jub ht 2003

ALGEBRAISK TALTEORI

KOMPLETTERINGAR TILL KURSBOKEN

1. Algebraiska talkroppar

Låt $K \subseteq L$ vara kroppar och låt $\alpha \in L$. Man betecknar med $K[\alpha]$ den minsta delring till L som innehåller K och α. $K[\alpha]$ består av alla polynomuttryck:

$$a_0 + a_1\alpha + \cdots + a_r\alpha^r, \text{ där } a_0, a_1, \ldots a_r \in K \text{ och } r \geq 0.$$

Ett element $\alpha \in L$ kallas **algebraiskt** över K om α är ett nollställe till ett polynom $p(X) \in K[X]$ som inte är nollpolynomet. Med **minimalpolynomet** för α över K menar man ett sådant polynom av minsta möjliga grad med högsta koefficienten 1. Man ser direkt att minimalpolynomet är entydigt, ty om både p och p' är minimalpolynom och $p \neq p'$ så är $p(\alpha) - p'(\alpha) = 0$ och graden av $p - p'$ är mindre än graden av p (och p'). Detta strider mot valet av p så att $p = p'$.

Exempel. (a) $\alpha = i$ är algebraiskt över Q ty $p(i) = 0$, där $p(X) = X^2 + 1$.

(b) $\alpha = \sqrt[3]{2}$ är algebraiskt över Q ty $p(\sqrt[3]{2}) = 0$, där $p(X) = X^3 - 2$.

(c) $\alpha = \sqrt{2} + i$ är algebraiskt över Q ty $\alpha^2 = 1 + 2i\sqrt{2}$ ger $(\alpha^2 - 1)^2 = -8$, dvs α satisfierar ekvationen $p(X) = 0$, där $p(X) = X^4 - 2X^2 + 9$.

(d) $\alpha = i$ är algebraiskt över R ty $p(i) = 0$, där $p(X) = X^2 + 1$. □

Ett element $\alpha \in L$ som inte är algebraiskt kallas **transcendent**. Om $K = \mathrm{Q}$ och α är ett komplext tal så säger man kort att α är algebraiskt eller transcendent (utan att behöva tillägga "över Q")

Det är inte så lätt att ge exempel på transcendenta tal. C. Hermite bevisade år 1873 att talet e är transcendent, och C.L.F. Lindemann visade 19 år senare att talet π är transcendent. Detta betyder att varken e eller π satisfierar någon polynomekvation $p(X) = 0$ med rationella koefficienter som inte alla är lika med 0.

Hur kan man hitta minimalpolynomet för ett algebraiskt element $\alpha \in L$ över K ? Svaret ger följande sats:

(1.1) Sats. *Låt $\alpha \in L \supseteq K$ vara ett algebraiskt element över K. Då gäller:*

(a) *Minimalpolynomet $p(x)$ för α över K är irreducibelt och det är en delare till varje polynom $f \in K[X]$ som har α som sitt nollställe,*

(b) *Om $q \in K[X]$ är ett irreducibelt polynom med högsta koefficienten 1 och $q(\alpha) = 0$ så är q minimalpolynomet för α.*

Bevis. (a) Om $p = p_1 p_2$, där $\text{grad}(p_1) < \text{grad}(p)$ och $\text{grad}(p_2) < \text{grad}(p)$ så ger $p(\alpha) = 0$ att $p_1(\alpha) = 0$ eller $p_2(\alpha) = 0$, vilket strider mot valet av p som ett polynom av minsta möjliga grad med α som ett nollställe.

Låt $f(\alpha) = 0$. Man har $f(X) = p(X)q(X) + r(X)$, där $\text{grad}(r) < \text{grad}(p)$ eller $r = 0$. Men även $r(\alpha) = 0$ så att r måste vara nollpolynomet enligt definitionen av p, dvs $p|f$.

(b) Enligt (a) är p en delare till q. Men q är irreducibelt så att $q = cp$, där c är en konstant. Denna konstant måste vara lika med 1, ty både p och q har högsta koefficienten 1. □

Exempel. (a) Minimalpolynomet för $\alpha = i$ över Q (eller R) är $p(X) = X^2 + 1$, ty detta polynom är irreducibelt över Q (eller R) och $p(i) = 0$.

(b) Minimalpolynomet för $\alpha = \sqrt[5]{2}$ över Q är $p(X) = X^5 - 2$, ty detta polynom är irreducibelt över Q (t ex enligt Eisensteins kriterium) och $p(\sqrt[5]{2}) = 0$. □

Det är mycket lätt att beskriva ringen $K[\alpha]$ om man känner graden av minimalpolynomet för α över K. Vår nästa sats ger en sådan beskrivning:

(1.2) Sats. *Låt $\alpha \in L \supseteq K$ och låt $p(X) \in K[X]$ vara minimalpolynomet för α över K. Låt grad$(p) = n$. Då är:*

(a) $K[\alpha] \cong K[X]/(p(X)$,

(b) $K[\alpha]$ *är en kropp och varje element i denna kropp kan skrivas entydigt på formen*

$$a_0 + a_1\alpha + \cdots a_{n-1}\alpha^{n-1}, \text{ där } a_0, a_1, \ldots a_{n-1} \in K.$$

Bevis. Betrakta ringhomomorfismen

$$\phi : K[X] \longrightarrow K[\alpha],$$

där $\phi(f(X)) = f(\alpha)$. Man har

$$\operatorname{Ker}\phi = \{f \in K[X] : \phi(f) = f(\alpha) = 0\} = (p(X)),$$

ty varje polynom som har α som sitt nollställe är en multipel av $p(X)$ enligt (b) i vår förra sats. Det är klart att bilden av ϕ är hela ringen $K[\alpha]$. Enligt Huvudsatsen om ringhomomorfismer är $K[X]/(p(X)) \cong K[\alpha]$. Vi vet att varje sidoklass i $K[X]/(p(X))$ kan representeras av exakt ett polynom

$$a_0 + a_1X + \cdots + a_{n-1}X^{n-1},\ a_i \in K,$$

så att varje element i $K[\alpha]$ kan skrivas entydigt som bilden

$$a_0 + a_1\alpha + \cdots a_{n-1}\alpha^{n-1}, a_i \in K,$$

av ett sådant polynom. Slutligen konstaterar vi att $K[\alpha]$ är en kropp därför att polynomet $p(X)$ är irreducibelt ($K[X]/(p(X))$ är en kropp då och endast då $p(x)$ är irreducibelt). □

