ÖVNINGSPROBLEM I GALOISTEORI

JULIUSZ BRZEZINSKI

MATEMATISKA VETENSKAPER
CHALMERS OCH GÖTEBORGS UNIVERSITET
GÖTEBORG 2003

Innehåll

BETECKNINGAR

$\mathbb{N}$	de naturliga talen
$\mathbb{Z}$	de hela talen
$\mathbb{Q}$	de rationella talen
$\mathbb{C}$	de komplexa talen
$\mathbb{Z}_n$	de hela talen modulo n
S_n	den symmetriska gruppen av grad n
C_n	en cyklisk grupp av ordning n
$\lvert X \rvert$	antalet element i mängden X

Tecknet "$*$" vid övningens nummer betyder att övningen är lite svårare.

1

Delkroppar, primkroppar och kroppens karakteristik

En **primkropp** är en kropp utan äkta delkroppar.

1.T$_1$ *Varje primkropp är isomorf med kroppen* $\mathbb{Q}$ *eller med en av kropparna* $\mathbb{Z}_p$ *för ett primtal* p.

1.T$_2$ *Varje kropp innehåller exakt en primkropp.*

Med **karakteristiken** av en kropp K menar man talet 0 om primkroppen i K är isomorf med $\mathbb{Q}$ och talet p om primkroppen i K är isomorf med $\mathbb{Z}_p$. Karakteristiken av K betecknas med $\text{char}(K)$. Man säger att en kropp L är en **utvidgning** av en kropp K om $L \supseteq K$. Om $K_i,\ i \in I$ (I en indexmängd) är delkroppar till L så är också deras snitt $\cap K_i,\ i \in I$, en delkropp till L. Om $L \supseteq K$ och X är en delmängd till L, så betecknar man med $K(X)$ snittet av alla delkroppar till L som innehåller både K och X ($K(X)$ är den minsta delkropp till L som innehåller både K och X). Om $X = \{\alpha_1, \ldots, \alpha_n\}$ så skriver man vanligen $K(X) = K(\alpha_1, \ldots, \alpha_n)$. Om $X = K'$ är en delkropp till L så betecknas $K(K')$ med KK' och kallas **kompositum** av K och K'.

ÖVNINGAR

1.1. Vilka av följande delmängder till $\mathbb{C}$ är kroppar med avseende på vanlig addition och multiplikation av tal:

a) $\mathbb{Z}$;
b) $\{0, 1\}$;
c) $\{0\}$;
d) $\{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$;
e) $\{a + b\sqrt[3]{2},\ a, b \in \mathbb{Q}\}$;
f) $\{a + b\sqrt[4]{2}, a, b \in \mathbb{Q}\}$;
g) $\{a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$;
h) $\{z \in \mathbb{C} : |z| \leq 1\}$.

1.2. Visa att varje delkropp till $\mathbb{C}$ innehåller $\mathbb{Q}$.

1.3. Ge exempel på en oändlig kropp av karakteristiken $\neq 0$.

1.4. Visa att karakteristiken av en kropp K är det minsta naturliga talet n sådant att $na = 0$ för varje $a \in K$ eller den är 0 om ett sådant n inte existerar.

1.5. Låt $L \supseteq K$ vara en kroppsutvidgning och $\alpha \in L \setminus K$, $\alpha^2 \in K$. Visa att

$$K(\alpha) = \{a + b\alpha, \text{ där } a, b \in K\}.$$

1.6. Beskriv alla tal som tillhör kropparna:

a) $\mathbb{Q}(\sqrt{2})$; b) $\mathbb{Q}(i)$; c) $\mathbb{Q}(\sqrt{2}, i)$; d) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

1.7. Visa att

a) $\mathbb{Q}(\sqrt{2}, i\sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$;
b) $\mathbb{Q}(\sqrt{2}, \sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$;
c) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$;
d) $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$, då $a, b \in \mathbb{Q}$, $\sqrt{a} + \sqrt{b} \neq 0$.

1.8. Beskriv följande delkroppar till $\mathbb{C}$:

a) $\mathbb{Q}(X)$, där $X = \{\sqrt{2}, 1 + 2\sqrt{8}\}$;
b) $\mathbb{Q}(i)(X)$, där $X = \{\sqrt{2}\}$;
c) K_1K_2, där $K_1 = \mathbb{Q}(i)$, $K_2 = \mathbb{Q}(\sqrt{5})$;
d) $\mathbb{Q}(X)$, där $X = \{z \in \mathbb{C} : z^4 = 1\}$.

1.9. Låt K vara en kropp.

a) Visa att alla matriser $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, där $a, b \in K$ bildar en kropp L med avseende på matrisaddition och matrismultiplikation då och endast då ekvationen $X^2 + 1 = 0$ saknar lösningar i K.

b) Visa att L innehåller en kropp isomorf med K.

c) Konstruera en kropp med 9 element och bestäm dess karakteristik.

1.10. Låt K vara en kropp

a) Formulera ett lämpligt villkor sådant att alla matriser $\begin{bmatrix} a & b \\ -b & a - b \end{bmatrix}$, $a, b \in K$, bildar en kropp med avseende på matrisaddition och matrismultiplikation.

b) Konstruera en kropp med 4 element och skriv ut additions- och multiplikationstabellerna för denna.

1.11. I en kropp K gäller likheten $a^4 = a$ för varje $a \in K$. Bestäm karakteristiken av K.

1.12. Låt K vara en kropp av karakteristiken p. Visa att $(a + b)^{p^m} = a^{p^m} + b^{p^m}$ då $a, b \in K$ och m är ett naturligt tal.

2

Algebraiska utvidgningar

Låt $L \supseteq K$ vara två kroppar. Man säger att ett element $\alpha \in L$ är **algebraiskt** över K om det finns ett nollskilt polynom $f \in K[X]$ sådant att $f(\alpha) = 0$. I det motsatta fallet kallas α **transcendent** över K. Om $\alpha \in \mathbb{C}$ är algebraiskt över $\mathbb{Q}$ så säger man att α är ett **algebraiskt tal**. Ett icke-algebraiskt tal kallas **transcendent**. Om $\alpha \in L$ är algebraiskt över K säger man att ett nollskilt polynom av lägsta möjliga grad bland alla polynom $f \in K[X]$ sådana att $f(\alpha) = 0$ är ett **minimalpolynom** för α över K. Graden av f kallas **graden** av α över K.

2.T$_1$ *Låt $\alpha \in L \supseteq K$ vara ett algebraiskt element över K.*

a) *Ett minimalpolynom för α över K är irreducibelt och delar varje polynom i $K[X]$ som har α som sitt nollställe.*

b) *Ett irreducibelt polynom $f \in K[X]$ sådant att $f(\alpha) = 0$ är ett minimalpolynom för α över K.*

c) *Alla minimalpolynom för α över K får man ur ett sådant polynom genom att multiplicera det med nollskilda konstanter ur K.*

Ibland, med hänsyn till sista delen av satsen, väljer man entydigt ett minimalpolynom – **minimalpolynomet** – det vars koefficient framför högsta potensen av variabeln är lika med 1.

2.T$_2$ a) *Om $\alpha \in L \supseteq K$ är ett algebraiskt element över K, så kan varje element i $K(\alpha)$ skrivas entydigt på formen $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$, där $a_i \in K$ och n är graden av minimalpolynomet för α över K.*

b) *Om $\alpha \in L \supseteq K$ är ett transcendent element över K, så är $K(\alpha) \simeq K(X)$, där $K(X)$ är kroppen av de rationella funktionerna över K.*

Om $L \supseteq K$ så kan man betrakta L som ett linjärt rum över K. Med **graden** $[L : K]$ menar man dimensionen av det linjära rummet L över K. Om den dimensionen är oändlig, så skriver man $[L : K] = \infty$. Sats $2.T_2$ a) säger att $[K(\alpha) : K] = \text{grad}\,(f)$ då α är ett algebraiskt element och f dess minimalpolynom.

2.T$_3$ *Om $M \supseteq L \supseteq K$, så är $[M : K] = [M : L][L : K]$.*

En utvidgning $L \supseteq K$ kallas **algebraisk** om varje element i L är algebraiskt över K. Den kallas **ändlig** om $[L : K] \neq \infty$. Man säger att utvidgningen $L \supseteq K$ är **ändligt genererad** om $L = K(\alpha_1, \ldots, \alpha_n)$, där $\alpha_i \in L$.

2.T$_4$ *En utvidgning $L \supseteq K$ är ändlig då och endast då den är algebraisk och ändligt genererad.*

2.T$_5$ *Låt $L \supseteq K$. Alla element i L som är algebraiska över K bildar en kropp.*

Om $K = \mathbb{Q}$ och $L = \mathbb{C}$, så kommer kroppen av de algebraiska talen över $\mathbb{Q}$ att betecknas med $\mathbb{A}$ (= kroppen av de algebraiska talen).

ÖVNINGAR

2.1. Vilka av följande tal är algebraiska?

a) $1 + \sqrt{2} + \sqrt{3}$;
b) $\sqrt{2} + \sqrt[5]{2}$;
c) $\sqrt[3]{3} + \sqrt{2}$;
d) $\sqrt{\pi} + 1$;
e) $\sqrt{\pi} + \sqrt{2}$;
f) $\sqrt[3]{1 + \sqrt{e}}$.

2.2. Bestäm minimalpolynomet och graden för α över K då:

a) $K = \mathbb{Q},\ \alpha = \sqrt[3]{\sqrt{3} + 1}$;
b) $K = \mathbb{Q},\ \alpha = \sqrt{2} + \sqrt[3]{2}$;
c) $K = \mathbb{Q},\ \alpha^5 = 1,\ \alpha \neq 1$;
d) $K = \mathbb{Q}(i),\ \alpha = \sqrt{2}$;
e) $K = \mathbb{Q}(\sqrt{2}),\ \alpha = \sqrt[3]{2}$;
f) $K = \mathbb{Q},\ \alpha^p = 1,\ \alpha \neq 1,\ p$ ett primtal.

