskaper hos ordnade kroppar.

Sats 1. För varje ordnad kropp K och för alla $x, y, z \in K$ gäller

(i) $x > 0 \Leftrightarrow -x < 0$.

(ii) $x > y \Leftrightarrow x - y > 0$.

(iii) $x < y \Leftrightarrow -x > -y$.

(iv) $z < 0 \ \wedge \ x < y \Rightarrow xz > xy$.

(v) $x > y \ \wedge \ y > 0 \Rightarrow xy > 0$.

(vi) $x^2 > 0 \quad \forall x \neq 0$. Särskilt gäller $1 = 1^2 > 0$.

(vii) $x > 0 \Rightarrow x^{-1} > 0$.

(viii) $x > y > 0 \Rightarrow x^{-1} < y^{-1}$.

Bevis. **(i)** (ok1) två gånger ger
$x > 0 \Leftrightarrow x + (-x) > 0 + (-x) \Leftrightarrow 0 > -x$.

(ii) (ok1) två gånger ger
$x > y \Leftrightarrow x + (-y) > y + (-y) \Leftrightarrow x - y > 0$.

(iii) (ok1) ger
$x < y \Leftrightarrow x - x - y < y - x - y \Leftrightarrow -y < -x$

(iv) Enligt (ii) gäller $z < 0 \Leftrightarrow -z > 0$. Enligt (iii) gäller $x < y \Leftrightarrow -x > -y$. (ok2) ger nu $(-x)(-z) > (-y)(-z) \Leftrightarrow xz > yz$.

(v) $x > y \wedge y > 0 \Rightarrow x > 0$ enär ordningsrelationen är transitiv. Enligt (ok2) har vi nu $xy > 0y \Leftrightarrow xy > 0$.

(vi) Antag att $x > 0$. (ok2) ger då $x^2 > 0$. Enligt (iii) gäller nu $(-x) < 0$, men $(-x)^2 = x^2 > 0$, så $x^2 > 0 \quad \forall x \neq 0$.

(vii) Låt $x > 0$ och antag $x^{-1} < 0$. (ok2) ger då $xx^{-1} < x0 \Leftrightarrow 1 < 0$ vilket motsäger (vi). Således är antagandet falskt och $x > 0 \Rightarrow x^{-1} > 0$.

(viii) Låt $x > y > 0$. Enligt (vii) och (ok2) gäller därmed även x^{-1}, y^{-1} och $x^{-1}y^{-1} > 0$. (ok2) igen ger $xx^{-1}y^{-1} > yx^{-1}y^{-1} \Leftrightarrow y^{-1} > x^{-1}$.

□

Anmärkning. Låt K vara en ordnad kropp och låt $P = \{x \in K \mid x > 0\}$. Vi har då en partition $K = P \sqcup \{0\} \sqcup -P$.

Korollarium 2. I en ordnad kropp K med P definierad som ovan har vi
$P < K^* = \langle K \setminus \{0\}, \cdot \rangle$, det vill säga, P är en delgrupp till $K : s$ multiplikativa grupp.

Bevis. Enligt Sats 1 (vi) är 1>0 i varje ordnad kropp, så $1 \in P$. Vidare är P sluten under multiplikation och inversion enligt Sats 1 (v) respektive (vi). □

Definition. För varje ring R finns ringhomomorfismen $f : \mathbb{Z} \to R$ definierad som

$$f(n) = n1 = \begin{cases} \overbrace{1 + ... + 1}^{n} & \text{om } n > 0 \\ 0 & \text{om } n = 0 \\ \underbrace{(-1) + ... + (-1)}_{|n|} & \text{om } n < 0 \end{cases}$$

Kärnan av f, $Ker(f)$, är ett ideal i $\mathbb{Z}$. Eftersom $\mathbb{Z}$ är ett principalidealområde finns ett unikt $c \in \mathbb{N}$ som genererar $Ker(f)$. *Karaktäristiken* av R, $\text{char}(R)$ definieras som detta c.

Anmärkning. En ofta använd, ekvivalent defintion av karakteristik är
$\text{char}(R) = \min\{c \in \mathbb{Z}_{>0} | \underbrace{1 + \ldots + 1}_{c} = 0\}$ om sådant c existerar, och 0 annars.

Korollarium 3. För varje kropp K gäller $\text{char}(K) = 0$ eller $\text{char}(K) = p$ där p är ett primtal.

Bevis. Antag att $\text{char}(K) = c = ab$ och $c \neq 0$. Eftersom $c \in Ker(f)$ har vi $0 = f(c) = f(ab) = f(a)f(b)$. I en kropp finns inga nolldelare, så $f(a) = 0$ eller $f(b) = 0$. Antag $f(a) = 0$. Då har vi $a \in Ker(f)$, så $c|a$. Enligt antagande har vi redan $a|c$, vilket medför $a = c$. Således är faktoriseringen $c = ab$ trivial och c är ett primtal. □

Anmärkning. I varje kropp K med karakteristik p gäller $(a+b)^p = a^p + b^p$ för alla $a, b \in K$.

Anmärkning. Alla ordnade kroppar har karakteristik 0, eftersom $0 < 1 < 1+1 < \ldots$. Det finns alltså inget $c > 0$ så att $\underbrace{1 + \ldots + 1}_{c} = 0 < 1$. Inga ändliga kroppas kan således ordnas.

Anmärkning. $\text{char}(K) = 0$ är ett nödvändigt men inte tillräckligt villkor för att K ska kunna ordnas. De komplexa talen $\mathbb{C}$ bildar en kropp med karakteristik 0 som inte kan ordnas. Enligt Sats 1 (vi) gäller $x^2 > 0 \; \forall x \in K \setminus \{0\}$. I $\mathbb{C}$ finns i med $i^2 = -1$, och $-1 < 0$ i varje ordnad kropp.

Frågan är nu: vad krävs för att en kropp ska kunna ordnas?

Sats 4. För varje kropp K är följande påståenden ekvivalenta

(i) K kan ordnas.

(ii) Ekvationen $x_1^2 + \ldots + x_m^2 = -1$, $m \geq 1$, saknar lösning i K.

(iii) Ekvationen $x_1^2 + \ldots + x_m^2 = 0$, $m \geq 1$, saknar lösning i $K \setminus \{0\}$.

Bevis. "$(ii) \Rightarrow (iii)$" Vi visar den ekvivalenta utsagan $\neg(iii) \Rightarrow \neg(ii)$. Antag $\neg(iii)$, alltså $x_1^2 + \ldots + x_m^2 = 0$ med $m \geq 1$, $x_1, \ldots, x_m \in K \setminus \{0\}$. Detta medför $-x_m^2 = x_1^2 + \ldots + x_{m-1}^2$, alltså $-1 = \frac{x_1^2 + \ldots + x_{m-1}^2}{x_m^2}$, alltså $-1 = (\frac{x_1}{x_m})^2 + \ldots + (\frac{x_{m-1}}{x_m})^2$. Notera att $m - 1 \geq 1$, eftersom $m - 1 = 0$ innebär $-1 = 0$, vilket inte gäller i någon kropp.