Rent allmänt kan man betrakta varje kropp $L \supseteq K$ som ett vektorrum över K. Om det finns element $\alpha_1, \alpha_2, \ldots \alpha_n \in L$ sådana att varje element x i L kan skrivas entydigt som linjärkombination av dessa element:

$$x = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n,$$

där $a_i \in K$, så säger man att $\alpha_1, \alpha_2, \ldots \alpha_n \in L$ bildar en bas för L över K och att L har dimensionen n över K. Man skriver då $[L : K] = n$. Observera att satsen säger att $1, \alpha, \ldots, \alpha^{n-1}$ bildar en bas för $K[\alpha]$ som vektorrum över K. Dimensionen av detta rum är således lika med $\operatorname{grad}(p) = n$, dvs $[K[\alpha] : K] = n$.

Exempel. (a) Låt $\alpha = \sqrt{2}$. Då är minimalpolynomet $p(X) = x^2 - 2$. Kroppen $\mathrm{Q}[\sqrt{2}]$ består enligt satsen av alla tal $a + b\sqrt{2}$, där $a, b \in \mathrm{Q}$. $1, \sqrt{2}$ är en bas för $\mathrm{Q}[\sqrt{2}]$ över Q. Vi har $[\mathrm{Q}[\sqrt{2}] : \mathrm{Q}] = 2$.

(b) Låt $\alpha = \sqrt[3]{2}$. Då är minimalpolynomet $p(X) = X^3 - 2$. Kroppen $\mathrm{Q}[\sqrt[3]{2}]$ består enligt satsen av alla tal $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, där $a, b, c \in \mathrm{Q}$. $1, \sqrt[3]{2}, \sqrt[3]{4}$ är en bas för $\mathrm{Q}[\sqrt[3]{2}]$ över Q. Vi har $[\mathrm{Q}[\sqrt[3]{2}] : \mathrm{Q}] = 3$. □

Med $K(\alpha)$ betecknar man den minsta delkropp till L som innehåller K och α. Eftersom $K[\alpha]$ är en kropp då α är algebraiskt över K, så är $K[\alpha] = K(\alpha)$.

Exempel. Låt $K = \mathrm{Q}(\sqrt{2})$ och låt $\alpha = i$. Minimalpolynomet för α över K är $p(X) = X^2 + 1$ ty detta polynom är irreducibelt i K och $p(i) = 0$. Enligt den sista satsen består $K(i)$ av alla tal $x + yi$, där $x, y \in K$. Men $x = a + b\sqrt{2}$ och $y = c + d\sqrt{2}$, där $a, b, c, d \in \mathrm{Q}$. Alltså kan varje element i $K(i)$ skrivas entydigt på formen:

$$a + b\sqrt{2} + ci + di\sqrt{2}, \text{ där } a, b, c, d \in \mathrm{Q}.$$

Kroppen $K(i) = \mathrm{Q}(\sqrt{2})(i)$ betecknas kortare som $\mathrm{Q}(\sqrt{2}, i)$. □

Nästa sats visar att varje ändlig algebraisk utvidgning är enkel.

(1.3) Sats. *Låt $L = K(\alpha_1, \alpha_2, \ldots \alpha_n)$ vara en talkropp. Då existerar $\theta \in L$ så att $L = K(\theta)$* [1].

Bevis. Det räcker om vi visar att om $L = K(\alpha, \beta)$ så $L = K(\theta)$ för ett lämpligt $\theta \in L$. Låt f och g vara minimalpolynomen för α och β över K och låt

$$\begin{aligned} f(t) &= (t - \alpha_1) \ldots (t - \alpha_n), \\ g(t) &= (t - \beta_1) \ldots (t - \beta_m), \end{aligned}$$

där $\alpha_1 = \alpha$, $\beta_1 = \beta$. Välj $c \in K$ så att

$$\alpha_i + c\beta_j \neq \alpha_1 + c\beta_1$$

för alla $(i, j) \neq (1, 1)$. Existensen av c följer ur det faktum att

$$\alpha_i + x\beta_j = \alpha_1 + x\beta_1$$

[1] Se sats 2.2 i boken

gäller för ett ändligt antal $x \in K$ (högst mn "dåliga" x). Definiera:

$$\theta = \alpha + c\beta$$

Vi har $K(\theta) \subset K(\alpha, \beta)$. Vi vill visa att $K(\alpha, \beta) \subset K(\theta)$. Det räcker om vi visar att $\beta \in K(\theta)$ ty då $\alpha = \theta - c\beta \in K(\theta)$. Betrakta polynomen:

$$f(\theta - ct) \quad \text{och} \quad g(t).$$

Dessa polynom har koefficienter i $K(\theta)$ och de har ett gemensamt nollställe β ty

$$f(\theta - c\beta) = f(\alpha) = 0 \quad \text{och} \quad g(\beta) = 0.$$

De har inte några andra gemensamma nollställen ty om $f(\theta - c\beta_j) = 0$ för något j så är $\theta - c\beta_j = \alpha_i$ för ett i. Altså är $\alpha_i + c\beta_j = \theta = \alpha + c\beta$ vilket inträffar endast för $i = j = 1$. Detta visar att

$$SGD(f(\theta - ct),\, g(t)) = t - \beta$$

Men SGD av två polynom med koefficienter i $K(\theta)$ är ett polynom med koefficienter i $K(\theta)$ så att $\beta \in K(\theta)$. □

(1.4) Sats. *Låt $K = \mathrm{Q}(\theta)$ vara en talkropp av grad n över* Q. *Då existerar exakt n olika inbäddningar (= monomorfismer)*

$$\sigma_i : K \to \mathrm{C},\ i = 1, 2, \ldots, n.$$

Elementen $\sigma_i(\theta) = \theta_i$ är alla nollställen till minimalpolynomet för θ över Q.