2.3. Bestäm graden och en bas för följande utvidgningar $L \supseteq K$:

a) $K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt{2}, i)$;
b) $K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$;
c) $K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$;
d) $K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt[3]{2} + 2\sqrt[3]{4})$;
e) $K = \mathbb{R}(X + \frac{1}{X}),\ L = \mathbb{R}(X)$;
f) $K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$;
g) $K = \mathbb{Q}(\sqrt{3}),\ L = \mathbb{Q}(\sqrt[3]{1 + \sqrt{3}})$;
h) $K = \mathbb{Z}_2,\ L = \mathbb{Z}_2(\alpha)$, där $\alpha^4 + \alpha + 1 = 0$;
i) $K = \mathbb{Z}_3,\ L = \mathbb{Z}_3(\alpha)$, där $\alpha^3 + \alpha^2 + 2 = 0$;
j) $K = \mathbb{R}(X^2 + \frac{1}{X^2}),\ L = \mathbb{R}(X)$.

2.4. Visa att ett komplext tal $z = a + bi$ är algebraiskt (över $\mathbb{Q}$) då och endast då a och b är algebraiska.

2.5. Visa att talen $\sin r\pi$ och $\cos r\pi$ är algebraiska om r är ett rationellt tal.

2.6. Låt $L = \mathbb{Q}(\sqrt[3]{2})$. Bestäm $a, b, c \in \mathbb{Q}$ sådana att $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ då

a) $x = \dfrac{1}{\sqrt[3]{2}}$; b) $x = \dfrac{1}{1+\sqrt[3]{2}}$; c) $x = \dfrac{1+\sqrt[3]{2}}{1+\sqrt[3]{2}+\sqrt[3]{4}}$.

2.7. Låt $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Bestäm $a, b, c, d \in \mathbb{Q}$ sådana att $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ då

a) $x = \dfrac{1}{\sqrt{2}+\sqrt{3}}$; b) $x = \dfrac{1}{1+\sqrt{2}+\sqrt{3}}$; c) $x = \dfrac{\sqrt{2}+\sqrt{3}}{1+\sqrt{2}+\sqrt{3}+\sqrt{6}}$.

2.8. Låt $L = \mathbb{Z}_2(\alpha)$, där $\alpha^4+\alpha+1 = 0$. Bestäm $a, b, c, d, \in \mathbb{Z}_2$ sådana att $x = a+b\alpha+c\alpha^2+d\alpha^3$ då

a) $x = \dfrac{1}{\alpha}$; b) $x = \alpha^5$; c) $x = \alpha^{15}$; d) $x = \dfrac{1}{\alpha^2+\alpha+1}$.

2.9. a)* Visa att om $\alpha \in K(X) \setminus K$ och $\alpha = \frac{p(X)}{q(X)}$, där $p, q \in K[X]$, och $SGD(p, q) = 1$ så är $[K(X) : K(\alpha)] = n$, där $n = \max(\operatorname{grad} p, \operatorname{grad} q)$.

b) Visa att om $\alpha \in K(X) \setminus K$, så är α transcendent över K.

2.10. Låt M_1, M_2 vara två kroppar mellan K och L.

a) Visa att om $[M_1 : K] \neq \infty$ och $[M_2 : K] \neq \infty$, så är $[M_1M_2 : K] \neq \infty$.

b) Visa att om $[M_1 : K] = r$ och $[M_2 : K] = s$, där $(r, s) = 1$, så är $[M_1M_2 : K] = rs$.

c) Vad kan man säga allmänt om sambandet mellan $[M_1 : K]$, $[M_2 : K]$ och $[M_1M_2 : K]$?

2.11. Visa att om $[K(\alpha) : K]$ är udda, så är $K(\alpha) = K(\alpha^2)$. Är det sant att $K(\alpha) = K(\alpha^2)$ implicerar att $[K(\alpha) : K]$ är udda?

2.12. Visa att om $f \in K[X]$ är irreducibelt över K och $L \supseteq K$ är en utvidgning sådan att $(\operatorname{grad} f, [L : K]) = 1$, så är f irreducibelt över L.

2.13. Visa att om L är en kropp och $[L : \mathbb{R}] \neq \infty$, så är $L \cong \mathbb{R}$ eller $L \cong \mathbb{C}$.

2.14. Är det sant att för varje delare d till $[L : K]$ existerar en kropp M mellan K och L sådan att $[M : K] = d$?

2.15. Man vet att talen e och π är transcendenta. Det är inte känt om $e + \pi$ och $e\pi$ är transcendenta. Visa att minst ett av talen $e + \pi$ eller $e\pi$ måste vara transcendent.

2.16. Man vet att α är ett algebraiskt tal. Visa att även följande tal är algebraiska

a) α^2; b) $\sqrt{\alpha}$; c) $\sqrt[3]{1+\sqrt{\alpha}}$.

3

Splittringskroppar. Ändliga kroppar

Om K är en kropp och $f \in K[X]$, så säger man att $L \supseteq K$ är en **splittringskropp** för f över K om $L = K(\alpha_1, \ldots, \alpha_n)$ och $f(X) = a(X - \alpha_1) \ldots (X - \alpha_n)$, där $a \in K$. Man säger då att f har alla sina nollställen i L och att L genereras över K av dessa nollställen. Ibland betecknar man splittringskroppen för f över K med $K(f = 0)$.

3.T$_1$ a) *Varje polynom $f \in K[X]$ har en splittringskropp över K.*

b) *Om $\tau : K_1 \to K_2$ är en isomorfism av kroppar, L_1 är en splittringskropp för ett polynom $f \in K_1[X]$ och L_2 är en splittringskropp för polynomet $\tau(f) \in K_2[X]$, så existerar en isomorfism $\sigma : L_1 \to L_2$*

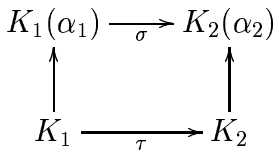
$$\begin{array}{ccc} L_1 & \xrightarrow[\sigma]{} & L_2 \\ \uparrow & & \uparrow \\ K_1 & \xrightarrow[\tau]{} & K_2 \end{array}$$

som förlänger τ (dvs $\sigma|_{K_1} = \tau$). Speciellt om $K_1 = K_2 = K$ och $\tau = id.$ så är två splittringskroppar för f över K K-isomorfa (dvs isomorfismen σ avbildar varje element i K på sig självt).

Man brukar bevisa den satsen med hjälp av följande partiella resultat:

3.T$_2$ a) *Om f är ett irreducibelt polynom över K, så existerar en kropp $L \supseteq K$ sådan att $L = K(\alpha)$ och $f(\alpha) = 0$.*

b) *Om $\tau : K_1 \to K_2$ är en isomorfism av kroppar, f ett irreducibelt polynom över K_1, $L_1 = K(\alpha_1)$, där $f(\alpha_1) = 0$ och $L_2 = K(\alpha_2)$, där $\tau(f)(\alpha_2) = 0$, så finns det en isomorfism $\sigma : K_1(\alpha_1) \to K_2(\alpha_2)$.*



sådan att $\sigma(\alpha_1) = \alpha_2$ *och* $\sigma|_{K_1} = \tau$.

Om $f(X) = a_0X + \ldots + a_nX^n \in K[X]$ så definierar man **derivatan** f' av f som polynomet $f'(X) = a_1 + 2a_2X + \ldots + na_nX^{n-1}$. Precis som för polynom ur $\mathbb{R}[X]$ gäller det att $(f_1 + f_2)' = f_1' + f_2'$ och $(f_1f_2)' = f_1'f_2 + f_1f_2'$.

3.T$_3$ *Ett polynom* $f \in K[X]$ *saknar multipla nollställen i varje utvidgning* $L \supseteq K$ *då och endast då* $SGD(f, f') = 1$.

Genom att utnyttja den satsen och konstruktionen av splittringskroppar kan man enkelt beskriva alla ändliga kroppar.

3.T$_4$ a) *Antalet element i en ändlig kropp är en potens av ett primtal.*

b) *Om* p *är ett primtal och* $n \geq 1$, *så är splittringskroppen för* $X^{p^n} - X$ *över* $\mathbb{Z}_p$ *en ändlig kropp med* p^n *element.*

c) *Två ändliga kroppar med lika många element är isomorfa. Mera exakt är varje ändlig kropp med* p^n *element en splittringskropp för* $X^{p^n} - X$ *över* $\mathbb{Z}_p$.

Man säger att $\bar{K}$ är ett **algebraiskt hölje** till kroppen K om varje polynom med koefficienter i K har alla sina nollställen i $\bar{K}$ och $\bar{K}$ genereras över K av alla nollställen till alla polynom i $K[X]$.

3.T$_5$ *För varje kropp* K *existerar ett algebraiskt hölje* $\bar{K}$ *och två algebraiska höljen till samma kropp* K *är* K*-isomorfa.*

En kropp kallas **algebraiskt sluten** om $K = \bar{K}$ (t.ex. $K = \mathbb{C}$).

ÖVNINGAR

3.1. Bestäm graden och en bas av en splittringskropp över K för $f \in K[X]$ då

a) $K = \mathbb{Q},\ f = (X^2-2)(X^2-5)$;
b) $K = \mathbb{Q},\ f = X^3-2$;
c) $K = \mathbb{Q},\ f = X^4-2$;
d) $K = \mathbb{Q},\ f = X^4+X^2-1$;
e) $K = \mathbb{Q},\ f = X^4+1$;
f) $K = \mathbb{Q}(i),\ f = X^4-2$;
g) $K = \mathbb{Q}(i),\ f = (X^2-2)(X^2-3)$;
h) $K = \mathbb{Q},\ f = X^p-1$, p ett primtal.

3.2. Avgör om följande par av kroppar är isomorfa:

a) $\mathbb{Q}(\sqrt[4]{2})$ och $\mathbb{Q}(i\sqrt[4]{2})$;
b) $\mathbb{Q}(\sqrt[3]{1+\sqrt{3}})$ och $\mathbb{Q}(\sqrt[3]{1-\sqrt{3}})$;
c) $\mathbb{Q}(\sqrt{2})$ och $\mathbb{Q}(\sqrt{3})$.

3.3. Visa att en kropp med p^n element innehåller en kropp med p^m element då och endast då $m|n$.

3.4. Låt $f(X)$ vara ett irreducibelt polynom i $\mathbb{Z}_p[X]$. Visa att $f(X)|X^{p^n}-X$ då och endast då grad $(f(X))|n$.