"$(iii) \Rightarrow (ii)$" Vi visar $\neg(ii) \Rightarrow \neg(iii)$. Antag $x_1^2 + \ldots + x_m^2 = -1$ med $m \geq 0$, $x_1, \ldots, x_m \in K$. Då har vi $1 + x_1^2 + \ldots + x_m^2 = 0$, vilket innebär $\neg(iii)$.

"$(i) \Rightarrow (iii)$" I varje ordnad kropp gäller enligt Sats 1 (vi) $x^2 > 0 \; \forall x \neq 0$. (ok1) ger då att $x_1^2 + \ldots + x_m^2 > 0$ för alla $x_1, \ldots, x_m \in K \setminus \{0\}$.

"$(iii) \Rightarrow (i)$" Vi börjar med en genomgång av bevisets struktur; detaljerna följer sedan. Definiera $S = \{x_1^2 + \ldots + x_m^2 \mid m \geq 1, x_i \in K \setminus \{0\}\}$. Notera att $S < K^*$ och att S är sluten under addition. Definiera nu $\mathscr{S} = \{R < K^* \mid S \subset R, R \text{ sluten under addition}\}$. $\mathscr{S}$ är icketom och partiellt ordnad med avseende på inklusion. Vidare har varje totalt ordnad delmängd $\mathscr{T} \subset \mathscr{S}$ en övre gräns i $\mathscr{S}$. Enligt Zorns lemma har $\mathscr{S}$ därmed ett maximalt element M. $M, \{0\}$ och $(-M)$ är parvis disjunkta delmängder av K, så $M \sqcup \{0\} \sqcup -M \subset K$. Å andra sidan gäller även $K \subset M \sqcup \{0\} \sqcup (-M)$, så $K = M \sqcup \{0\} \sqcup -M$.

För att visa den andra inklusionen, välj något $a \in K$ så att $a \neq 0$ och $-a \notin M$ och visa att $a \in M$. Låt $M' = \{x + ay \mid x, y \in M \cup \{0\}, x \neq 0 \vee y \neq 0\}$. $M \subset M' \wedge M' \subset M \Rightarrow M' = M \Rightarrow a \in M$. Således finns en partition $K = M \sqcup \{0\} \sqcup (-M)$ och K kan ordnas med $x > y \Leftrightarrow x - y \in M$.

Vi går nu igenom bevisets detaljer. Att S är sluten under addition följer direkt från definitionen. Vi visar nu att $S < K^*$. $0 \notin S$ eftersom vi antog (iii), det vill säga att 0 inte är en summa av nollskilda kvadrater i K. Att $1 = 1^2 \in S$ är klart.

S är sluten under multiplikation: $(\sum_{i=1}^{k} x_i^2)(\sum_{j=1}^{l} y_j^2) = \sum_{i=1}^{k}(\sum_{j=1}^{l}(x_i y_j)^2) = \sum_{\substack{1 \leq i \leq k \\ 1 \leq j \leq l}} (x_i y_j)^2$.

S är sluten under inversion, eftersom $x = x_1^2 + \ldots + x_m^2 \in S$ medför att

$$x^{-1} = \frac{x}{x^2} = \frac{x_1^2 + \ldots + x_m^2}{x^2} = (\frac{x_1}{x})^2 + \ldots + (\frac{x_m}{x})^2 \in S$$

.

Betrakta nu $\mathscr{S}$ som ovan. Vi har $S \in \mathscr{S}$, så $\mathscr{S}$ är icketom. Dessutom är $\mathscr{S}$ partiellt ordnad med avseende på inklusion. Vi visar nu att varje totalt ordnad delmängd $\mathscr{T} \subset \mathscr{S}$ har en övre gräns i $\mathscr{S}$. Låt $\mathscr{T} = \{T_i | i \in I\}$ där I är någon indexmängd. En övre gräns för $\mathscr{T}$ i $\mathscr{S}$ är nu $U = \cup_{i \in I} T_i$. Att $T_i \subset U \ \forall i \in I$ är klart; vad som måste visas är $U \in \mathscr{S}$. Till att börja med har vi $S \subset T_i \ \forall i \in I$, så $S \subset U$. Vidare har vi $0 \notin U$, ty $0 \in U$ innerbär att det finns något $i \in I$ så att $0 \in T_i$, vilket betyder att T_i inte är en multiplikativ delgrupp till K^* och inte ligger i $\mathscr{S}$. Dessutom har vi $1 \in S \subset T_i \ \forall i \in I$, så $1 \in U$.

U är sluten under addition och multiplikation: tag $x, y \in U$. $\exists i \in I : x \in T_i$ och $\exists j \in I : y \in T_j$. Eftersom $\mathscr{T}$ är totalt ordnad har vi $T_i \subset T_j$ eller $T_j \subset T_i$. Antag $T_i \subset T_j$. Vi har nu $x, y \in T_j$. Eftersom $T_j \in \mathscr{T}$ får vi även $x + y, xy \in T_j \Rightarrow x + y, xy \in U$.

U är sluten under inversion eftersom T_i är sluten under inversion $\forall i \in I$.

Sammantaget ser vi att $U < K^*$, $S \subset U$ och U är sluten under addition, så $U \in \mathscr{S}$. Därmed har varje totalt ordnad delmängd av $\mathscr{S}$ en övre gräns och Zorns lemma ger att $\mathscr{S}$ har ett maximalt element M.

Vi visar nu att $K = M \sqcup \{0\} \sqcup -M$. Välj något $a \in K : a \neq 0, a \notin -M$ och betrakta M' som ovan. Att $M \subset M'$ är klart - välj $y = 0$ för alla värden på $x \in M$. Vi visar nu att $M' = M$, så att $a \in M$; därmed gäller att varje element i K ligger i antingen M, $\{0\}$ eller $-M$. Eftersom M är maximalt i $\mathscr{S}$ räcker det att visa $M' \in \mathscr{S}$. Vi har $S \subset M$ vilket medför $S \subset M'$ och $1 \in S$, varför $1 \in M'$.

Vidare gäller $0 \notin M'$, ty $x + ay = 0$ skulle innebära $a = -\frac{x}{y}$ alltså $-a = \frac{x}{y} \in M$ vilket motsäger antagandet om att $-a \notin M$. (Kom ihåg att fallet $x = y = 0$ redan är uteslutet.) M' är sluten under addition eftersom M är det: $(x+ay)+(z+at) = (x+z)+a(y+t)$. M' är även sluten under multiplikation: $(x+ay)(z+at) = xz+axt+ayz+a^2yt = (xz+a^2yt)+a(xt+yz)$. (Kom ihåg att $a^2 \in S \subset M$.)