Bevis. Låt p vara minimalpolynomet för θ över Q och låt $\theta_1 = \theta, \theta_2, \ldots, \theta_n$ vara alla nollställen till p (det finns exakt n nollställen ty $[K : \mathrm{Q}] = n$). Från GRK eller AS[2] vet man att

$$\mathrm{Q}(\theta) \cong \frac{\mathrm{Q}[X]}{(p(X))}.$$

för varje nollställe θ till $p(X)$ varvid en isomorfism är definierad så att $(p(x)) + r(X)$ går på $r(\theta)$ (i synnerhet går $(p(X)) + X$ på θ). Om man tar ett godtyckligt nollställe θ_i får man alltså en isomorfism:

$$\sigma_i : \mathrm{Q}(\theta) \to \mathrm{Q}(\theta_i) \subset \mathrm{C}$$

Om σ är en monomorfism så är $\sigma(p(\theta)) = p(\sigma(\theta)) = 0$ ty $p(\theta) = 0$. Alltså är $\sigma(\theta) = \theta_i$ för något i. Detta visar att $\sigma = \sigma_i$ så att σ_i är alla monomorfismer. □

[2]GRK= Grupper, ringar och kroppar, AS= Algebraiska strukturer

(1.5) Sats. *Låt $K = \mathrm{Q}(\theta)$ ha grad n över Q och låt $\alpha \in K$ ha grad m över Q. Då gäller:*

(a) *Karakteristiska polynomet* [3] *för α i K är en potens av minimalpolynomet för α över Q.*

(b) *Om $\sigma_i : K \to \mathrm{C}$ är alla inbäddningar av K i C, $i = 1, 2, \ldots, n$, så är $\sigma_i(\alpha)$ alla nollställen till minimalpolynomet för α över Q och varje sådant nollställe förekommer $\frac{n}{m}$ gånger i sekvensen $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$.*

(c) *$\alpha \in \mathrm{Q}$ då och endast då $\sigma_1(\alpha) = \ldots = \sigma_n(\alpha) = \alpha$.*

(d) *$\mathrm{Q}(\theta) = \mathrm{Q}(\alpha)$ då och endast då alla $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ är olika* [4].

Bevis. (a) Låt $f(t) = \prod_{i=1}^{n}(t - \sigma_i(\alpha))$ vara karakteristiska polynomet för α. Låt $p(t)$ vara minimalpolynomet för α. Vi har

$$f(t) = p^r(t)g(t)$$

för ett $r > 0$ och $g(t)$ relativt primt med $p(t)$. Detta följer ur det faktum att $f(\alpha) = 0$ så att $p|f$ (och entydigheten av faktoruppdelningen i $\mathrm{Q}[t]$). Vi vill visa att $g(t)$ är konstant. Om det inte är fallet så $g(\sigma_i(\alpha)) = 0$ för något i. Men $p(\sigma_i(\alpha)) = 0$ ty $\sigma_i(p(\alpha)) = p(\sigma_i(\alpha))$ och $p(\alpha) = 0$. Alltså har g och p ett gemensamt nollställe så att $p|g$ – en motsägelse. Detta visar att $f(t) = p^r(t)$ ty $g(t)$ har högsta koefficienten 1 ("moniskt").

(b) Likheten $f(t) = p^r(t)$ visar att $n = m \cdot r$ och varje nollställe till p förekommer $r = \frac{n}{m}$ gånger bland nollställena till $f(t)$.

(c) $\alpha \in \mathrm{Q} \Rightarrow \sigma_1(\alpha) = \ldots = \sigma_n(\alpha) = \alpha$. Om $\sigma_1(\alpha) = \ldots = \sigma_n(\alpha) = \alpha$ så är graden av p lika med 1 ty alla nollställen till p är olika (se Corollary 1.3 i kursboken). Alltså $\alpha \in \mathrm{Q}$.

(d) $\mathrm{Q}(\theta) = \mathrm{Q}(\alpha)$ ger $[\mathrm{Q}(\alpha) : \mathrm{Q}] = n$ så att $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ är olika. Om $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ är olika så är graden av p lika med n (ty $r = 1$). Alltså är $[\mathrm{Q}(\alpha) : \mathrm{Q}] = n$. Ur $\mathrm{Q} \subseteq \mathrm{Q}(\alpha) \subseteq \mathrm{Q}(\theta)$ följer då att $[\mathrm{Q}(\theta) : \mathrm{Q}(\alpha)] = 1$ dvs $\mathrm{Q}(\theta) = \mathrm{Q}(\alpha)$. □

[3] karakteristiskt polynom=field polynomial

[4] Se Thm. 2.5 i kursboken.

2. Ringutvidgningar och algebraiska heltal

(2.1) Definition. Låt $R \subseteq S$ vara en ringutvidgning. Man säger att $\alpha \in S$ är **helt** över R om

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0,$$

där $a_i \in R$ dvs α uppfyller en polynomekvation med koefficienter i R och med högsta koefficienten 1. Om $R = \mathrm{Z}$ och $S = \mathrm{C}$ så säger man att α är ett **algebraiskt heltal**.

Exempel. $\alpha = \sqrt{2}$ är ett algebraiskt heltal ty $p(\sqrt{2}) = 0$ där $p(X) = X^2 - 2$. På liknande sätt visas att t ex $\sqrt[3]{2}$, i, $\sqrt{2} + \sqrt{3}$ är algebraiska heltal. □

(2.2) Definition. Låt $\alpha \in S$. Med $R[\alpha]$ betecknas den minsta delring till S som innehåller både R och α.