3.5* Låt $v_p(n)$ beteckna antalet irreducibla polynom av n:te graden i $\mathbb{Z}_p[X]$. Visa att

$$\sum_{d|n} d v_p(d) = p^n \quad \text{och} \quad v_p(n) = \frac{1}{n}\sum_{d|n} p^d \mu(\frac{n}{d}),$$

där $\mu(n)$ är Möbiusfunktionen dvs $\mu(n) = 0$ om det finns ett primtal p vars kvadrat är en delare till n, och $\mu(n) = (-1)^k$ om n är en produkt av k olika primtal samt $\mu(1) = 1$.

3.6 Ett irreducibelt polynom $f \in \mathbb{Z}_p[X]$ av n:te graden kallas primitivt om $f \nmid X^m - X$ då $m < p^n$. Visa att antalet primitiva polynom av n:te graden är lika med $\frac{1}{n}\varphi(p^n-1)$, där φ är Eulers funktion.

3.7 a)* Visa att en ändlig delgrupp till den multiplikativa gruppen K^* av en kropp K är cyklisk.

b) Visa att om $L \supseteq K$ är ändliga kroppar så finns det ett element $\epsilon \in L$ sådant att $L = K(\epsilon)$.

4

Automorfismgrupper av kroppar. Galoisgrupper

Låt L vara en kropp. Med en **automorfism** av L menar man en omvändbar funktion $\sigma : L \to L$ som avbildar L på hela L och sådan att

a) $\sigma(x+y) = \sigma(x) + \sigma(y)$
b) $\sigma(xy) = \sigma(x)\sigma(y)$

för godtyckliga $x, y \in L$. Om $L \supseteq K$ är en kroppsutvidgning så säger man att en automorfism $\sigma : L \to L$ är en K**-automorfism** om

c) $\sigma(x) = x$ för varje $x \in K$.

4.T$_1$ *Alla K-automorfismer av L bildar en grupp med avseende på sammansättning av automorfismer.*

Gruppen av alla K-automorfismer av L betecknas med $G(L : K)$ och kallas **Galoisgruppen** av L över K. Om G är en godtycklig grupp som består av automorfismer av L (t.ex. $G = G(L : K)$ då $L \supseteq K$), så definierar man

$$L^G = \{x \in L : \forall_{\sigma \in G} \sigma(x) = x\}.$$

4.T$_2$ *Om G är en grupp av automorfismer av L (ändlig eller oändlig) så är L^G en delkropp till L och $[L : L^G] = |G|$.*

Nästan alla övningar kommer att koncentreras kring denna viktiga sats som är en konsekvens av följande resultat:

4.T$_3$ Dedekinds Lemma. *Om $\sigma_1, \sigma_2, \ldots, \sigma_n$ är olika automorfismer av en kropp L och likheten $a_1\sigma_1(x) + a_2\sigma_2(x) + \ldots + a_n\sigma_n(x) = 0$, där $a_i \in L$, gäller för varje $x \in L$, så är $a_1 = a_2 = \ldots = a_n = 0$.*

Dedekinds Lemma kan också formuleras så att olika automorfismer av en kropp L är linjärt oberoende över L (i det linjära L-rum som består av alla funktioner $f : L \to L$). Med **Galoisgruppen** över K av ekvationen $f(X) = 0$ eller polynomet $f(X)$, där $f(X) \in K[X]$, menar man Galoisgruppen för splittringskroppen $K(f = 0)$ över K.

ÖVNINGAR

4.1. Låt $L \supseteq K$ vara en kroppsutvidgning.

a) Visa att om $\alpha \in L$ är ett nollställe till $f \in K[X]$ och $\sigma \in G(L : K)$, så är också $\sigma(\alpha)$ ett nollställe till f.

b) Visa att om $L = K(\alpha_1, \ldots, \alpha_r)$ och två automorfismer $\sigma, \tau \in G(L : K)$ är lika för varje generator α_i (dvs $\sigma(\alpha_i) = \tau(\alpha_i)$ för varje i), så är $\sigma = \tau$ dvs $\sigma(\alpha) = \tau(\alpha)$ för varje $\alpha \in L$).

4.2. Bestäm Galoisgrupper för följande utvidgningar $L \supseteq K$:

a) $L = \mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}$;
b) $L = \mathbb{Q}(\sqrt[3]{2})$, $K = \mathbb{Q}$;
c) $L = \mathbb{Q}(\sqrt[4]{2})$, $K = \mathbb{Q}$;
d) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K = \mathbb{Q}$;
e) $L = \mathbb{Z}_2(X)$, $K = \mathbb{Z}_2(X^2)$;
f) $L = \mathbb{Z}_5(X)$, $K = \mathbb{Z}_5(X^4)$.

4.3. Visa att identiteten är den enda automorfismen av en primkropp (dvs $\mathbb{Q}$ eller $\mathbb{Z}_p$).

4.4. Visa att kroppen av de reella talen $\mathbb{R}$ saknar icke-triviala automorfismer.

4.5. Visa att om $[L : K] < \infty$, så är ordningen av Galoisgruppen $G(L : K)$ en delare till utvidgningens grad $[L : K]$.

4.6. Visa att om σ är en K-automorfism av kroppen $K(X)$, så är $\sigma(X) = \frac{aX+b}{cX+d}$, där $a, b, c, d \in K$ och $ad - bc \neq 0$.

4.7. Låt $L = \mathbb{Z}_2(X)$ och låt G vara gruppen av alla $\mathbb{Z}_2$-automorfismer av L (se övn. 4.6). Bestäm L^G.

4.8. Låt $L = \mathbb{Z}_3(X)$ och låt G vara gruppen av alla automorfismer av L sådana att $\sigma(X) = aX + b$, där $a, b \in \mathbb{Z}_3$ och $a \neq 0$. Bestäm L^G.

4.9. a) Låt $L = \mathbb{R}(X, Y)$ och $G = \{\sigma_1, \sigma_2\}$, där σ_1 är identiteten och σ_2 definieras av $\sigma_2(X) = -X$, $\sigma_2(Y) = Y$. Bestäm L^G.

b) Visa med hjälp av a) att om $f(X, Y) \in \mathbb{R}(X, Y)$ är sådant att $f(-X, Y) = -f(X, Y)$, så är $\int f(\sin x, \cos x)dx = \int g(t)dt$ för en funktion $g \in \mathbb{R}(t)$ och $t = \cos x$.

4.10. a) Låt $L = \mathbb{R}(X, Y)$ och $G = \{\sigma_1, \sigma_2\}$, där σ_1 är identiteten och σ_2 definieras av $\sigma_2(X) = -X$, $\sigma_2(Y) = -Y$. Bestäm L^G.

b) Låt $f(X, Y) \in \mathbb{R}(X, Y)$ och $f(-X, -Y) = f(X, Y)$. Visa med hjälp av a) hur man kan uttrycka integralen $\int f(\sin x, \cos x)dx$ som en integral av en rationell funktion.

4.11. Låt $L = \mathbb{Q}(X, Y)$ och $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ vara den grupp av automorfismer av L som definieras av tabellen

	X	Y
σ_1	X	Y
σ_2	$-X$	Y
σ_3	X	$-Y$
σ_4	$-X$	$-Y$

Bestäm L^G.

4.12. Låt $L = \mathbb{Q}(X)$ och $G =< \sigma >$, där $\sigma(X) = X + 1$. Bestäm L^G.

4.13. a) Låt $L = K(X, Y)$ och $G =< \sigma_1, \sigma_2 >$, där σ_1 är identiteten och $\sigma_2(X) = Y$, $\sigma_2(Y) = X$. Bestäm L^G.

b) Låt $L = K(X_1, \ldots, X_n)$ och $G = S_n$. Definiera $\sigma(X_i) = X_{\sigma(i)}$ för $\sigma \in S_n$. Visa att $L^G = K(s_1, \ldots, s_n)$, där s_i är de elementära symmetriska polynomen av variablerna $X_1, \ldots, X_n$.

4.14. Är det sant att om $[L : K_1] \neq \infty$ och $[L : K_2] \neq \infty$, så är $[L : K_1 \cap K_2] \neq \infty$, där K_1, K_2 är delkroppar till en kropp L?

5

Normala utvidgningar

Man säger att en utvidgning $L \supseteq K$ är **normal** om varje irreducibelt polynom som har ett nollställe i L har alla sina nollställen i L (dvs L innehåller dess splittringskropp).

5.T$_1$ *En ändlig utvidgning $L \supseteq K$ är normal då och endast då L är en splittringskropp av ett polynom med koefficienter i K.*

Man säger att N är ett **normalt hölje** till $L \supseteq K$ om $N \supseteq L$ är en kroppsutvidgning sådan att $N \supseteq K$ är normal och om $N \supseteq N' \supseteq L$, där N' är en normal utvidgning av K, så är $N' = N$.

5.T$_2$ *Låt $L = K(\alpha_1, \ldots, \alpha_n)$ vara en ändlig utvidgning. Då är ett normalt hölje till $L \supseteq K$ entydigt bestämt så när som på en L-isomorfism. Mera exakt är varje normalt hölje till $L \supseteq K$ en splittringskropp över K för $f = f_1 \cdots f_n$, där f_i är minimalpolynomet för α_i över K.*

ÖVNINGAR

5.1. Vilka av följande utvidgningar är normala:

a) $L = \mathbb{Q}(\sqrt[4]{2})$, $K = \mathbb{Q}$;
b) $L = \mathbb{Q}(\sqrt[3]{2})$, $K = \mathbb{Q}$;
c) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K = \mathbb{Q}$;
d) $L = \mathbb{C}$, $K = \mathbb{R}$;
e) $L = \mathbb{Q}(\sqrt[3]{2}, i)$, $K = \mathbb{Q}$;
f) $L = \mathbb{Q}(\sqrt[4]{2})$, $k = \mathbb{Q}(\sqrt{2})$;
g) $L = \mathbb{Q}(\sqrt[4]{2}, i)$, $K = \mathbb{Q}$;
h) $L = \mathbb{Q}(X)$, $K = \mathbb{Q}(X^3)$;
i) $L = \mathbb{C}(X)$, $K = \mathbb{C}(X^3)$;
j) $L = \mathbb{Z}_3(X)$, $K = \mathbb{Z}_3(X^2)$.