Dessutom är M' är sluten under inversion. Eftersom $v = x+ay \in M'$ medför $v^2 \in S \subset M$, så $v^{-1} = \frac{v}{v^2} = \frac{x}{v^2} + a\frac{y}{v^2} \in M'$.

Således har vi $M' \in \mathscr{S}$ och $M \subset M'$, vilket medför $M' = M$. Vi har därmed en partition $K = M \sqcup \{0\} \sqcup -M$.

K kan nu ordnas med $x < y :\Leftrightarrow y - x \in M$. Vi visar nu att denna ordningsrelation uppfyller (ok1) och (ok2).

(ok1) $x < y \Leftrightarrow y - x \in M \Leftrightarrow (y + z) - (x + z) \in M \Leftrightarrow x + z < y + z$

(ok2) $z > 0 \Leftrightarrow z \in M$
Eftersom M är sluten under multiplikation har vi
$x < y \Leftrightarrow y - x \in M \Leftrightarrow z(y - x) \in M \Leftrightarrow zy - zx \in M \Leftrightarrow zx < zy$.

□

3 Reellt slutna kroppar

Hittills har vi diskuterat ordnade kroppar, alltså kroppar med en total ordning. Faktum är dock att det kan finnas flera olika totala ordningar som gör en och samma kropp K till en ordnad kropp.

Definition. En kropp K är *formellt reell* om K är ordningsbar, det vill säga, om det finns någon total ordning på K som gör K till en totalt ordnad kropp.

En naturlig fråga att ställa är nu: givet en formellt reell kropp K, vilka kroppsutvidgningar $K \subset L$ är formellt reella?

Ett första svar, som inte visas här, är att om K är en formellt reell kropp så är även $K(X) = \{\frac{p(x)}{q(x)} | p, q \in K[X], q \neq 0\}$ formellt reell. Ytterligare två svar presenteras nu.

Sats 5. Låt K formellt reell kropp och låt $K \subset L$ vara en kroppsutvidgning där $\alpha \in L$. Om $\alpha^2 \in K$ och $\alpha^2 > 0$ i K m.a.p. någon ordningsrelation som gör K till en ordnad kropp så är $K(\alpha)$ formellt reell.

Bevis. Om $\alpha \in K$ har vi $K(\alpha) = K$ och är klara. Antag nu att $\alpha \notin K$. Då har varje element i $K(\alpha)$ en unik representation på formen $x + \alpha y$ med $x, y \in K$. Vi visar nu att -1 inte kan skrivas som en summa av kvadrater i $K(\alpha)$. Antag $-1 = \sum_{i=1}^{n}(x_i + \alpha y_i)^2$. Då är

$$-1 = \sum_{i=1}^{n}(x_i^2 + \alpha^2 y_i^2 + 2\alpha x_i y_i) = \sum_{i=1}^{n}(x_i^2 + \alpha^2 y_i^2) + \alpha \sum_{i=1}^{n} 2x_i y_i$$

. Detta medför $\sum_{i=1}^{n}(x_i^2 + \alpha^2 y_i^2) = -1$, vilket motsäger antagandet om att K är formellt reell. Således är $K(\alpha)$ formellt reell. □

Sats 6. Om K är en formellt reell kropp så är varje ändlig utvidgning av K av udda grad formellt reell.

Bevis. Satsen bevisas med induktion över n, för alla formellt reella kroppar K och alla ändliga utvidgningar $K \subset L$ av udda grad $[L : K] = n$ samtidigt.
Om $n = 1$ har vi $L = K$ och är klara.
Antag nu att $n > 1$ och att alla utvidgningar av K av udda grad m, där $1 \leq m < n$, är formellt reella. Välj något $\alpha \in L \setminus K$.

Fall 1: $K(\alpha) \subsetneq L$. Nu har vi $K \subsetneq K(\alpha) \subsetneq L$, alltså $n = [L : K] = [L : K(\alpha)][K(\alpha) : K]$ där $[L : K(\alpha)] \neq 1$ och $[K(\alpha) : K] \neq 1$. Eftersom $[L : K(\alpha)], [K(\alpha) : K] | n$ måste vi ha $1 < [L : K(\alpha)], [K(\alpha) : K] < n$ och $[L : K(\alpha)], [K(\alpha) : K]$ udda.
Enligt induktionsantagande är $K(\alpha)$ nu formellt reell, vilket medför att även L är formellt reell.

Fall 2: $L = K(\alpha)$. Antag nu att L inte är formellt reell. Låt $q = \mathrm{irr}_K(\alpha)$. Då har vi $\deg(q) = [L : K] = n$. Dessutom har vi för varje $x \in K$ ett unikt $f \in K[X]$ så att $x = f(\alpha)$ och $\deg(f) < n$. Om L inte är formellt reell har vi $-1 = \sum_{i=1}^{k} f_i(\alpha)^2$ där $f_i \in K[X]$ och $\deg(f_i) < n$. Därmed har vi $(1 + \sum_{i=1}^{k} f_i^2)(\alpha) = 0$. Eftersom α är ett nollställe till $(1 + \sum_{i=1}^{k} f_i^2) \in K[X]$ måste q dela $1 + \sum_{i=1}^{k} f_i^2$, så $1 + \sum_{i=1}^{k} f_i^2 = gq$ för något $g \in K[X]$. Den ledande koefficienten i varje f_i^2 är en kvadrat i K och således positiv. Dessutom gäller $\deg(f_i) < n$, vilket medför

$$\deg(1 + \sum_{i=1}^{k} f_i^2) = \max_{1 \leq i \leq k} (\deg(f_i^2)) = 2 \max_{1 \leq i \leq k} (\deg(f_i)) = 2m$$

där $m < n$. Därmed har vi $2m = \deg(gq) = \deg(g) + \deg(q) = \deg(g) + n$, så g har udda grad $\deg(g) < n$. Dessutom har g en irreducibel faktor r med udda grad $\deg(r) < n$. Eftersom $r \in K[X]$ finns något $\beta \in \overline{K}$ så att $r(\beta) = 0$. Detta medför $g(\beta) = 0$, alltså $(1 + \sum_{i=1}^{k} f_i^2)(\beta) = (gq)(\beta) = g(\beta)q(\beta) = 0$, alltså $-1 = \sum_{i=1}^{k} f_i^2(\beta) \in K(\beta)$. Således är $K(\beta)$ inte formellt reell. Men $[K(\beta) : K] = \deg(r) < n$ och udda, så $K(\beta)$ är formellt reell enligt antagande. Denna motsägelse betyder att antagandet L ej formellt reell var falskt, varför även L måste vara formellt reell. □

Vi har nu sagt något om formellt reella utvidgningar av formellt reella kroppar. Faktum är dock att det finns formellt reella kroppar som saknar formellt reella utvidgningar. Sådana kroppar ska nu undersökas.