Man ser utan större svårigheter att

$$R[\alpha] = \{a_0 + a_1\alpha + a_2\alpha + \ldots + a_N\alpha^N : a_i \in R,\ N \geq 0\}.$$

Exempel. $\mathrm{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathrm{Z}\}$, ty $(\sqrt{2})^n$ är antingen ett heltal eller ett heltalig multipel av $\sqrt{2}$. På liknande sätt är $\mathrm{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4},\ a, b, c \in \mathrm{Z}\}$ därför att $(\sqrt[3]{2})^n$ är ett heltal eller en heltalig multipel av $\sqrt[3]{2}$ eller en heltalig multipel av $\sqrt[3]{4}$. □

(2.3) Definition. Man säger att S är en **ändlig utvidgning** av R om det finns element $v_1, \ldots, v_n \in S$ sådana att varje $x \in S$ kan skrivas på formen:

$$x = a_1v_1 + a_2v_2 + \ldots + a_nv_n,$$

där $a_i \in R$. Om en sådan framställning är entydig säger man att $v_1, v_2, \ldots, v_n$ bildar **en bas** för S över R. Annars säger man att $v_1, \ldots, v_n$ **genererar** S över R.

Exempel. (a) $\mathrm{Z}[i] \supset \mathrm{Z}$ är ändlig ty $v_1 = 1$, $v_2 = i$ ger en bas: $x \in \mathrm{Z}[i]$ kan skrivas entydigt på formen $x = a + bi$.

(b) $\mathrm{Z}[\sqrt[3]{2}] \supset \mathrm{Z}$ är ändlig ty $v_1 = 1$, $v_2 = \sqrt[4]{2}$, $v_3 = \sqrt[3]{4}$ ger en bas: varje element $x \in \mathrm{Z}[\sqrt[3]{2}]$ kan skrivas entydigt på formen $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$. Entydigheten följer ur satsen om enkla kroppsutvidgningar (se (1.2)). □

Vårt närmaste syfte är ett bevis att algebraiska heltal bildar en ring (se sats (2.7)).

(2.4) Lemma. *Om $R \subseteq S$ är ändlig och $S \subseteq T$ är ändlig så är $R \subseteq T$ ändlig.*

Bevis. Låt $x \in T$. Då är $x = s_1u_1 + \ldots + s_mu_m$, där $s_i \in S$. Men $s_i = r_{i1}v_1 + \ldots + r_{in}v_n$ där $r_{ij} \in R$. Alltså är

$$x = \sum_{i=1}^{m} s_iu_i = \sum_{i=1}^{m}(\sum_{j=1}^{n} r_{ij}v_j)u_i = \sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}u_iv_j$$

Detta visar att $S \subseteq T$ är ändlig ty u_iv_j generar T över S. □

(2.5) Lemma. *Ett komplext tal α är helt över en talring R då och endast då $\alpha \in S$, där S är en ändlig utvidgning av R.*

Bevis. "⇒" Om $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$ där $a_i \in R$, så är $R[\alpha] = S$ en ändlig utvidgning av R ty

$$\alpha^n = -a_0 - a_1\alpha - \ldots - a_{n-1}\alpha^{n-1} \in R + R\alpha + \ldots + R\alpha^{n-1}$$

så att α^n är en linjär kombination av $1, \alpha, \ldots, \alpha^{n-1}$. Detta ger att varje potens α^N, $N \geq n$, är en linjär kombinaiton av $1, \alpha, \ldots, \alpha^{n-1}$. Man får detta påstående med induktion: Om $\alpha^N \in R + R\alpha + \ldots + R\alpha^{n-1}$ så har vi $\alpha^{N+1} = \alpha \cdot \alpha^N \in R\alpha + R\alpha^2 + \ldots + R\alpha^n \subseteq R + R\alpha + \ldots + R\alpha^{n-1}$ ty $\alpha^n \in R + R\alpha + \ldots + R\alpha^{n-1}$.

"⇐" Låt $\alpha \in S = Rv_1 + \ldots + Rv_n$. Då har vi:

$$\begin{cases} \alpha v_1 = a_{11}v_1 + \ldots + a_{1n}v_n \\ \alpha v_2 = a_{21}v_1 + \ldots + a_{2n}v_n \\ - - - - - - - - - - - - \\ \alpha v_n = a_{n1}v_1 + \ldots + a_{nn}v_n \end{cases}$$

Detta ger:

$$\begin{cases} (a_{11} - \alpha)v_1 + a_{12}v_2 + \ldots + a_{1n}v_n = 0 \\ a_{21}v_1 + (a_{22} - \alpha)v_2 + \ldots + a_{2n}v_n = 0 \\ - - - - - - - - - - - - - - - - \\ a_{n1}v_1 + a_{n2}v_2 + \ldots + (a_{nn} - \alpha)v_n = 0 \end{cases}$$

Ekvationssystemet är homogent och har en icke-trivial lösning $(v_1, \ldots, v_n)$. Alltså måste dess determinant vara lika med 0 dvs

$$\det \begin{bmatrix} a_{11} - \alpha & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} - \alpha & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} - \alpha \end{bmatrix} = (-1)^n\alpha^n + A_{n-1}\alpha^{n-1} + \ldots + A_0 = 0,$$

där $A_i \in R$. Alltså är α ett algebraiskt heltal. □

Som en viktig konsekvens av första delen i beviset har vi följande egenskap:

(2.6) Följdsats. *Om α är helt över R så är $R[\alpha]$ ändlig över R.*

(2.7) Sats. *Algebraiska heltal bildar en ring.*

Bevis. Låt α, β vara algebraiska heltal och betrakta ringutvidgningar

$$\mathrm{Z} \subseteq \mathrm{Z}[\alpha] \subseteq \mathrm{Z}[\alpha, \beta]$$

Utvidgningarna $\mathrm{Z} \subseteq \mathrm{Z}[\alpha]$ och $\mathrm{Z}[\alpha] \subseteq \mathrm{Z}[\alpha, \beta]$ är ändliga därför att α och β är algebraiska heltal. Enligt Lemma (2.4) är utvidgningen $\mathrm{Z} \subseteq \mathrm{Z}[\alpha, \beta]$ ändlig. Men $\alpha \pm \beta$, $\alpha\beta \in \mathrm{Z}[\alpha, \beta]$ så att dessa tal är hela enligt (2.5) (med $R = \mathrm{Z}[\alpha, \beta]$). □

(2.8) Sats. *Om θ är ett komplext nollställe till ett polynom $p(x) = X^n + \alpha_{n-1}X^{n-1} + \ldots + \alpha_1 x + \alpha_0$, där α_i är algebraiska heltal så är θ ett algebraiskt heltal.*

Bevis. Betrakta ringutvidgningarna:

$$\mathrm{Z} \subseteq \mathrm{Z}[\alpha_0] \subseteq \mathrm{Z}[\alpha_0, \alpha_1] \subseteq \ldots \subseteq \mathrm{Z}[\alpha_1, \alpha_1, \ldots, \alpha_{n-1}] \subseteq \mathrm{Z}[\alpha_0, \alpha_1, \ldots, \alpha_{n-1}, \theta]$$

Enligt Lemma (2.4) är utvidgningen $\mathrm{Z} \subseteq \mathrm{Z}[\alpha_0, \alpha_1, \ldots, \alpha_{n-1}, \theta]$ ändlig. Men

$$\theta \in \mathrm{Z}[\alpha_0, \alpha_1, \ldots, \alpha_{n-1}, \theta]$$

så att θ är ett algebraiskt heltal enligt (2.5). □

3. Hur bestämmer man en helbas ?

Detta avsnitt handlar om algoritmer med vars hjälp man kan beräkna en helbas för en algebraisk talkropp. Låt $\mathcal{O}_K$ beteckna heltalen och Δ_K diskriminanten av talkroppen K. Om R är en delring till $\mathcal{O}_K$ så betecknar $|\mathcal{O}_K/R|$ eller $[\mathcal{O}_K : R]$ ordningen av gruppen $\mathcal{O}_K/R$.

(3.1) Sats. *Låt $R = \mathrm{Z}\alpha_1 + \ldots + \mathrm{Z}\alpha_n$ vara en delring till $\mathcal{O}_K$. Då är $\Delta[\alpha_1, \ldots, \alpha_n] = |\mathcal{O}_K/R|^2\Delta_K$* [5].

Bevis. Låt $\mathcal{O}_K = \mathrm{Z}e_1 + \ldots + \mathrm{Z}e_n$, där $e_1, ..., e_n$ är en helbas för K och låt $\alpha_i = \sum a_{ij}e_j$. Då är $\Delta[\alpha_1, \ldots, \alpha_n] = (\det[a_{ij}])^2 \cdot \Delta[e_1, \ldots, e_n]$. Men $|\det[a_{ij}]| =$ antalet element i kvotgruppen $\mathcal{O}_K/R$ och $\Delta[e_1, \ldots, e_n] = \Delta_K$. □

(3.2) Proposition. *Låt $p||\mathcal{O}_K/R|$, där $R = \mathrm{Z}\alpha_1 + \ldots + \mathrm{Z}\alpha_n$. Då existerar ett heltal*

$$\alpha = \frac{1}{p}(\lambda_1\alpha_1 + \ldots + \lambda_n\alpha_n) \neq 0$$

där $\lambda_i \in \mathrm{Z}$ och $0 \leq \lambda_i \leq p - 1$ [6].

Bevis. p är en delare till ordningen av den abelska gruppen $\mathcal{O}_K/R$. Alltså finns i denna grupp ett element av ordningen p dvs $\alpha_0 + R \neq R$ och $p\alpha_0 + R = R$ dvs $p\alpha_0 \in R$. Detta betyder att $\alpha_0 \notin R$ och

$$p\alpha_0 = a_1\alpha_1 + \ldots + a_n\alpha_n, \quad a_i \in \mathrm{Z}.$$

Låt $a_i = pq_i + \lambda_i$ där $0 \leq \lambda_i \leq p - 1$. Då är $p(\alpha_0 - \sum_{i=1}^n q_i\alpha_i) = \sum_{i=1}^n \lambda_i\alpha_i$. Låt $\alpha = \alpha_0 - \sum q_i\alpha_i$. α är ett heltal och

$$\alpha = \frac{1}{p}(\lambda_1\alpha_1 + \ldots \lambda_n\alpha_n).$$

Samtidigt är $\alpha \neq 0$ ty ananrs $\alpha_0 = \sum q_i\alpha_i \in R$ – en motsägelse. □

Hur tillämpas dessa resultat?

[5] se Thm. 2.19 i kursboken.
[6] se Prop. 2.20 i kursboken

Metod 1

(1) Välj R som troligen är $\mathcal{O}_K$.

(2) Välj alla p som kan dividera $[\mathcal{O}_K : R]$ – de finns bland p med $p^2|\Delta[\alpha_1, \ldots, \alpha_n]$.

(3) Visa att $\frac{1}{p}(\lambda_1\alpha_1 + \ldots + \lambda_n\alpha_n) \neq 0$ inte finns.

Alltså $p \nmid [\mathcal{O}_K : R]$. Om det gäller för varje p så är $[\mathcal{O}_K : R] = 1$ dvs $\mathcal{O}_K = R$.

Metod 2

(1) och (2) som ovan

(3) Visa att om $\alpha \in \mathcal{O}_K$ och $p\alpha \in R$ så $\alpha \in R$.