5.2. Bestäm normala höljet till var och en av följande utvidgningar:

a) $L = \mathbb{Q}(\sqrt[4]{2})$, $K = \mathbb{Q}$;
b) $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, $K = \mathbb{Q}$;
c) $L = \mathbb{Q}(\epsilon), \epsilon^5 = 1, \epsilon \neq 1$, $K = \mathbb{Q}$;
d) $L = \mathbb{Q}(X)$, $K = \mathbb{Q}(X^3)$;
e) $L = \mathbb{Q}(X)$, $K = \mathbb{Q}(X^4)$;
f) $L = \mathbb{Z}_3(X)$, $K = \mathbb{Z}_3(X^4)$.

5.3. Låt $M \supseteq L \supseteq K$.

a) Låt $M \supseteq L$ och $L \supseteq K$ är normala. Är $M \supseteq K$ normal?
b) $M \supseteq K$ är normal. Är $M \supseteq L$ normal?
c) $M \supseteq K$ är normal. Är $L \supseteq K$ normal?

5.4. Låt $L \supseteq K$ är vara en normal utvidgning och $\alpha, \beta \in L$ två nollställen till ett irreducibelt polynom med koefficienter i K. Visa att det finns en automorfism $\sigma \in G(L : K)$ sådan att $\sigma(\alpha) = \beta$.

5.5. Låt $N \supseteq L \supseteq K$, där $N \supseteq K$ är ändlig och normal. Visa att $L \supseteq K$ är normal då och endast då $\sigma L = L$ för varje $\sigma \in G(N : K)$.

5.6. Låt $L \supseteq K$ vara en ändlig utvidgning och M_1, M_2 är två kroppar mellan K och L. Visa att

a) om $M_1 \supseteq K$ och $M_2 \supseteq K$ är normala, så är $M_1 M_2 \supseteq K$ normal,
b) om $M_1 \supseteq K$ är normal, så är $M_1 M_2 \supseteq M_2$ normal.

5.7. Låt $L \supseteq K$ vara en kroppsutvidgning och $\alpha, \beta \in L$. Visa att om $K(\alpha) \supseteq K$ och $K(\beta) \supseteq K$ är normala utvidgningar och $K(\alpha) \cap K(\beta) = K$, så är $[K(\alpha, \beta) : K] = [K(\alpha) : K][K(\beta) : K]$.

6

Separabla utvidgningar

Ett irreducibelt polynom $f \in K[X]$ kallas **separabelt** över K om det saknar multipla nollställen (i varje utvidgning $L \supseteq K$ – se $3.T_3$). Man säger att $\alpha \in L \supseteq K$ är ett **separabelt element** över K om dess minimalpolynom över K är separabelt. Man säger att $L \supseteq K$ är en **separabel utvidgning** om varje element i L är separabelt över K.

6.T$_1$ a) *Om char $(K) = 0$, så är varje irreducibelt polynom $f \in K[X]$ separabelt.*

b) *Om char $(K) = p$, så är ett irreducibelt polynom $f \in K[X]$ icke separabelt då och endast då $f' \equiv 0$, vilket är ekvivalent med att $f(X) = g(X^p)$, där $g \in K[X]$.*

6.T$_2$ *Varje algebraisk utvidgning av en kropp av karakteristiken 0 eller av en ändlig kropp är separabel.*

Man säger att $\gamma \in L$ är ett **primitivt element** för utvidgningen $L \supseteq K$ om $L = K(\gamma)$.

6.T$_3$ Satsen om primitiva element. *Om $L = K(\alpha_1, \ldots, \alpha_n)$, där $\alpha_1, \ldots, \alpha_n$ är algebraiska och alla utom möjligen ett element är separabla över K, så finns det ett primitivt element för $L \supseteq K$.*

ÖVNINGAR

6.1. a) Visa att $\mathbb{Z}_2(X)$ är icke-separabel över kroppen $\mathbb{Z}_2(X^2)$.

b) Konstruera för varje primtal p en icke-separabel utvidgning av en lämplig kropp av karakteristiken p.

6.2 Låt $\alpha \in L \supseteq K$, där $\text{char}\,(K) = p$. Visa att α är separabelt över K då och endast då $K(\alpha^p) = K(\alpha)$.

6.3 Visa att $K(\alpha_1, \ldots, \alpha_n) \supseteq K$ är separabel då och endast då $\alpha_1, \ldots, \alpha_n$ är separable över K.

6.4 Låt $L \supseteq K$ vara en kroppsutvidgning. Visa att alla element $\alpha \in L$ som är separabla över K bildar en delkropp L_s mellan K och L.

Anmärkning. Graden $[L_s : K]$ kallas den **separabla graden** av L över K och betecknas $[L : K]_s$ (om $[L : K] < \infty$, så betyder det att $[L : K]_s$ är en delare till $[L : K]$ och $[L : K]_s = [L : K]$ då $L \supseteq K$ är separabel).

6.5 Låt $L \supseteq K$ och $\text{char}\,(K) = p$. Visa att för varje $\alpha \in L$ existerar en exponent p^r sådan att α^{p^r} är separabelt över K (dvs. $\alpha^{p^r} \in L_s$, där L_s är definierad i övn. 6.4).

6.6 Låt $N \supseteq L \supseteq K$, där N är en normal utvidgningar av K och utvidgningen $L \supseteq K$ är ändlig. Visa att antalet olika restriktioner $\sigma|_L$, där $\sigma \in G(N : K)$ är lika med $[L : K]_s$ (se övn. 6.4).

6.7 Låt $M \supseteq L \supseteq K$. Visa att utvidgningen $M \supseteq K$ är separabel då och endast då utvidgningarna $M \supseteq L$ och $L \supseteq K$ är separabla.

6.8 Låt $M \supseteq L \supseteq K$. Visa att $[M : K]_s = [M : L]_s [L : K]_s$ (se övn. 6.4).

6.9 Bestäm ett primitivt element för $L \supseteq K$ då

a) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K = \mathbb{Q}$;
b) $L = \mathbb{Q}(\sqrt{2} - i, \sqrt{3} + i)$, $K = \mathbb{Q}$;
c) $L = \mathbb{Q}(\sqrt{2} + \sqrt{3}, \sqrt{2} + i, \sqrt{3} - i)$, $K = \mathbb{Q}$;
d) $L = \mathbb{R}(X, Y)$, $K = \mathbb{R}(X^2, Y^2)$;
e) $L = \mathbb{Q}(X, Y)$, $K = \mathbb{Q}(X + Y, XY)$;
f) $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, $K = \mathbb{Q}$.

6.10 Visa att om $L = \mathbb{Z}_2(X, Y)$, $K = \mathbb{Z}_2(X^2, Y^2)$, så är utvidgningen $L \supset K$ inte enkel dvs det finns inte $\gamma \in L$ sådant att $L = K(\gamma)$.

6.11 Visa att utvidgningen $L \supseteq K$ är enkel och algebraisk då och endast då antalet kroppar mellan K och L är ändligt.

6.12 Ge ett exempel på en ändlig utvidgning $L \supseteq K$ sådan att antalet kroppar mellan K och L är oändlig.

6.13 Låt $L \supseteq \mathbb{Q}$ vara en ändlig normal utvidgning vars grad är udda. Visa att $L \subseteq \mathbb{R}$.

7

Galois utvidgningar

Man säger att en utvidgning $L \supseteq K$ är en **Galoisutvidgning** om den är ändlig, normal och separabel.

7.T$_1$ *En ändlig utvidgning $L \supseteq K$ är en Galoisutvidgning då och endast då $[L : K] = |G(L : K)|$.*

Om $L \supseteq K$ är en kroppsutvidgning, $\mathcal{F}$ mängden av alla kroppar mellan K och L och $\mathcal{G}$ mängden av alla delgrupper till $G(L : K)$, så definierar man två funktioner:

$$f : \mathcal{G} \to \mathcal{F} \quad \text{och} \quad g : \mathcal{F} \to \mathcal{G}$$

på följande sätt:

$$f(H) = L^H = \{x \in L : \forall_{\sigma \in H} \sigma(x) = x\}$$

och

$$g(M) = G(L : M) = \{\sigma \in G(L : K) : \forall_{x \in M} \sigma(x) = x\}.$$

7.T$_2$ Galoisteorins huvudsats. *Om $L \supseteq K$ är en Galoisutvidgning så är f och g inbördes inversa antiisomorfismer mellan partiellt ordnade med hjälp av inklusion mängden $\mathcal{F}$ av alla kroppar mellan K och L och mängden $\mathcal{G}$ av alla delgrupper till $G(L : K)$ dvs $f \circ g = id_{\mathcal{F}}$, $g \circ f = id_{\mathcal{G}}$ samt $f(H_1) \supseteq f(H_2)$ om $H_1 \subseteq H_2$, och $g(M_1) \supseteq g(M_2)$ om $M_1 \subseteq M_2$.*

Ibland kallar man för Galoisteorins huvudsats både den sista satsen och följande sats:

7.T$_3$ *Låt $K \subseteq L$ vara en Galoisutvidgning och M en kropp mellan K och L.*

a) *Utvidgningen $L \supseteq M$ är en Galoisutvidgning.*

b) *Utvidgningen $M \supseteq K$ är en Galoisutvidgning då och endast då $G(L : M)$ är normal i $G(L : K)$. Om detta är fallet, så är $G(M : K) \cong G(L : K)/G(L : M)$.*

ÖVNINGAR

7.1. Är det sant att om $L \supseteq M$ och $M \supseteq K$ är Galoisutvidgningar så är $L \supseteq K$ en Galoisutvidgning?

7.2. Vilka av följande utvidgningar $L \supseteq K$ är Galoisutvidgningar?

a) $K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt[3]{2})$;
b) $K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt[4]{2})$;
c) $K = \mathbb{Q}(\sqrt{2}),\ L = \mathbb{Q}(\sqrt[4]{2})$;
d) $K = \mathbb{Q}(i),\ L = \mathbb{Q}(i, \sqrt[4]{2})$;
e) $K = \mathbb{Q}(X^2),\ L = \mathbb{Q}(X)$;
f) $K = \mathbb{Z}_p(X^2),\ L = \mathbb{Z}_p(X)$, p ett primtal;
g) $K = \mathbb{Z}_2(X^2 + X),\ L = \mathbb{Z}_2(X)$;
h) $K = \mathbb{R}(X^3),\ L = \mathbb{R}(X)$.