Definition. En kropp K är *reellt sluten* om K är formellt reell och det inte finns någon formellt reell algebraisk utvidgning $K \subsetneq L$.

Sats 7. En formellt reell kropp K är reellt sluten om och endast om

(i) varje positivt element i K är en kvadrat i K, och

(ii) varje polynom av udda grad i $K[X]$ har en rot i K.

I så fall har vi $\overline{K} = K(\imath)$ där $\imath^2 = -1$.

Bevis. Antag först att K är en reellt sluten kropp; visar nu att (i) och (ii) gäller.

(i) Att varje positivt element i K är en kvadrat i K betyder att varje polynom på formen $X^2 - a \in K[X]$, med $a > 0$, har en rot i K. Det finns något $\alpha \in \overline{K}$ så att $\alpha^2 = a$. Eftersom $a = \alpha^2 > 0$ är $K(\alpha)$ formellt reell enligt Sats 5. Men K är reellt sluten, så $K(\alpha) = K$, vilket medför $\alpha \in K$. Därmed är a är en kvadrat i K.

(ii) Låt $p \in K[X]$ vara ett polynom av udda grad. p har nu en irreducibel faktor r av udda grad och $\exists \alpha \in \overline{K} : \mathrm{irr}_K(\alpha) = r$. Eftersom $[K(\alpha) : K] = \deg(r)$ är udda är $K(\alpha)$ formellt reell enligt Sats 6. Därmed måste vi ha $K(\alpha) = K$, alltså $\alpha \in K$. Eftersom α är en rot till r i K är det en också en rot till p i K.

Låt nu K vara en formellt reell kropp där (i) och (ii) gäller. Vi visar först att det inte finns någon ändlig utvidgning $K \subsetneq L$ av udda grad. $(*)$ Antag att vi har $K \subset L$ och att $[L : K]$ är udda. Välj något $\alpha \in L$. Vi har $[L : K] = [L : K(\alpha)][K(\alpha) : K] = [L : K(\alpha)] \deg(\mathrm{irr}_K \alpha)$, vilket medför att $\deg(\mathrm{irr}_K \alpha)$ är udda. (ii) ger nu att $\mathrm{irr}_K \alpha$ har en rot i K, så $\deg(\mathrm{irr}_K \alpha) = 1$ och $\alpha \in K$. Alltså måste vi ha $L = K$.

Betrakta nu $C = K(\imath)$ där $i^2 = -1$. $[C : K] = \deg(\mathrm{irr}_K i) = \deg(X^2 + 1) = 2$, så $K \subsetneq C$. C är inte formellt reell eftersom -1 är en kvadrat i C. Vi visar nu $\overline{C} = C$, vilket medför $\overline{K} = C$ och K reellt sluten.

Först och främst är varje element i C en kvadrat i C. Elementen i C är på formen $a + bi$ med $a, b \in K$.

Fall 1: $b = 0$.
Låt $a > 0$. (i) ger nu att a är en kvadrat i K och därmed även i C. Vidare är $-a = (i)^2 a$ en kvadrat i C. Om $a = 0$ har vi uppenbarligen $a = 0^2$.

Fall 2: $b \neq 0$.
Ekvationen $a + bi = (x + yi)^2$ ger ekvationssystemet $\begin{cases} a = x^2 - y^2 \\ b = 2xy \end{cases}$, vilket tillsammans med villkoret $b \neq 0$ är ekvivalent med
$\begin{cases} a = x^2 - y^2 \\ y = \frac{b}{2x} \end{cases}$.
Detta medför $a = x^2 - \frac{b^2}{4x^2}$, alltså $x^4 - ax^2 - \frac{b^2}{4} = 0$.
Vi har nu en kvadratisk ekvation i x^2 med koefficienter i K och diskriminant $a^2 + b^2 > 0$. (Minns att $a, b \in K$ och kvadrater är positiva i K.) Således har ekvationen två distinkta lösningar s_1 och s_2 i K. Dessa uppfyller dessutom $s_1 s_2 = -\frac{b^2}{4}$, så exakt en av s_1 och s_2 är positiv. Antag $s_1 > 0$. Då har vi $x^2 = s_1 > 0$ i K, så (i) ger att $x \in K$. Därmed har vi även $\frac{b}{2x} \in K$, varför $a + bi = (x + \frac{b}{2x} i)^2$.

Nu har alla andragradspolynom i $C[X]$ en rot i C, eftersom $X^2 + \beta x + \gamma \in C[X]$ har rötterna $-\frac{\beta}{2} \pm \frac{\sqrt{\beta^2 - 4\gamma}}{2} \in \overline{C}$. Enär $\beta^2 - 4\gamma \in C$ är en kvadrat i C har vi $-\frac{\beta}{2} \pm \frac{\sqrt{\beta^2 - 4\gamma}}{2} \in C$. Därmed finns ingen utvidgning $C \subset E$ av grad 2, eftersom vi då skulle ha $E = C(\alpha)$ med $\deg(\mathrm{irr}_C \alpha) = 2$.

Vi visar nu att det inte finns någon äkta algebraisk utvidgning $C \subset E$. Välj något $\alpha \in \overline{C} = \overline{K}$ och betrakta $\mathrm{irr}_K \alpha$. Låt $\alpha = \alpha_1, \ldots, \alpha_n \in \overline{C}$ vara rötterna till $\mathrm{irr}_K \alpha$. Nu är $E = K(i, \alpha_1, \ldots, \alpha_n)$ splittkroppen till $\mathrm{irr}_K \alpha$ och $X^2 + 1$. Enligt Sats A19 är $K \subset E$ dessutom separabel, så E är en ändlig galoisutvidgning av K. Eftersom E är galois över K är E även galois över C enligt Sats A22. Låt $G = Gal(E : K)$. Vi har nu

$$|G| = [E : K] = [E : C][C : K] = 2[E : C].$$

Eftersom 2 delar $|G|$ säger Sylows första sats att G har en maximal Sylow-2-delgrupp S. Låt F vara dess fixkropp över K. Eftersom S är en maximal 2-delgrupp av G måste indexet $[G : S]$ vara udda. Vi har $[F : K] = [G : S]$, och $(*)$ ger nu att $F = K$. Detta medför $G = S$, så $|G| = 2^k$ för något $k \geq 1$. Sambandet $2^k = |G| = 2[E : C]$ medför $[E : C] = 2^m$ där $m = k - 1 \geq 0$.

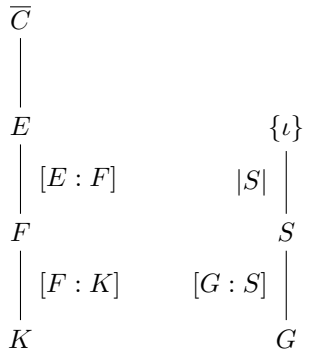


Diagram över galoiskorrespondensen. Till vänster kroppsutvidgningarna, till höger motsvarande galoisgrupper.