Detta visar att α ur (3.2) inte kan existera ty om α existerar, så medför $p\alpha \in R$ att $\alpha \in R$, vilket ger en motsägelse om något $\lambda_i \neq 0$. Alltså gäller (3) i Metod 1.

Ett misslyckande i (3) säger hur man borde justera R. Då upprepar man proceduren tills man får $R = \mathcal{O}_K$.

Bra exempel finns i kursboken.

4. Fria abelska grupper

Vi vet redan att heltalen R i en algebraisk talkropp har en entydig framställning:

$$(\star) \qquad a_1e_1 + a_2e_2 + \cdot + a_ne_n,$$

där $e_1, e_2, ..., e_n \in R$ bildar en bas för R över Z och $a_1, a_2, ..., a_n \in \mathrm{Z}$. R med addition är därmed ett exempel på en abelsk grupp med ändlig bas eller, som man säger, en **ändligt genererad fri abelsk grupp**. Rent allmänt säger man att en abelsk grupp G har en **ändlig bas** (dvs är **fri** och **ändligt genererad**) om det finns element $e_1, e_2, ..., e_n \in G$ sådana att varje element i G har framställning $(\star)$. I detta avsnitt visar vi en grundläggande sats om sådana grupper.

(4.1) Sats. (a) *Om G är en abelsk grupp med en ändlig bas över* Z *och H är en delgrupp till G så har även H en ändlig bas över* Z*. Antalet element i baser för H är högst lika med antalet element i baser för G.*

(b) *Om det finns $m \in \mathrm{Z}$, $m > 0$ sådant att $mG \subseteq H$, så finns det en bas $e_1, \ldots, e_n$ för G över* Z *och naturliga tal $a_1, \ldots, a_n$ sådana att $a_1e_1, \ldots, a_ne_n$ är en bas för H över* Z*. Man kan välja a_i så att $a_1|a_2 \ldots |a_n$.*

(c) *$|G/H| = a_1a_2 \ldots a_n$ och om $[a_{ij}]$ är övergångsmatrisen från en godtycklig bas för G till en godtycklig bas för H så är $|G/H| = |\det[a_{ij}]|$.*

Bevis. (a) visas med hjälp av en okomplicerad induktion (se Thm 1.12 i kursboken).

(b) Låt $e_1, \ldots, e_n$ vara en godtycklig bas för G. Eftersom $me_1, me_2, \ldots, me_n \in H$ är linjärt oberoende över Z måste varje bas för H innehålla exakt n element. Låt $f_1, f_2, \ldots, f_n$ vara en bas för H.

Då är

$$f_i = \sum a_{ij}e_j$$

Betrakta matrisen

$$(1) \qquad \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix}$$

Nu vill vi ersätta baserna $e_1, e_2, \ldots, e_n$ och $f_1, f_2, \ldots, f_n$ med två andra baser så att övergångsmatrisen är så enkel som möjligt. Vi tillåter två typer av basbyten:

- addition av en basvektor multiplicerad med ett heltal till en annan (övergångsmatrisen har determinant 1);
- omkastning av två basvektorer (övergångsmatrisen har determinant -1).

Mot dessa två typer av basbyten svarar de elementära rad- och kolonnoperationerna:

- addition av en rad (eller en kolonn) multiplicerad med ett heltal till en annan rad (eller kolonn);
- omkastning av två rader (eller kolonner).

Låt oss välja bland alla möjliga matriser (1) som kan fås för olika baser för G och H (dvs med hjälp av de elementära rad- och kolonnoperationerna) en sådan att $a_{11} > 0$ och a_{11} antar minsta möjliga värdet. Då är a_{11} en delare till alla element i första raden och i första kolonnen ty annars en elementär rad eller kolonnoperation kan producera ett element mindre än a_{11} och detta element kan väljas som a_{11} – en motsägelse (a_{11} var det minsta). Vidare kan man ersätta (1) med en matris med alla element i första raden och i första kolonnen lika med 0. Då följer att $a_{11}|a_{ij}$ med $i > 1$ och $j > 1$ ty första raden (eller första kolonnen) kan adderas till varje annan och därefter med elementära rad- eller kolonnoperationer kan man producera ett element $\neq 0$ mindre än a_{11} om $a_{11} \nmid a_{ij}$. Nu kan vi betrakta matrisen

$$\begin{bmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & a_{n2} & \ldots & a_{nn} \end{bmatrix}$$

och avsluta bevis av (b) genom induktion.

(c) Låt $G = \mathrm{Z}e_1 + \ldots + \mathrm{Z}e_n$ och $H = \mathrm{Z}a_1e_1 + \ldots + \mathrm{Z}a_ne_n$. Betrakta grupphomomorfismen $\varphi : G \to \mathrm{Z}_{a_1} \times \ldots \times \mathrm{Z}_{a_n}$ där

$$\varphi(x_1e_1 + \ldots + x_ne_n) = ([x_1]_{a_1}, \ldots, [x_n]_{a_n})$$

Den homomorfismen är surjektiv och dess kärna består av $x_1e_1 + \ldots + x_ne_n$ sådana att $a_1|x_1, \ldots, a_n|x_n$ dvs Ker $\varphi = \mathrm{Z}a_1e_1 + \ldots + \mathrm{Z}a_ne_n = H$. Alltså är

$$G/H \cong \mathrm{Z}_{a_1} \times \ldots \times \mathrm{Z}_{a_n}$$

så att $|G/H| = a_1 \ldots a_n$.