7.3. Bestäm alla undergrupper till Galoisgruppen $G(L : K)$ för splittringskroppen L av polynomet f samt motsvarande kroppar M mellan K och L då

a) $K = \mathbb{Q}, f(X) = (X^2 - 2)(X^2 - 5)$;
b) $K = \mathbb{Q}, f(X) = (X^4 - 1)(X^2 - 5)$;
c) $K = \mathbb{Q}, f(X) = X^5 - 1$;
d) $K = \mathbb{Q}, f(X) = X^4 + 1$;
e) $K = \mathbb{Q}(i), f(X) = X^4 - 2$;
f) $K = \mathbb{Q}, f(X) = X^3 - 5$;
g) $K = \mathbb{Q}, f(X) = X^4 + X^2 - 1$;
h) $K = \mathbb{Q}(i), f(X) = X^3 - 1$.

7.4. Visa att utvidgningen $L \supseteq K$ är en Galoisutvidgning, bestäm Galoisgruppen $G(L : K)$, alla undergrupper till den samt motsvarande delkroppar mellan K och L då

a) $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}, i)$;
b) $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2}, \epsilon), \epsilon^3 = 1, \epsilon \neq 1$;
c) $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt[4]{2}, i)$;
d) $K = \mathbb{R}(X^2 + \frac{1}{X^2}), L = \mathbb{R}(X)$;
e) $K = \mathbb{R}(X^2, Y^2), L = \mathbb{R}(X, Y)$;
f) $K = \mathbb{R}(X^2 + Y^2, XY), L = \mathbb{R}(X, Y)$.

7.5. Låt G vara automorfismgruppen av kroppen $\mathbb{Z}_3(X)$ bestående av alla automorfismer $X \to aX + b$, där $a \neq 0$ (se övn. 4.8). Bestäm alla undergrupper till G samt motsvarande kroppar mellan fix kroppen $\mathbb{Z}_3(X)^G$ för G och $\mathbb{Z}_3(X)$.

7.6. Låt $L \supseteq K$ vara en Galoisutvidgning och M en kropp mellan K och L. Visa att $[M : K] = |G(L : K)|/|G(L : M)|$.

7.7. Låt $L \supseteq K$ vara ändliga kroppar.

a) Visa att utvidgningen $L \supseteq K$ är en Galoisutvidgning.

b) Visa att Galoisgruppen $G(L : K)$ är cyklisk och genereras av automorfismen $\sigma(x) = x^{p^m}$ (**Frobeniusautomorfismen**), där $|K| = p^m$.

7.8. Låt $L \supseteq K$ vara en Galoisutvidgning och M en kropp mellan K och L. Visa att antalet olika kroppar mellan K och L som är K-isomorfa med M är $[M : K]/|G(M : K)|$.

7.9. Låt $M_1 \supseteq K$ och $M_2 \supseteq K$ vara Galoisutvidgningar och L en kropp som innehåller både M_1 och M_2. Visa att

a) $M_1M_2 \supseteq K$ är en Galoisutvidgning;
b) $G(M_1M_2 : K) \cong G(M_1 : K) \times G(M_2 : K)$ om $M_1 \cap M_2 = K$.

7.10. Konstruera en utvidgning $L \supset \mathbb{Q}$ vars Galoisgrupp är

a) C_2; e) $C_2 \times C_2$; i) D_4 (kvadratgruppen);
b) C_3; f) $C_2 \times C_4$; j) S_3;
c) C_4; g) $C_2 \times C_2 \times C_2$; k) S_4;
d) C_5; h) $C_3 \times C_3$; l) A_4.

7.11. Visa att varje cyklisk grupp är Galoisgruppen för en utvidgning $L \supseteq \mathbb{Q}$.

7.12. Är det sant att om $M \supset L \supset K$, $[M : K] < \infty$ och $|G(M : K)| = 1$, så är $|G(L : K)| = 1$?

7.13. Låt $L \supseteq K$ vara en Galoisutvidgning och M_1, M_2 två kroppar mellan K och L. Låt $G(L : M_1) = H_1$, $G(L : M_2) = H_2$. Bestäm $G(L : M_1M_2)$ och $G(L : M_1 \cap M_2)$.

7.14. Låt $L \supset K$ vara en Galoisutvidgning med en abelsk Galoisgrupp $G(L : K)$. Låt f vara minimalpolynomet för $\alpha \in L$. Visa att f har alla sina nollställen i $K(\alpha)$.

8

Lösbarhet av ekvationer

Man säger att $L \supseteq K$ är en r**-utvidgning** om det finns en kedja av kroppar

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L$$

sådan att $K_{i+1} = K_i(\alpha_i)$, där $\alpha_i^{r_i} \in K_i$ och r_i är naturliga tal för $i = 0, 1, \ldots, n-1$. Man säger att ekvationen $f(X) = 0$, $f \in K[X]$ är r**-lösbar** över K (K en kropp av karakteristiken 0) om splittringskroppen $K(f = 0)$ för f över K ligger i en r-utvidgning $L \supseteq K$.

8.T$_1$ *Om* $\mathrm{char}\,(K) = 0$, *så är ekvationen* $f(X) = 0$, $f \in K[X]$ r*-lösbar då och endast då Galoisgruppen för* f *över* K *är lösbar.*

Den **allmänna ekvationen** av n:te graden över K är

$$f(X) = X^n - s_1 X^{n-1} + s_2 X^{n-2} + \ldots + (-1)^n s_n = 0,$$

där s_i är de elementära symmetriska funktionerna av $X_1, X_2, \ldots, X_n$ (dvs $s_1 = \sum X_i$, $s_2 = \sum X_i X_j, \ldots, s_n = X_1 X_2 \ldots X_n$) och $K(X_1, X_2, \ldots, X_n)$ är kroppen av de rationella funktionerna i variablerna $X_1, X_2, \ldots, X_n$.

8.T$_2$ *Galoisgruppen över* $K(s_1, s_2, \ldots, s_n)$ *för den allmänna ekvationen* $f(X) = 0$ *av* n*:te graden är* S_n*, så att* $f(X) = 0$ *inte är* r*-lösbar då* $n \geq 5$.

ÖVNINGAR

8.1. Motivera att följande utvidgningar $L \supset \mathbb{Q}$ är r-utvidgningar:

a) $L = \mathbb{Q}(\sqrt[5]{1+\sqrt{3}})$; b) $L = \mathbb{Q}(\sqrt[3]{1-\sqrt{5}}, \sqrt[7]{\sqrt{2}+\sqrt{3}})$

8.2. Visa att följande ekvationer är r-lösbara över $\mathbb{Q}$:

a) $X^4 - 4X^2 - 21 = 0$; b) $X^6 - 2X^3 - 2 = 0$.

8.3. a) Visa Webers sats: Om $f \in \mathbb{Q}[X]$ är ett irreducibelt polynom av grad p, där p är ett primtal ≥ 5 med $p-2$ reella och 2 komplexa nollställen, så är dess Galoisgrupp S_p.

b) Visa att ekvationen $X^5 - q^2X - q = 0$, q ett primtal, inte är r-lösbar över $\mathbb{Q}$.

8.4. Ge exempel på en polynomekvation $f(X) = 0$ över $\mathbb{Q}$ av graden n $(n \geq 5)$ som inte är r-lösbar.

8.5. Visa att varje ekvation $f(X) = 0$, där $f \in K[X]$, grad $f \leq 4$ är r-lösbar (char$(K) = 0$).

8.6. Visa att ekvationen $f(X) = 0$ är r-lösbar över K då och endast då ekvationen $f(X^n) = 0$ är r-lösbar över K (n ett naturlig tal).

8.7. Låt $f(X) = X^3 + pX + q$, $p, q \in K$ och char$(K) \neq 2, 3$.

a) Visa att $(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2 = -4p^3 - 27q^2$, där x_1, x_2, x_3 är alla nollställen till f (i en splittringskropp $L \supseteq K$).

b) Visa att $K(x_1, x_2, x_3) = K(\sqrt{\Delta},\ x_1)$.

c) Visa att om f är irreducibelt i $K[X]$ så är dess Galoisgrupp isomorf med C_3 eller S_3 beroende på om $\sqrt{\Delta} \in K$ eller $\sqrt{\Delta} \notin K$,

8.8. Låt $L = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, där $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ är alla nollställen till polynomet $f(x) = x^4 + px^2 + qx + r$, där $p, q, r \in K$(char $(K) \neq 2, 3$).

a) Visa att $(\alpha_1 + \alpha_2)^2$, $(\alpha_1 + \alpha_3)^2$, $(\alpha_1 + \alpha_4)^2$ är alla nollställen till

$$r(f) = x^3 + 2px^2 + (p^2 - 4r)x - q^2.$$

Polynomet $r(f)$ kallas för **resolventen** till f.

b) Låt L_0 vara splittringskroppen i L för $r(f)$. Visa att $L = L_0(\alpha_1)$.

c) Antag att f är irreducibelt över K. Visa att

$$G(L:K) = \begin{cases} S_4 & \text{om} \quad [L_0 : K] = 6, \\ A_4 & \text{om} \quad [L_0 : K] = 3, \\ V_4 & \text{om} \quad [L_0 : K] = 1, \\ C_4 & \text{om} \quad [L_0 : K] = 2 \quad \text{och } f \text{ är reducibelt över } L_0, \\ D_4 & \text{om} \quad [L_0 : K] = 2 \quad \text{och } f \text{ är irreducibelt över } L_0. \end{cases}$$

d) I varje fall i c) ge exempel på ett polynom f över $\mathbb{Q}$ med motsvarande Galoisgrupp.

9

Geometriska konstruktioner

Låt X vara en godtycklig punktmängd i planet.

- En linje är definierad av X om den går genom två olika punkter tillhörande X.
- En cirkel är definierad av X om dess centrum tillhör X och dess radie är lika med avståndet mellan två punter tillhörande X.

Man säger att en punkt $P = (a, b)$ **kan direkt konstrueras ur** X med passare och linjal om P är skärningspunkten av två linjer eller två cirklar eller en linje med en cirkel som är definierade av X. Låt X_1 vara mängden av alla punkter i planet som kan direkt konstrueras ur $X = X_0$, X_2 mängden av alla punkter som kan direkt konstrueras ur X_1, X_3 mängden av alla punkter som kan direkt konstrueras ur X_2 osv. Man säger att en punkt $P = (a, b)$ **kan konstrueras ur** X med passare och linjal om $P \in X^\star = \bigcup_{i=0}^{\infty} X_i$ (dvs $P \in X_i$ för något $i \geq 0$).