Låt $G' = Gal(E:C)$. Vi har då $|G'| = 2^m$. Om $C \subsetneq E$, så att $|G'| > 1$, måste vi ha $m \geq 1$. Då har G' en delgrupp H med index 2. Låt $F' = Fix_E(H)$ så att $Gal(E:F') = H$. Nu har vi $[F':C] = [G':H] = 2$, vilket vi sett är omöjligt eftersom C inte har någon utvidgning av grad 2.

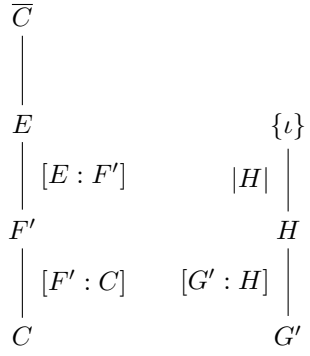


Diagram över galoiskorrespondensen. Till vänster kroppsutvidgningarna, till höger motsvarande galoisgrupper.

Således måste vi ha $E = C$, varför $\overline{C} = C$ så att $\overline{K} = C$ och K är reellt sluten.

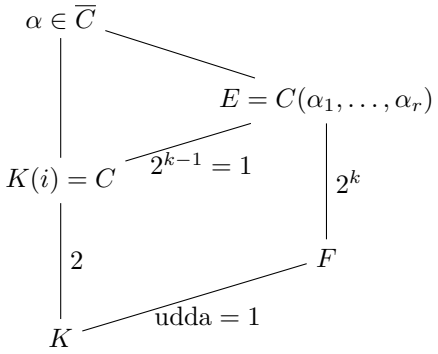


Diagram över kroppsutvidningarna med graderna utmarkerade. □

Som tidigare påpekats är det möjligt att en formellt reell kropp kan ordnas på flera olika sätt. Så är dock inte fallet om kroppen dessutom är reellt sluten.

Korollarium 8. En reellt sluten kropp K kan ordnas på exakt ett sätt.

Bevis. Varje ordningsrelation på K uppfyller $x > y \Leftrightarrow x - y > 0$. Om K är reellt sluten är detta ekvivalent med $x - y \in \{a^2 | a \in K \setminus \{0\}\}$. □

Korollarium 9. Låt K vara en reellt sluten kropp. Då är $p \in K[X]$ är irreducibelt om och endast om $\deg(p) = 1$ eller $\deg(p) = 2$ och p saknar rot i K.

Bevis. " $\Leftarrow$ " gäller för varje kropp K.
" $\Rightarrow$ "
Låt $p \in K[X]$ vara irreducibelt. Det finns något $\alpha \in \overline{K} = K(i)$ så att $\text{irr}_K \alpha = p$. Eftersom $2 = [\overline{K} : K] = [\overline{K} : K(\alpha)][K(\alpha) : K] = [\overline{K} : K(\alpha)] \cdot \deg(p)$ måste $\deg(p)|2$, så $\deg(p) = 1$ eller $\deg(p) = 2$. Om $\deg(p) = 2$ måste p sakna rot i K eftersom p är irreducibelt över K. □

Korollarium 10. Kroppen av alla reella algebraiska tal, A, är reellt sluten.

Bevis. Vi visar att A uppfyller (i) och (ii) i Sats 7, som då säger att A är reellt sluten. $A = \mathbb{A} \cap \mathbb{R}$. Att $\mathbb{R}$ uppfyller (i) och (ii) följer ur Sats 7, eftersom $\mathbb{R}$ är reellt sluten.
(i)
Välj något $\alpha \in \mathbb{R}$ som är en rot till $f(X) = X^2 - a \in A[X] \subset \mathbb{R}[\mathbb{X}]$ där $a > 0$. Låt $E = \mathbb{Q}(a)$. Då har vi $f \in E[X]$. Eftersom $\mathbb{Q} \subset E$ och $E \subset E(\alpha)$ är ändliga utvidgningar är även $\mathbb{Q} \subset E(\alpha)$ ändlig och således algebraisk. Därmed är α algebraiskt över $\mathbb{Q}$ och $\alpha \in \mathbb{A}$. Vi har redan $\alpha \in \mathbb{R}$, så $\alpha \in A$. Således är $f(X) = X^2 - a \in A[X]$ reducibelt och a är en kvadrat i A.
(ii)
Beviset för att A uppfyller (ii) följer samma procedur som beviset för (i). Välj $\alpha \in \mathbb{R}$ som är en rot till $f(X) = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} + X^n \in A[X]$, där n är udda, och låt $E = \mathbb{Q}(a_0, a_1, \ldots, a_{n-1})$. Nu har vi $f \in E[X]$. Eftersom $a_0, a_1, \ldots, a_{n-1} \in A$ är varje a_i algebraiskt över $\mathbb{Q}$. Enligt Sats A18 är $\mathbb{Q} \subset E$ därför ändlig. Därmed är även $\mathbb{Q} \subset E(\alpha)$ ändlig och således algebraisk, varför α är algebraiskt över $\mathbb{Q}$. Detta medför $\alpha \in A$, så f har en rot α i A. □

Vi har nu sett hur vi kan finna formellt reella utvidgningar av formellt reella kroppar, men också att vissa kroppar saknar äkta utvidgningar som är formellt reella. Vi minns att varje kropp har en maximal algebraisk utvigdning - en algebraiska tillslutning. En liknande egenskap som avser formellt reella kroppsutvidgningar beskrivs nu.

Definition. En *reell tillslutning* av en ordnad kropp K är en reellt sluten kropp som är algebraisk över K och vars ordnigsrelation inducerar ordningsrelationen på K.

Sats 11. Varje ordnad kropp har en reell tillslutning.

Bevis. Låt K vara en ordnad kropp och låt $L \subset \overline{K}$ vara kroppen som genereras av alla kvadratrötter av positiva element i K. Vi visar först att L är formellt reell. Om $-1 = \sum_{i=1}^{k} \beta_i^2$ i L så är $-1 = \sum_{i=1}^{k} \beta_i^2$ i $K(\alpha_1, \ldots, \alpha_n) \subset L$ där $\alpha_1^2, \ldots, \alpha_n^2 \in K, \alpha_1^2, \ldots, \alpha_n^2 > 0$ i K. Således är $K(\alpha_1, \ldots, \alpha_n)$ ej formellt reell. Sats 5 och induktion säger dock att $K(\alpha_1, \ldots, \alpha_n)$ är formellt reell. Denna motsägelse ger att -1 inte är en summa av kvadrater i L, så är L formellt reell.