Nu skall vi relatera $|G/H|$ till $\det[a_{ij}]$, där $[a_{ij}]$ är övergångsmatrisen från en godtycklig bas för G till en godtycklig bas för H. Låt $f_i = \sum a_{ij}e_j$, där $e_1, \ldots, e_n$ är en bas för G och $f_1, \ldots, f_n$ en bas för H. Vi vet att med hjälp av elementära rad- och kolonnoperationer kan $[a_{ij}]$ överföras på en diagonalmatris:

$$\begin{bmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & a_n \end{bmatrix}.$$

Alltså gäller

$$P \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix} Q = \begin{bmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & a_n \end{bmatrix}$$

där P och Q är heltaliga matriser med determinanter ± 1 som svarar mot sammansättningen av alla nödvändiga elementära rad- och kolonnoperationer (varje elementär rad- och kolonnoperation betyder multiplikation av $[a_{ij}]$ med en lämplig matris vars determinant är ± 1). Alltså är $\det[a_{ij}] = \pm a_1 \ldots a_n$, dvs $|G/H| = |\det[a_{ij}]|$. □

5. Hela element i cyklotomiska kroppar

Vi börjar med en sats som ofta kan användas för att bestämma helbaser i algebraiska talkroppar. Satsen visas med hjälp av de kunskaper som finns i kapitel 5 (och därför kommer att visas senare). Men man kan med fördel använda resultatet redan nu.

(5.1) Sats. *Låt $R = \mathrm{Z}[\theta] \subseteq \mathcal{O}_K$. Om θ uppfyller en Eisenstein ekvation*

$$(*) \qquad \theta^n + a_{n-1}\theta^{n-1} + \ldots + a_1\theta + a_0 = 0,\ n > 1,$$

där $p|a_{n-1}, \ldots, p|a_1$, $p|a_0$ och $p^2 \nmid a_0$, så $p \nmid [\mathcal{O}_K : R]$.

Bevis. Först visar vi att det finns ett primideal $\mathfrak{p}$ sådant att

$$(p) = \mathfrak{p}^n \quad \text{och} \quad (\theta) = \mathfrak{p}\mathfrak{b},\ \mathfrak{p} \nmid \mathfrak{b}.$$

Låt $\mathfrak{p}$ vara ett primideal som dividerar p (dvs $(p) = \mathfrak{p}\ldots$). Då säger ekvationen $(*)$ att $\mathfrak{p}$ dividerar θ. Låt

$$(p) = \mathfrak{p}^k\mathfrak{a},\ \mathfrak{p} \nmid \mathfrak{a} \quad \text{och} \quad (\theta) = \mathfrak{p}^l\mathfrak{b},\ \mathfrak{p} \nmid \mathfrak{b}, \quad k \geq 1, l \geq 1.$$

Vi har:

$$(\theta^n) = \mathfrak{p}^{ln}\ldots,\ (a_{n-1}\theta^{n-1}) = \mathfrak{p}^{k+l(n-1)}\ldots, \ldots, (a_1\theta) = \mathfrak{p}^{k+l}\ldots,\ (a_0) = \mathfrak{p}^k\ldots$$

Ekvationen $(*)$ säger nu att $ln < k + l$, ty annars tillhör varje term med undantag av den sista $\mathfrak{p}^{k+l}$. Då måste även a_0 tillhöra $\mathfrak{p}^{k+l}$ – en motsägelse ty $k + l > k$. Altså är $l(n-1) < k \leq n$ (den sista olikheten därför att $N(p) = p^n = N(\mathfrak{p})^k N(\mathfrak{a}) = p^k N(\mathfrak{a})$). Om nu $l \geq 2$ så får vi $2(n-1) < n$ så att $n < 2$ – en motsägelse. Alltså är $l = 1$ och $k = n$. Likheten $(p) = \mathfrak{p}^n\mathfrak{a}$ ger $p^n = N(\mathfrak{p})^n N(\mathfrak{a})$ så att $N(\mathfrak{p}) = p$ och $N(\mathfrak{a}) = 1$ dvs $\mathfrak{a} = R$. Detta visar att $(p) = \mathfrak{p}^n$.

Nu kan vi bevisa satsen. Enligt (3.2) skall man visa att

$$\alpha \in \mathcal{O}_K \quad \text{och} \quad p\alpha \in R \Rightarrow \alpha \in R.$$

Låt

$$p\alpha = x_0 + x_1\theta + \ldots + x_{n-1}\theta^{n-1}.$$

$p \in \mathfrak{p}$ och $\theta \in \mathfrak{p}$ ger att $x_0 \in \mathfrak{p}$ dvs $N(\mathfrak{p}) = p|x_0^n$ så att $p|x_0$. Låt $x_0 = px_0'$. Då är

$$p(\alpha - x_0') = \theta(x_1 + x_2\theta + \ldots + x_{n-1}\theta^{n-2}).$$

Nu har vi $\mathfrak{p}^n|\theta(x_1 + x_2\theta + \ldots + x_{n-1}\theta^{n-2})$ och $\mathfrak{p}^2 \nmid \theta$. Alltså $\mathfrak{p}^{n-1}|x_1 + x_2\theta + \ldots + x_{n-1}\theta^n$. Men $\mathfrak{p}|\theta$ så att $\mathfrak{p}|x_1$ dvs $p|x_1$ med samma argument som för x_0. Låt $x_1 = px_1'$. Då är

$$p(\alpha - x_0' - x_1'\theta) = \theta^2(x_2 + x_3\theta + \ldots + x_{n-1}\theta^{n-3}).$$

Här är $\mathfrak{p}^2|(\theta)^2$ men $\mathfrak{p}^3 \nmid (\theta)^2$. Eftersom $\mathfrak{p}^n$ dividerar höger led får vi $\mathfrak{p}^{n-2}|x_2 + x_3\theta + \ldots + x_{n-1}\theta^{n-3}$ vilket ger $\mathfrak{p}|x_2$ osv. Slutligen är

$$p\alpha = p(x_0' + x_1'\theta + \ldots + x_{n-1}'\theta^{n-1})$$

dvs $\alpha = x_0' + x_1'\theta + \ldots + x_{n-1}'\theta^{n-1} \in R$. □

Nu visar vi att de algebraiska heltalen i den cyklotomiska kroppen $\mathrm{Q}(\zeta)$, $\zeta^p = 1$, $\zeta \neq 1$, bildar ringen $\mathrm{Z}[\zeta]$. Först följer vi beviset i kursboken och därefter visar vi samma sats med hjälp av (5.1).