Man definierar också **reella tal konstruerbara** ur X som sådana $r \in \mathbb{R}$ att $|r|$ = avståndet mellan två punkter konstruerbara ur X.

Ofta börjar man med två punkter i planet – säg (0,0) och (1,0) – och försöker beskriva alla punkter i planet som med hjälp av passare och linjal kan konstrueras från dessa två. Med andra ord väljer man $X = \{(0, 0), (1, 0)\}$. De tal som är konstruerbara ur $X = \{(0, 0), (1, 0)\}$ kommer att betecknas med $\mathbb{K}$. Den minsta talkropp som innehåller koordinaterna av $(0, 0)$ och $(1, 0)$ är självklart $\mathbb{Q}$.

9.T$_1$ *Låt K vara den minsta underkropp till $\mathbb{R}$ som innehåller koordinater av alla punkter tillhörande en punktmängd X i planet. En punkt $P = (a, b)$ kan konstrueras ur X med*

passare och linjal då och endast då det finns en kedja av kroppar:

$$K = K_0 \subset K_1 \subset \ldots \subset K_n = L$$

sådan att $a, b \in L$ *och* $[K_{i+1} : K_i] = 2$ *för* $i = 0, 1, \ldots, n-1$.

I praktiska sammanhang utnyttjar man den satsen då man vill visa att en punkt $P = (a, b)$ inte är konstruerbar – man visar att $[K(a, b) : K]$ inte är en potens av 2. Om man vill visa att en punkt är konstruerbar utnyttjar man ofta följande sats:

9.T$_2$ *Låt K vara den minsta underkropp till $\mathbb{R}$ som innehåller koordinater av alla punkter tillhörande en punktmängd X i planet. Om det finns en normal utvidgning $L \supseteq K$ sådan att $L \subset \mathbb{R}$, $a, b \in L$ och $[L : K]$ är en potens av 2, så är punkten $P = (a, b)$ konstruerbar ur X med passare och linjal.*

ÖVNINGAR

9.1. Låt X vara en punktmängd i planet. Visa att en punkt $P = (a, b)$ kan konstrueras ur X då och endast då dess koordinater kan konstrueras ur X.

9.2. Visa att följande geometriska konstruktioner inte är möjliga:

a) att konstruera* en kub med volymen 2 då en kub med volymen 1 är given dvs att konstruera en sträcka av längden $\sqrt[3]{2}$ då en sträcka av längden 1 är given (kubens fördubbling);

b) att konstruera vinkeln $20°$ då vinkeln $60°$ är given (vinkelns tredelning);

(c) att konstruera en kvadrat vars area är π då en cirkelskiva med arean π är given** (cirkelns kvadratur).

9.3. a) Är det möjligt att konstruera en cirkelskiva vars area är lika med summan av areor av två givna cirkelskivor?

b) Är det möjligt att konstruera en kula vars volym är lika med summan av volymer av två givna kulor?

9.4. Är det möjligt att konstruera en kvadrat vars area är lika med arean av en given triangel?

9.5. Är det möjligt att konstruera en kub vars volym är lika med volymen av en regelbunden tetraeder vars kanter är lika med 1?

*Här och i fortsättningen att konstruera" betyder att konstruera med passare och linjal".

**En cirkelskiva (eller en kula) är given om dess radie är given.

9.6. Visa i följande steg Gauss sats: En regelbunden n-hörning är konstruerbar om en sträcka av längden 1 är given då och endast då $n = 2^r,\ r \geq 2$ eller $n = 2^r p_1 p_2 \dots p_s,\ r \geq 0,\ s \geq 1$ och p_i är olika Fermatprimtal (p är ett Fermatprimtal om $p = 2^{2^t} + 1,\ t \geq 0$):

a) om $k|n$ och n-hörningen är konstruerbar, så är k-hörningen konstruerbar;

b) om $n = kl$, där k och l är relativt prima, så är n-hörningen konstruerbar då och endast då k-hörningen och l-hörningen är konstruerbara;

c) om $n = 2^r,\ r \geq 2$ så är n-hörningen konstruerbar;

d) om $n = p^2$, där p är ett udda primtal, så är n-hörningen inte konstruerbar;

e) om $n = p$, där p är ett udda primtal, så är n-hörningen konstruerbar då och endast då p är ett Fermatprimtal.

9.7. Konstruera en regelbunden n-hörning då $(0, 0)$ och $(1, 0)$ är givna om

a) $n = 5$; b) $n = 15$; c) $n = 20$.

9.8. Vilka av följande vinklar α kan konstrueras då $(0, 0)$ och $(1, 0)$ är givna:

a) $\alpha = 1°$; b) $\alpha = 3°$; c) $\alpha = 5°$.

9.9. Ge ett exempel på en vinkel α som inte kan konstrueras då $(0, 0)$ och $(1, 0)$ är given men som kan tredelas då man har denna vinkeln given.

10

APPENDIX: Några bevis

2.T$_1$ *Låt $\alpha \in L \supseteq K$ vara ett algebraiskt element över K.*

a) *Ett minimalpolynom för α över K är irreducibelt och delar varje polynom i $K[X]$ som har α som sitt nollställe.*

b) *Ett irreducibelt polynom $f \in K[X]$ sådant att $f(\alpha) = 0$ är ett minimalpolynom för α över K.*

c) *Alla minimalpolynom för α över K får man ur ett sådant polynom genom att multiplicera det med nollskilda konstanter ur K.*

Bevis. a) Låt p vara ett minimalpolynom för α över K. Om $p = p_1 p_2$, där grad$(p_1) <$ grad(p) och grad$(p_2) <$ 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.

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

c) Låt både p och p' vara minimalpolynom för α över K. Enligt a) delar de varandra, så att $p' = cp$, där c är en nollskild konstant. □

2.T$_2$ a) *Om $\alpha \in L \supseteq K$ är ett algebraiskt element över K, så kan varje element i $K(\alpha)$ skrivas entydigt på formen $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$, där $a_i \in K$ och n är graden av minimalpolynomet för α över K.*

b) *Om $\alpha \in L \supseteq K$ är ett transcendent element över K, så är $K(\alpha) \simeq K(X)$, där $K(X)$ är kroppen av de rationella funktionerna över K.*

Bevis. Betrakta ringhomomorfismen

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

där $\phi(f(X)) = f(\alpha)$. Man har

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

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 (Enligt en sats är $K[X]/(p(X))$ en kropp då och endast då $p(x)$ är irreducibelt). □

6.T$_3$ Satsen om primitiva element. *Låt K vara en oändlig kropp. Om $L = K(\gamma_1, \ldots, \gamma_n)$, där $\gamma_1, \ldots, \gamma_n$ är algebraiska och alla utom möjligen ett element är separabla över K, så finns det ett primitivt element för $L \supseteq K$.*

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 $\alpha_1 = \alpha$, $\beta_1 = \beta$. Enligt förutsättningen är alla nollställen till både f och g olika (f och g är separabla polynom). 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

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

gäller för ett ändligt antal $x \in K$ (mindre än 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. Alltså 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 $\beta \in K(\theta)$. $\square$

11

Ledningar och svar

1.1 Endast d) är en kropp.

1.3 T.ex. $\mathbb{Z}_p(X)$, där p är ett primtal.

1.6 a) $a + b\sqrt{2},\ a, b \in \mathbb{Q}$;
b) $a + bi,\ a, b \in \mathbb{Q}$;
c) $a + b\sqrt{2} + ci + di\sqrt{2},\ a, b, c, d \in \mathbb{Q}$;
d) $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6},\ a, b, c, d \in \mathbb{Q}$.

1.8 a) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$;
b) $\mathbb{Q}(i, \sqrt{2}) = \{a + bi + c\sqrt{2} + di\sqrt{2} : a, b, c, d \in \mathbb{Q}\}$;
c) $\mathbb{Q}(i, \sqrt{5}) = \{a + bi + c\sqrt{5} + di\sqrt{5} : a, b, c, d \in \mathbb{Q}\}$;
d) $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$.

1.9 c) Välj $K = \mathbb{Z}_3$ i a).

1.10 a) Polynomet $X^2 - X + 1$ måste vara irreducibelt över K.
b) Välj $K = \mathbb{Z}_2$ i a).

1.11 2.

* * *

2.1 a), b), c) är algebraiska; d), e), f) är transcendenta.

2.2 a) $X^6 - 2X^3 - 2$;
b) $X^6 - 6X^4 - 4X^3 + 12X^2 - 24X - 4$;
c) $X^4 + X^3 + X^2 + X + 1$;
d) $X^2 - 2$;
e) $X^3 - 2$;
f) $X^{p-1} + X^{p-2} + \ldots + X + 1$.

2.3 a) 4; en bas: $1, i, \sqrt{2}, i\sqrt{2}$;
b) 4; en bas $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$;
c) 6; en bas $1, \sqrt{2}, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt[6]{2}, \sqrt[6]{32}$;
d) 3; en bas: $1, \sqrt[3]{2}, \sqrt[3]{4}$;
e) 2; en bas: $1, X$;
f) 8; en bas: $1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}$;
g) 3; en bas: $1, \alpha, \alpha^2$, där $\alpha = \sqrt[3]{1+\sqrt{3}}$;
h) 4; en bas: $1, \alpha, \alpha^2, \alpha^3$;
i) 3; en bas: $1, \alpha, \alpha^2$;
j) 4; en bas: $1, X, X^2, X^3$.

2.4 Utnyttja $2.T_5$.

2.5 Utnyttja 2.4.

2.6 a) $x = \frac{1}{2}\sqrt[3]{4}$; b) $x = \frac{1}{3}(1 - \sqrt[3]{2} + \sqrt[3]{4})$; c) $x = -1 + \sqrt[3]{4}$.

2.7 a) $x = -\sqrt{2} + \sqrt{3}$; b) $x = \frac{1}{2} + \frac{1}{4}\sqrt{2} - \frac{1}{4}\sqrt{6}$; c) $x = \frac{1}{2}(-5 + 4\sqrt{2} + 3\sqrt{3} - 2\sqrt{6})$.