Betrakta nu $\mathscr{S} = \{S \subset \overline{K} \mid L \subset S \text{ och } S \text{ formellt reell}\}$. Vi ser att $\mathscr{S}$ är icketom eftersom $L \in \mathscr{S}$. Dessutom är $\mathscr{S}$ partiellt ordnad med avseende på inklusion. Vi visar nu att varje totalt ordnad delmängd $\mathscr{T} \subset \mathscr{S}$ har en övre gräns i $\mathscr{S}$. Låt $\mathscr{T} \subset \mathscr{S}$ vara totalt ordnad och antag att $\mathscr{T} = \{T_i \mid i \in I\}$ där I är någon indexmängd. $T_i \in \mathscr{S} \forall\ i \in I$. En övre gräns för $\mathscr{T}$ i $\mathscr{S}$ är nu $U = \cup_{i \in I}$. Att $T_i \subset U\ \forall i \in I$ är klart. Att $U \subset \overline{K}$ följer direkt ur att $\mathscr{T}$ är totalt ordnad (se beviset av Sats 4 för detaljer). Vad som återstår att visa är att U är formellt reell. Antag att $-1 = \sum_{i=1}^{k} x_i^2$ i U. Eftersom $\mathscr{T}$ är totalt ordnad finns det ett $j \in I\ :\ x_1, \ldots, x_k \in T_j$. Då är $-1 = \sum_{i=1}^{k} x_i^2$ i T_j och T_j är inte formellt reell, vilket motsäger $T_j \in \mathscr{S}$. Således är -1 inte en summa av kvadrater i U, varför U är formellt reell.

Zorns lemma säger nu att $\mathscr{S}$ har ett maximalt element M. Eftersom M är maximal i $\mathscr{S}$ är M reellt sluten - en äkta algebraisk utvidgning av M kan inte vara formellt reell. Vidare har vi $K \subset L \subset M \subset \overline{K}$, så M är algebraisk över K. Vi visar nu att ordningsrelationen på M inducerar ordningsrelationen på K, alltså att för alla $x \in K \setminus \{0\}$ gäller

$$x > 0 \text{ i } K \Leftrightarrow x > 0 \text{ i } M.$$

Detta är ekvivalent med

$$(x > 0 \text{ i } K \Rightarrow\ x > 0 \text{ i } M) \wedge (x < 0 \text{ i } K \Rightarrow\ x < 0 \text{ i } M).$$

Om $x > 0$ i K är x en kvadrat i $L \subset M$ och därmed positiv i M. Om $x < 0$ i K är $-x$ positiv i K och därmed i M, varför x måste vara negativ i M.

Sammanfattningsvis ser vi att M är en reell tillslutning till K. □

Anmärkning. Alla reella tillslutningar av en ordnad kropp är isomorfa som ordnade kroppar.

4 Artin-Schreiers teorem

Sats 12. (Artin-Schreiers teorem)
För varje kropp $K \neq \overline{K}$ är följande påståenden ekvivalenta.

(i) K är reellt sluten.

(ii) $[\overline{K} : K] < \infty$.

(iii) deg(irr($K[X]$)) är begränsad.

(iv) $[\overline{K} : K] = 2$.

(v) deg(irr($K[X]$)) $= \{1, 2\}$.

Artin-Schreiers teorem ger oss en trikotomi av kroppar.

Korollarium 13. För varje kropp K gäller exakt ett av följande alternativ.

(i) K är algebraiskt sluten. I så fall gäller $[\overline{K} : K] = 1$ och deg(irr($K[X]$)) $= \{1\}$.

(ii) K är reellt sluten. I så fall gäller $[\overline{K} : K] = 2$ och deg(irr($K[X]$)) $= \{1, 2\}$.

(iii) K är ickesluten. I så fall gäller $[\overline{K} : K] = \infty$ och deg(irr($K[X]$)) är obegränsad.

Bevis. (Korollarium)
Vi visar först trikotomin.

Om K är reellt sluten är K formellt reell. Då saknar ekvationen $x^2+1=0$ saknar lösning i K, så $X^2+1 \in irr(K[X])$ och K är inte algebraiskt sluten.
K ickesluten $:\Leftrightarrow K$ varken algebraiskt sluten eller reellt sluten.

Vi visar nu "I så fall..."
(i) följer från definitionen av algebraisk slutenhet.
(ii) följer från Artin-Schreiers teorem.
(iii) följer från Artin-Schreiers teorem. □

För beviset av Artin-Schreiers teorem krävs tre lemman.

Lemma 14. Om deg(irr($K[X]$)) är begränsad så är K perfekt.

Bevis. Vi visar den ekvivalenta utsagan om K inte är perfekt så är deg(irr($K[X]$)) obegränsad. Antag att K inte är perfekt. I så fall har K primtalskarakteristik p och det finns något $c \in K$ som inte är en $p:te$ potens i K. Vi visar nu att $f(X) = X^{p^r} - c \in K[X]$ är irreducibelt $\forall r \geq 0$. Faktorisera $f = q_1 \cdot \ldots \cdot q_k$ med $q_i \in K[X]$ moniska och irreducibla. Låt $\alpha \in \overline{K}$ vara en rot till f. Då är $\alpha^{p^r} = c$ och $f = X^{p^r} - \alpha^{p^r} = (X-\alpha)^{p^r}$. (Minns char$(K) = p$.) Därmed har vi $q_i = (X-\alpha)^{t_i}, t_i > 0$. Låt $t = \min(t_1, \ldots, t_k)$. Då är $q := (X-\alpha)^t$ irreducibelt över $K[X]$ och q delar $q_1, \ldots, q_k$ över $\overline{K}[X]$. Därmed måste q dela $q_1, \ldots, q_k$ även över $K[X]$. Vi kan först och främst finna unika polynom $g_i, r_i \in K[X]$ så att $q_i = qg_i + r_i$ och $\deg(r_i) < \deg(q)$. Denna faktorisering gäller dock även i $\overline{K}[X]$, och då måste $r_i = 0$. Därför måste vi ha $q_1 = \ldots = q_k = q$, vilket medför $f = q^k = (X-\alpha)^{kt} = (X-\alpha)^{p^r}$.

Å ena sidan har vi nu $kt = p^r \Rightarrow p|k \ \vee \ k = 1$. Å andra sidan ser vi att $c = \alpha^{kt} = (\alpha^t)^k$. Eftersom $(-\alpha)^t$ är konstanttermen i q och ligger det i K. Enär c saknar $p:te$ rot i K kan p inte dela k, varför vi har $k = 1$. Alltså är $f = q$, så f är irreducibelt. □

Lemma 15. Om K är en kropp i vilken -1 är en kvadrat och $K \subset L$ är en galoisutvidgning av primtalsgrad p så är $L \neq \overline{L}$

Bevis. Eftersom $|Gal(L:K)| = [L:K] = p$ prim är $Gal(L:K)$ cyklisk, så $K \subset L$ ären cyklisk utvidgning.