(5.2) Sats. *Algebraiska heltalen i den cyklotomiska kroppen* $\mathrm{Q}(\zeta)$, $\zeta^p = 1$, $\zeta \neq 1$, *bildar ringen* $\mathrm{Z}[\zeta]$.

Bevis. Låt $\mathcal{O}$ beteckna heltalen i $\mathrm{Q}(\zeta)$. Det är klart att $\mathrm{Z}[\zeta] \subseteq \mathcal{O}$. Vi vill visa att om $\alpha \in \mathcal{O}$ så $\alpha \in \mathrm{Z}[\zeta]$. Talen $1, \zeta, \ldots, \zeta^{p-2}$ bildar en bas för $\mathrm{Q}(\zeta)$ över Q så att

$$\alpha = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2}$$

där $a_i \in \mathrm{Q}$. Antag att $\alpha \in \mathcal{O}$. Man visar först att $pa_i \in \mathrm{Z}$ som i kursboken på sid. 67. Betrakta nu $\lambda = 1 - \zeta$. Vi har $\mathrm{Z}[1-\zeta] = \mathrm{Z}[\zeta]$ så att vi vill visa att $\alpha \in \mathrm{Z}[\lambda]$. Vi har:

$$p\alpha = pa_0 + pa_1\zeta + \ldots + pa_{p-2}\zeta^{p-2} =$$

$$pa_0 + pa_1(1-\lambda) + \ldots + pa_{p-2}(1-\lambda)^{p-2} = c_0 + c_1\lambda + \ldots + c_{p-2}\lambda^{p-2}$$

där $c_i \in \mathrm{Z}$. Vi vill visa nu att $p|c_i$ för alla i. Då kan man dela den sista likheten med p, vilket ger

$$\alpha = \frac{c_0}{p} + \frac{c_1}{p}\lambda + \ldots + \frac{c_{p-2}}{p}\lambda^{p-2} \in \mathrm{Z}[\lambda].$$

Vi skall visa om en stund att $p = \lambda^{p-1}\epsilon$, där ϵ är en enhet i $\mathcal{O}$. Därför är

$$\lambda^{p-1}\epsilon\alpha = c_0 + c_1\lambda + \ldots + c_{p-2}\lambda^{p-2} \tag{1}$$

så att $\lambda|c_0$, vilket ger $N(\lambda) = p|N(c_0) = c_0^{p-1}$ dvs $p|c_0$. Låt $c_0 = pc_0' = \lambda^{p-1}\epsilon c_0'$. Likheten (1) ger då (efter förkortning med λ):

$$\lambda^{p-2}\epsilon\alpha = \lambda^{p-2}\epsilon c_0' + c_1 + c_2\lambda + \ldots + c_{p-2}\lambda^{p-3}. \tag{2}$$

Den likheten ger $\lambda|c_1$ så att $N(\lambda) = p|N(c_1) = c_1^{p-1}$ dvs $p|c_1$. Låt $c_1 = pc_1' = \lambda^{p-1}\epsilon c_1'$. Likheten (2) ger på liknande sätt:

$$\lambda^{p-3}\epsilon\alpha = \lambda^{p-3}\epsilon c_0' + \lambda^{p-2}\epsilon c_1' + c_2 + c_3\lambda + \ldots + c_{p-2}\lambda^{p-4}$$

om $p > 4$. Vidare fortsätter man med enkel induktion. □

Det återstår att visa:

(**5.3**) **Lemma.** *$p = \lambda^{p-1}\epsilon$, där ϵ är en enhet.*

Bevis. Vi vet att $(1-\zeta)(1-\zeta^2)\dots(1-\zeta^{p-1}) = p$ (se (3.9) sid. 66 i kursboken). Men $1-\zeta^i = \epsilon_i\lambda$, där

$$\epsilon_i = \frac{1-\zeta^i}{1-\zeta} \quad \text{och} \quad \lambda = 1-\zeta.$$

ϵ_i är en enhet ty $\epsilon_i = 1+\zeta+\ldots+\zeta^{i-1}$ är ett algebraiskt heltal och

$$\frac{1}{\epsilon_i} = \frac{1-\zeta}{1-\zeta^i} = \frac{1-(\zeta^i)^j}{1-\zeta^i} = 1+\zeta^i+(\zeta^i)^2+\ldots+(\zeta^i)^{j-1}$$

är ett algebraiskt heltal, där j väljs så att $ij \equiv 1 \pmod{p}$. Alltså är $p = \lambda\cdot\lambda\epsilon_2\cdot\ldots\cdot\lambda\epsilon_{p-1} = \lambda^{p-1}\epsilon, \epsilon$ en enhet. □

Nu visar vi samma sats (5.2) med hjälp av (5.1).

Bevis. Vi skall använda Metod 2 på sid. 11. Först konstaterar man enkelt (se Thm. 3.6 i kursboken) att

$$\Delta[1,\zeta,...,\zeta^{p-2}] = (-1)^{(p-1)/2}p^{p-2}.$$

Alltså kan $|\mathcal{O}/R|$ eventuellt vara delbar med p. Vi har $R = \mathrm{Z}[\zeta] = \mathrm{Z}[\zeta-1]$ och $-\lambda = \zeta-1$ satisfierar ekvationen:

$$p_{-\lambda}(x) = (x+1)^{p-1}+\cdots+(x+1)+1 = \frac{(x+1)^p-1}{(x+1)-1}.$$

$p_{-\lambda}$ är ett Eisensteinpolynom därför att alla dess koefficienter är delbara med p med undantag av den högsta och den lägsta koefficienten är p. Enligt (5.1) är inte p en delare till $|\mathcal{O}/R|$ så att $|\mathcal{O}/R| = 1$ dvs $\mathcal{O} = R$. □