2.8 a) $x = 1 + \alpha^3$; b) $x = \alpha + \alpha^2$; c) $x = 1$; d) $x = \alpha + \alpha^2$.

2.9 a) Visa att $p(Y) - \frac{p(X)}{q(X)}q(Y)$ är minimalpolynomet för X över $K(\alpha)$.
b) Utnyttja den enkla delen av a): $[K(X) : K(\alpha)] \leq n$ och $2.T_3$.

2.10 a) och b) – utnyttja $2.T_3$.
c) Allmänt är $[M_1M_2 : K] \leq [M_1 : K][M_2 : K]$.

2.11 Tänk på $[K(\alpha) : K(\alpha^2)]$ och utnyttja $2.T_3$. På andra delen är svaret nej (konstruera ett motexempel!)

2.12 Utnyttja $2.T_2$ a) och $2.T_3$ (man kan också utnyttja 2.10 b) och $2.T_2$ a)).

2.13 Betrakta minimalpolynomet för ett element $\alpha \in L \setminus \mathbb{R}$ (om ett sådant finns) och utnyttja algebrans fundamentalsats.

2.14 Nej. Betrakta $\mathbb{Q}(\alpha) \supset \mathbb{Q}$, där $\alpha^4 + \alpha + 1 = 0$.

* * *

3.1 a) 4; $1, \sqrt{2}, \sqrt{5}, \sqrt{10}$;
b) 6; $1, \sqrt[3]{2}, \sqrt[3]{4}, \epsilon, \epsilon\sqrt[3]{2}, \epsilon\sqrt[3]{4}$, $\epsilon^3 = 1$, $\epsilon \neq 1$;
c) 8; $1, i, \sqrt{2}, i\sqrt{2}, \sqrt[4]{2}, i\sqrt[4]{2}, \sqrt[4]{8}, i\sqrt[4]{8}$;
d) 8; $1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3$, där $\alpha = \sqrt{\frac{1}{2}(-1+\sqrt{5})}$;
e) $4, 1, \alpha, \alpha^2, \alpha^3$, där $\alpha = e^{\frac{\pi i}{4}}$;
f) 4; $1, \alpha, \alpha^2, \alpha^3$, där $\alpha = \sqrt[4]{2}$;
g) 4; $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$;
h) $p-1$; $1, \alpha, \ldots, \alpha^{p-2}$, där $\alpha = e^{\frac{2\pi i}{p}}$.

3.2 a) ja; b) ja; c) nej.

3.3 Utnyttja $3.T_4$ och $2.T_3$.

3.4 Betrakta kroppen $\mathbb{Z}_p[X]/(f(X))$ och utnyttja $3.T_4$ och 3.3.

3.5 Bevisa första formeln genom att utnyttja 3.4 (det är mycket lätt!). Andra formeln är ett specialfall av följande allmänna sats: Om $f : \mathbb{N} \to \mathbb{C}$ och $g : \mathbb{N} \to \mathbb{C}$ är två godtyckliga funktioner och

$$f(n) = \sum_{d|n} g(d), \text{ så är } g(n) = \sum_{d|n} f(d)\mu(\frac{n}{d}).$$

Den sista implikationen kallas Möbius inversionsformel och bevisas ganska enkelt med hjälp av likheten $\sum_{d|n} \mu(d) = 0$ om $n \neq 1$. Använd inversionsformlen då $f(n) = p^n$ och $g(n) = nv_p(n)$.

3.6 Beräkna antalet element i en kropp med p^n element som genererar denna över $\mathbb{Z}_p$. Bestäm därefter antalet irreducibla polynom som dessa element uppfyller. Utnyttja 3.4.

3.7 a) Det följer t.ex. från det att en abelsk grupp är en produkt av cykliska grupper.

b) Enligt a) är gruppen L^* cyklisk.

* * *

4.1 a) $G = \{\sigma_0, \sigma_1\}$, $\sigma_0 = id.$, $\sigma_1(\sqrt{2}) = -\sqrt{2}$;
b) $G = \{\sigma_0\}$, $\sigma_0 = id.$;
c) $G = \{\sigma_0, \sigma_1\}$, $\sigma_0 = id.$, $\sigma_1(\sqrt[4]{2}) = -\sqrt[4]{2}$;
d)

G	$\sqrt{2}$	$\sqrt{3}$
σ_0	$\sqrt{2}$	$\sqrt{3}$
σ_1	$-\sqrt{2}$	$\sqrt{3}$
σ_2	$\sqrt{2}$	$-\sqrt{3}$
σ_3	$-\sqrt{2}$	$-\sqrt{3}$

e) $G = \{\sigma_0\}$, $\sigma_0 = id.$;
f) $G = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$. $\sigma_i(X) = iX$.

4.4 Visa att $\sigma(x) > 0$ om $x > 0$ (utnyttja att $x = (\sqrt{x})^2$). Antag att t.ex. $\sigma(x) > x$ och välj $r \in \mathbb{Q}$ så att $\sigma(x) > r > x$. Utnyttja därefter 4.3.

4.5 Betrakta $L^{G(L:K)}$.

4.6 Utnyttja 2.9.

4.7 $|G| = 6$, $L^G = \mathbb{Z}_2(\alpha)$, där $\alpha = \frac{(X^3+X+1)(X^3+X^2+1)}{(X^2+X)^2}$.

4.8 $|G| = 6$, $L^G = \mathbb{Z}_3(X^6 + X^4 + X^2)$.

4.9 a) $L^G = \mathbb{R}(X^2, Y)$.

4.10 a) $L^G = \mathbb{R}(X^2, XY)$.

4.11 $L^G = \mathbb{Q}(X^2, Y^2)$.

4.12 $L^G = \mathbb{Q}$. Utnyttja $4.T_2$ och 2.9.

4.13 a) $L^G = K(X + Y, XY)$.

4.14 Nej. Konstruera ett motexempel genom att välja $L = K(X)$.

* * *

5.1 a), b), e) och h) är inte normala.

5.2 a) $\mathbb{Q}(\sqrt[4]{2}, i)$;
b) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \epsilon),\ \epsilon^3 = 1,\ \epsilon \neq 1$;
c) L;
d) $\mathbb{Q}(X, \epsilon),\ \epsilon^3 = 1,\ \epsilon \neq 1$;
e) $\mathbb{Q}(X, i),\ i^2 = -1$;
f) $L(\alpha), \alpha^2 + 1 = 0$.

5.3 a) ej nödvändigt! Ge ett exempel!
b) ja
c) se a) ovan.

5.4 Utnyttja $3.T_1$ b).

5.5 Utnyttja 5.4.

5.6 a), b) Utnyttja $5.T_1$.

5.7 Visa att minimalpolynomet för β över K är irreducibelt över $K(\alpha)$.

* * *

6.1 b) T. ex. $L \supset K$, där $L = \mathbb{Z}_p(X),\ K = \mathbb{Z}_p(X^p)$.

6.2 Betrakta $K \subseteq K(\alpha^p) \subseteq K(\alpha)$. Utnyttja $6.T_1$ b).

6.3 Utnyttja 6.2.

6.4 Utnyttja 6.3.

6.5 Utnyttja $6.T_1$ b).

6.6 Antag först att $L = K(\gamma)$.

6.7 Utnyttja 6.3.

6.8 Utnyttja 6.6.

6.9 a) T. ex. $\sqrt{2}+\sqrt{3}$; d) T. ex. $X+Y$;
b) T. ex. $\sqrt{2}+\sqrt{3}+i$; e) T. ex. X;
c) T. ex. $\sqrt{2}+\sqrt{3}+i$; f) T. ex. $\sqrt{2}+\sqrt[3]{2}$.

6.10 Visa att om γ existerar så är $\gamma^2 \in K$. Beräkna $[L:K]$.

6.11 Om $L = K(\gamma)$ och M ligger mellan K och L så får man M genom att adjungera till K alla koefficienter av minimalpolynomet för γ över M (visa det!). Detta polynom är en delare till minimalpolynomet för γ över K. Omvänt. Visa att L är ändligt genererad och algebraisk över K. Använd induktion och reducera till $L = K(\alpha, \beta)$. Betrakta separat K ändlig och K oändlig.

6.12 Betrakta $K \subset L$ ur 6.10 (t. ex. $\mathbb{Z}_p(X^2, Y^2, X+cY)$, där $c \in K$).

6.13 Utnyttja satsen om primitiva element.

* * *

7.1 Nej

7.2 c), d), e), f) om $p \neq 2$, g) är Galoisutvidgningar.

7.3 a) $L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$; $[L:\mathbb{Q}] = |G(L:\mathbb{Q})| = 4$, $G = G(L:\mathbb{Q}) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$, där

G	$\sqrt{2}$	$\sqrt{5}$	O
σ_0	$\sqrt{2}$	$\sqrt{5}$	1
σ_1	$-\sqrt{2}$	$\sqrt{5}$	2
σ_2	$\sqrt{2}$	$-\sqrt{5}$	2
σ_3	$-\sqrt{2}$	$-\sqrt{5}$	2

Delgrupper till G**:** $I = \{\sigma_0\}$,
$H_1 = \{\sigma_0, \sigma_1\}$, $H_2 = \{\sigma_0, \sigma_2\}$, $H_3 = \{\sigma_0, \sigma_3\}$.
Kroppar mellan $\mathbb{Q}$ **och** L**:** $L^G = \mathbb{Q}$, $L^I = L$,
$L^{H_1} = \mathbb{Q}(\sqrt{5})$, $L^{H_2} = \mathbb{Q}(\sqrt{2})$, $L^{H_3} = \mathbb{Q}(\sqrt{10})$.

b) $L = \mathbb{Q}(i, \sqrt{5})$. Jfr a).

c) $L = \mathbb{Q}(\epsilon)$, $\epsilon = e^{\frac{2\pi i}{5}}$, $[L:\mathbb{Q}] = |G(L:\mathbb{Q})| = 4$, $G = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$, där

G	ϵ	O
σ_0	ϵ	1
σ_1	ϵ^2	4
σ_2	ϵ^3	4
σ_3	ϵ^4	2

Delgrupper till G**:** $G, I = \{\sigma_0\}$, $H = \{\sigma_0, \sigma_3\}$.
Kroppar mellan $\mathbb{Q}$ **och** L**:** $L^G = \mathbb{Q}$, $L^I = L$,
$L^H = \mathbb{Q}(\epsilon + \epsilon^4) = \mathbb{Q}(\cos\frac{2\pi}{5}) = \mathbb{Q}(\sqrt{5})$.