Fall 1: char$(K) = p$.
Enligt Sats A24 har vi $L = K(\alpha)$ där $c = \alpha^p - \alpha \in K$. Därmed gäller $\text{irr}_K(\alpha) = X^p - X - c$ och $1, \alpha, \ldots, \alpha^{p-1}$ är en bas för L över K. Låt $\beta = b_0 + b_1\alpha + \ldots + b_{p-1}\alpha^{p-1} \in L$ där $\beta_1, \ldots, \beta_{p-1} \in K$. Eftersom K har karakteristik p och $\alpha^p = \alpha + c$ har vi

$$\beta^p = b_0^p + b_1^p\alpha^p + \ldots + b_{p-1}^p\alpha^{p(p-1)} = b_0^p + b_1^p(\alpha+c) + \ldots + b_{p-1}^p(\alpha+c)^{p-1}.$$

Därmed kan vi skriva

$$\beta^p - \beta - c\alpha^{p-1} = a_0 + a_1\alpha + \ldots + a_{p-1}\alpha^{p-1}$$

där

$$a_{p-1} = b_{p-1}^p - b_{p-1} - c.$$

Således har vi $\beta^p - \beta - c\alpha^{p-1} \neq 0$, eftersom $\beta^p - \beta - c\alpha^{p-1} = 0$ skulle innebära $a_{p-1} = 0$, alltså $b_{p-1}^p - b_{p-1} - c = 0$. I så fall är b_{p-1} en rot till $X^p - X - c$ i K, vilket är omöjligt då $X^p - X - c$ antogs vara irreducibelt över K. Därmed saknar $X^p - X - c\alpha^{p-1}$ rot i L, så L är inte algebraiskt sluten.

Fall 2: $\text{char}(K) \neq p$.
Vi kan anta att L innehåller en primitiv $p:te$ enhetsrot ϵ - annars är L inte algebraiskt sluten och vi är klara. ϵ är en rot till $\Phi_p = X^{p-1} + \ldots + X + 1 \in K[X]$, så $[K(\epsilon) : K] < p$. Eftersom $K(\epsilon)$ är en mellankropp till $K \subset L$ måste $[K(\epsilon) : K]$ dela p, så $[K(\epsilon) : K] = 1$ och $\epsilon \in K$. Enligt Sats A23 har vi nu $L = K(\alpha)$ där $\alpha^p \in K$. Vi visar nu att α ej har en $p:te$ rot i L, så att $X^p - \alpha \in L[X]$ är irreducibelt och L inte är algebraiskt sluten. Antag att $\alpha = \beta^p$ där $\beta \in L$. Låt $\sigma \in Gal(L:K)$, $\zeta = \frac{\sigma(\beta)}{\beta}$ och $\eta = \frac{\sigma(\zeta)}{\zeta}$. Eftersom $\beta^{p^2} = \alpha^p \in K$ har vi $(\sigma(\beta))^{p^2} = \sigma(\beta^{p^2}) = \beta^{p^2}$ och $(\zeta^p)^p = ((\frac{\sigma(\beta)}{\beta})^p)^p = \frac{(\sigma(\beta))^{p^2}}{\beta^{p^2}} = 1$. Alltså är ζ^p en $p:te$ enhetsrot, så $\zeta^p \in K$ och $(\sigma(\zeta))^p = \zeta^p$. Därmed är $\eta^p = 1$, varför $\eta \in K$. Vidare har vi $\zeta\beta = \sigma(\beta)$ och $\eta\zeta = \sigma(\zeta)$.

Vi visar nu att $\sigma^k\beta = \eta^{k(k-1)/2}\zeta^k\beta \quad \forall k \geq 1$.
Om $k = 1$ är likheten redan visad. Antag att likheten gäller för något $k \geq 1$ (IA); visar nu att den gäller för $k+1$.

$$\begin{aligned}
\text{HL}_{k+1} &= \eta^{k(k+1)/2}\zeta^k\beta \\
\text{VL}_{k+1} &= \sigma^{k+1}(\beta) \\
&= \sigma(\sigma^k(\beta)) \\
&= \sigma(\eta^{k(k-1)/2}\zeta^k(\beta)) \\
&= \sigma(\eta^{k(k-1)/2}\sigma(\zeta^k)\sigma(\beta) \\
&= \eta^{k(k-1)/2}(\eta\zeta)^k\zeta\beta \\
&= \eta^{k(k+1)/2}\zeta^{k+1}\beta = \text{HL}_{k+1}
\end{aligned}$$

Enligt induktionsaxiomet gäller likheten nu för alla k. Särskilt gäller den för p. Minns nu att $\sigma \in Gal(L:K)$ med $|Gal(L:K)| = p$, så σ^p är identiteten. Det innebär att

$$\eta^{p(p-1)/2}\zeta^p\beta = \sigma^p(\beta) = \beta, \text{ alltså } \eta^{p(p-1)/2}\zeta^p = 1.$$

Vi visar nu att $\zeta^p = 1$, vilkdet medför $\alpha \in K$ och motsäger antagandet $K \subsetneq L$.

Om p är udda har vi $p|\frac{p(p-1)}{2}$. Eftersom $\eta^p = 1$ måste nu även $\eta^{p(p-1)/2} = 1$, vilket medför $\zeta^p = 1$.

Om $p = 2$ har vi $1 = (\zeta^p)^p = \zeta^4$, alltså $\zeta^2 = \pm 1$. Om $\zeta^2 = 1$ är vi klara. Om $\zeta^2 = -1$ har vi $\zeta \in K$ eftersom -1 antogs vara en kvadrat i K. Då måste $\eta^{p(p-1)/2} = \eta = \frac{\sigma(\zeta)}{\zeta} = 1$. Därmed har vi även $\zeta^2 = 1$, varför -1=1 i K och $\text{char}(K) = 2 = p$, vilket motsäger antagandet $(K) \neq p$.

Vi ser att fallet $\zeta^2 = -1$ inte kan inträffa men att detta är irrelevant då vi i alla möjliga fall får $\zeta^p = 1$. Därmed har vi $\sigma(\alpha) = \sigma(\beta)^p = (\sigma(\beta))^p = (\zeta\beta)^p = \zeta^p\beta^p = \beta^p = \alpha$, så $\sigma\alpha = \alpha$. Alltså måste $\alpha \in K$ och $L = K$, vilket motsäger $[L:K] = p$. Därmed saknar α p:te rot i K och $X^p - \alpha \in L[X]$ saknar rot i L, så L är inte algebraiskt sluten. □

Lemma 16. Om $[\overline{K} : K] = n < \infty$ så har varje irreducibelt polynom i $K[X]$ grad högst n, K är perfekt och $\overline{K} = K(i)$ där $i^2 = -1$.

Bevis. Varje irreducibelt polynom $q \in K[X]$ har en rot $\alpha \in \overline{K}$, så $q = \text{irr}_K(\alpha)$ och $\deg(q) = [K(\alpha) : K] \leq [\overline{K} : K] = n$.

Att K är perfekt följer nu direkt ur Lemma 14.

Vi visar nu att $\overline{K} = K(i)$, där $i \in \overline{K}$ är en rot till $X^2 + 1 \in K[X]$. Vi har $[\overline{K} : K] = n$ och K är perfekt, så enligt Sats A21 är $\overline{K}$ är galois över K. Om $K(i) \subsetneq \overline{K}$ så är $\overline{K}$ galois över $K(i)$. Dessutom har vi $1 < |Gal(\overline{K} : K(i))| < n$, så enligt Sylows första sats har $Gal(\overline{K} : K(i))$ en delgrupp H av primtalsordning. Låt F vara $H : s$ fixkropp i $\overline{K}$. Eftersom $i \in F$ är -1 en kvadrat i F. Samtidigt är $\overline{K}$ galois över F och $[\overline{K} : F] = |H|$ är ett primtal, vilket motsäger Lemma 15. Därmed har vi $K(i) = \overline{K}$.

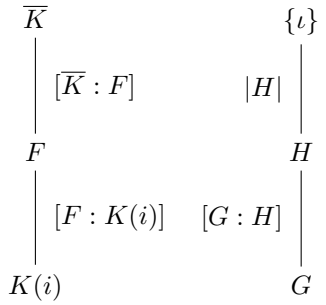


Diagram över galoiskorrespondensen. Till vänster kroppsutvidgningarna, till höger motsvarande galoisgrupper. □

Bevis. (Artin-Schreiers teorem)
Det räcker att visa (i)⇔(ii)⇔(iii), för
(iv)⇒(ii) och (v)⇒(iii) är triviala och
(i)⇒(iv) och (i)⇒(v) följer från Sats 7.

"$(i) \Rightarrow (ii)$"
Följer direkt från Sats 7.

"$(ii) \Rightarrow (iii)$"
Följer direkt från Lemma 16.

"$(iii) \Rightarrow (ii)$"
Om alla irreducibla polynom i $K[X]$ har grad högst n så är K perfekt enligt Lemma 14. Således är $K \subset \overline{K}$ separabel enligt Sats A21. Nu säger Sats A20 att $[\overline{K} : K] \leq n$.

"$(ii) \Rightarrow (i)$"
Om $[\overline{K} : K] < \infty$ ger Lemma 16 att det finns en övre gräns för graden hos de irreducibla polynomen i $K[X]$, K är perfekt och $\overline{K} = K(i)$ där $i^2 = -1$. Eftersom $K \neq \overline{K}$ enligt antagande har vi $i \notin K$. Elementen i $\overline{K}$ är på formen $x + iy$ med $x, y \in K$. För varje $z = x + iy \in \overline{K}$ sätter vi $\bar{z} = x - iy$. Då gäller $z\bar{z} = x^2 + y^2 \in K$ och $\bar{z^2} = \bar{z}^2$. Eftersom $\overline{K}$ är algebraiskt sluten är varje $x \in \overline{K}$ en kvadrat, det vill säga $\forall z \in K\ \exists u \in K : z = u^2$. Detta medför att $x^2 + y^2 = z\bar{z} = u^2\bar{u^2} = u^2\bar{u}^2 = (u\bar{u})^2$. Eftersom $u\bar{u} \in K$ ger induktion att varje summa av kvadrater i K är en kvadrat i K. Enär $i \notin K$ är -1 inte en summa av kvadrater i K, så K är formellt reell. Den enda äkta algebraiska utvidngningen av K är $\overline{K} = K(i)$ som inte är formellt reell. Således är K reellt sluten. □

5 Appendix

Här presenteras satser som utnyttjas ovan men som inte bevisas här.

Sats A17. (Zorns lemma)
Låt P vara en icketom partiellt ordnad mängd.
Om varje totalt ordnad delmängd $T \subset P$ har en övre gräns i P, så har P ett maximalt element.

Bevis. Zorns lemma är ekvivalent med urvalsaxiomet. [1] □

Sats A18. Om $E = K(\alpha_1, \ldots, \alpha_n)$ och varje α_i är algebraisk över K så är $K \subset E$ ändlig och därmed algebraisk.

Bevis. [1, (IV.3.2)] □

Sats A19. Om K har karakteristik 0 så är varje algebraisk utvidgning av K separabel.

Bevis. [1, (IV.5.5)] □

Sats A20. Om $K \subset L$ är separabel och $\deg(\mathrm{irr}_K(\alpha)) \leq n$ för alla $\alpha \in K$, så är $K \subset L$ ändlig och $[L : K] \leq n$.

Bevis. [1, (IV.5.13)] □

Sats A21. Varje algebraisk utvidgning av en perfekt kropp är separabel.

Bevis. [1, (V.2.13)] □

Sats A22. Om F är galois över K och $K \subset E \subset F$ så är F galois över E.

Bevis. [1, (V.3.1)] □

Sats A23. Låt $n > 0$.
Låt K vara en kropp så att $\mathrm{char}(K) = 0$ eller $\mathrm{char}(K) \nmid n$, och K innehåller en $n : te$ enhetsrot.
Om $K \subset L$ är en cyklisk utvidgning av grad n så är $L = K(\alpha)$ där $\alpha^n \in K$.
Om $L = K(\alpha)$ där $\alpha^n \in K$ så är $K \subset L$ cyklisk, $m = [L : K] | n$ och $\alpha^m \in K$.

Bevis. [1, (V.7.8)] □

Sats A24. Låt K vara en kropp med karakteristik $p \neq 0$.
Om $K \subset L$ är en cyklisk utvidgning av grad p så är $L = K(\alpha)$ där $\alpha^p - \alpha \in K$.
Om $L = K(\alpha)$ där $\alpha^p - \alpha \in K$ så är $K \subset L$ en cyklisk utvidgning av grad p.

Bevis. [1, (V.7.10)] □

Sats A25. (Sylows första sats)
Låt G vara en ändlig grupp och låt p vara ett primtal. Om p^k delar $|G|$ så har G en delgrupp av ordning p^k.

Bevis. [1, (II.5.1)] □

Referenser

[1] Grillet, P A. *Abstract Algebra. Graduate Texts in Mathematics 242*. Second edition. Springer, 2007.

[2] Artin, E. och O. Schreier. *Algebraische Konstruktion reeller Körper*. Abh. Math. Sem. Univ. Hamburg 5 (1926), 85-99.

[3] Artin, E. och O. Schreier. *Eine Kennzeichnung der reell abgeschlossenen Körper*. Abh. Math. Sem. Univ. Hamburg 5 (1927), 225-231.