d) $L = \mathbb{Q}(i, \sqrt{2})$. Jfr a).

e) $L = K(\sqrt[4]{2})$; $[L:K] = |G(L:K)| = 4$, $G = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$, där

G	$\sqrt[4]{2}$	O
σ_0	$\sqrt[4]{2}$	1
σ_1	$-\sqrt[4]{2}$	2
σ_2	$\sqrt[4]{2}$	4
σ_3	$-i\sqrt[4]{2}$	4

Delgrupper till G**;** $G, I = \{\sigma_0\}$, $H = \{\sigma_0, \sigma_1\}$.
Kroppar mellan K **och** L**:** $L^G = K : L^I = L$,
$L^H = K(\sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$.

f) $L = \mathbb{Q}(\sqrt[3]{5}, \epsilon), \epsilon^3 = 1, \epsilon \neq 1; [L : \mathbb{Q}] = |G(L : \mathbb{Q})| = 6, G = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$, där

G	$\sqrt[3]{5}$	ϵ	O
σ_0	$\sqrt[3]{5}$	ϵ	1
σ_1	$\sqrt[3]{5}$	ϵ^2	2
σ_2	$\epsilon\sqrt[3]{5}$	ϵ	3
σ_3	$\epsilon\sqrt[3]{5}$	ϵ^2	2
σ_4	$\epsilon^2\sqrt[3]{5}$	ϵ	3
σ_5	$\epsilon^2\sqrt[3]{5}$	ϵ^2	2

Delgrupper till G**:** $G, I = \{\sigma_0\}$, $H_1 = \{\sigma_0, \sigma_1\}$, $H_2 = \{\sigma_0, \sigma_3\}$, $H_3 = \{\sigma_0, \sigma_5\}$, $H = \{\sigma_0, \sigma_2, \sigma_4\}$.
Kroppar mellan $\mathbb{Q}$ **och** L**:** $L^G = \mathbb{Q}$, $L^I = L, L^{H_1} = \mathbb{Q}(\sqrt[3]{5})$, $L^{H_2} = \mathbb{Q}(\epsilon^2\sqrt[3]{5})$, $L^{H_3} = \mathbb{Q}(\epsilon\sqrt[3]{5})$, $L^H = \mathbb{Q}(\epsilon)$.

g) $L = \mathbb{Q}(\alpha, i)$, $\alpha = \sqrt{\frac{1}{2}(\sqrt{5} - 1)}; [L : \mathbb{Q}] = |G(L : \mathbb{Q})| = 8$. Jfr. 7.4 c).

h) $L = K(\epsilon)$, $\epsilon^3 = 1$, $\epsilon \neq 1; [L : K] = |G(L : K)| = 2$, $G = \{\sigma_0, \sigma_1\}$, där $\sigma_0 = id.$, $\sigma_1(\epsilon) = \epsilon^2$. Endast triviala delgrupper och mellankroppar.

7.4 a) Jfr. 7.3 a)
b) Jfr. 7.3 f)
c) $[L : \mathbb{Q}] = |G(L : \mathbb{Q})| = 8$ ty L är splittringskroppen för $X^4 - 2$ över $\mathbb{Q}$. $G = G(L : \mathbb{Q}) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7\}$, där

G	$\sqrt[4]{2}$	i	O
σ_0	$\sqrt[4]{2}$	i	1
σ_1	$-\sqrt[4]{2}$	i	2
σ_2	$i\sqrt[4]{2}$	i	4
σ_3	$-i\sqrt[4]{2}$	i	4
σ_4	$\sqrt[4]{2}$	$-i$	2
σ_5	$-\sqrt[4]{2}$	$-i$	2
σ_6	$i\sqrt[4]{2}$	$-i$	2
σ_7	$-i\sqrt[4]{2}$	$-i$	2

Delgrupper till G**:** $G, I = \{\sigma_0\}, H_1 = \{\sigma_0, \sigma_1\}$, $H_2 = \{\sigma_0, \sigma_4\}, H_3 = \{\sigma_0, \sigma_5\}, H_4 = \{\sigma_0, \sigma_6\}$, $H_5 = \{\sigma_0, \sigma_7\}, G_1 = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ $G_2 = \{\sigma_0, \sigma_1, \sigma_4, \sigma_5\}, G_3 = \{\sigma_0, \sigma_1, \sigma_6, \sigma_7\}$.
Kroppar mellan $\mathbb{Q}$ **och** L**:** $L^G = \mathbb{Q}, L^I = L$; $L^{H_1} = \mathbb{Q}(\sqrt{2}, i), L^{H_2} = \mathbb{Q}(\sqrt[4]{2}), L^{H_3} = \mathbb{Q}(i\sqrt[4]{2})$, $L^{H_4} = \mathbb{Q}((1+i)\sqrt[4]{2}), L^{H_5} = \mathbb{Q}((1-i)\sqrt[4]{2})$, $L^{G_1} = \mathbb{Q}(i), L^{G_2} = \mathbb{Q}(\sqrt{2}), L^{G_3} = \mathbb{Q}(i\sqrt{2})$.

d) $[L : K)| = 4$ ty K är fixkroppen för gruppen $G = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ av K-automorfismer av L, där:

G	X	O
σ_0	X	1
σ_1	$-X$	2
σ_2	$1/X$	2
σ_3	$-1/X$	2

Delgrupper till G**:** $G, I = \{\sigma_1\}, H_1 = \{\sigma_0, \sigma_1\}$ $H_2 = \{\sigma_0, \sigma_2\}$, $H_3 = \{\sigma_0, \sigma_3\}$.
Kroppar mellan K **och** L**:** $L^G = K, L^I = L$, $L^{H_1} = \mathbb{R}(X^2)$, $L^{H_2} = \mathbb{R}(X + \frac{1}{X}), L^{H_3} = \mathbb{R}(X - \frac{1}{X})$.

e) $[L : K] = |G(L : K)| = 4$ ty K är fixkroppen för gruppen $G = G(L : K) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ av K-automorfismer L, där

G	X	Y	O
σ_0	X	Y	1
σ_1	$-X$	Y	2
σ_2	X	$-Y$	2
σ_3	$-X$	$-Y$	2

Delgrupper till G**:** $G, I = \{\sigma_0\}$, $H_1 = \{\sigma_0, \sigma_1\}$, $H_2 = \{\sigma_0, \sigma_2\}$, $H_3 = \{\sigma_0, \sigma_3\}$.
Kroppar mellan K **och** L**:** $L^G = K, L^I = L$, $L^{H_1} = \mathbb{R}(X^2, Y)$, $L^{H_2} = \mathbb{R}(X, Y^2)$, $L^{H_3} = \mathbb{R}(X^2, XY)$.

f) $[L : K] = |G(L : K)| = 4$ ty K är fixkroppen för gruppen $G = G(L : K) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ av K-automorfismer av L, där

G	X	Y	O
σ_0	X	Y	1
σ_1	$-X$	$-Y$	2
σ_2	Y	X	2
σ_3	$-Y$	$-X$	2

Delgrupper till G**:** $G, I = \{\sigma_0\}$, $H_1 = \{\sigma_0, \sigma_1\}$, $H_2 = \{\sigma_0, \sigma_2\}$, $H_3 = \{\sigma_0, \sigma_3\}$.
Kroppar mellan K **och** L**:** $L^G = K$, $L^I = L$, $L^{H_1} = \mathbb{R}(X^2, XY)$, $L^{H_2} = \mathbb{R}(X + Y, XY)$, $L^{H_3} = \mathbb{R}(X - Y, XY)$.

7.5 $L = \mathbb{Z}_3(X)$, $L^G = \mathbb{Z}_3(X^6 + X^4 + X^2)$, $[L : L^G] = 6$.

G	X	O
σ_0	X	1
σ_1	$X + 1$	3
σ_2	$X + 2$	3
σ_3	$2X$	2
σ_4	$2X + 1$	2
σ_5	$2X + 2$	2

Delgrupper till G**:** $G, I = \{\sigma_0\}, H_1 = \{\sigma_0, \sigma_3\}$, $H_2 = \{\sigma_0, \sigma_4\}, H_3 = \{\sigma_0, \sigma_5\}, H = \{\sigma_0, \sigma_1, \sigma_2\}$.
Kroppar mellan L^G **och** L**:** $L^G, L^I = L, L^{H_1} = \mathbb{Z}_3(X^2)$, $L^{H_2} = \mathbb{Z}_3(X^2 - X), L^{H_3} = \mathbb{Z}_3(X^2 + X), L^H = \mathbb{Z}_3(X^3 - X)$.

7.6 $L \supseteq M$ och $L \supseteq K$ är Galoisutvidgningar. Utnyttja $7.T_1$.

7.7 a) Utnyttja t.ex. $3.T_4$ och $6.T_2$.
b) Utnyttja 1.12.

7.8 Betrakta $H = \{\sigma \in G(L : K) : \sigma M = M\}$. Visa att det är en delgrupp till $G(L : K)$. Beräkna index av H i $G(L : K)$ genom att betrakta homomorfismen $\varphi : H \to G(M : K)$, där $\varphi(\sigma) = \sigma|_M$. Utnyttja $7.T_1$ (eller 7.6).

7.9 a) Utnyttja 5.6 och 6.7.

b) Betrakta homomorfismen $\varphi : G(M_1M_2 : K) \to G(M_1 : K) \times G(M_2 : K)$, där $\varphi(\sigma) = (\sigma|_{M_1}, \sigma|_{M_2})$. Visa att Ker $\varphi = \{e\}$. Beräkna därefter ordningarna $G(M_1M_2 : K)$ och $G(M_1 : K) \times G(M_2 : K)$ genom att utnyttja $7.T_1$ och 5.7.

7.10 a) T.ex. $\mathbb{Q}(i)$;

b) T.ex. $\mathbb{Q}(\epsilon + \frac{1}{\epsilon})$, där $\epsilon = e^{\frac{2\pi i}{7}}$;

c) T.ex. 7.3 c);

d) T.ex. $\mathbb{Q}(\epsilon + \frac{1}{\epsilon})$, där $\epsilon = e^{\frac{2\pi i}{11}}$;

e) T.ex. 7.3 a);

f) $\mathbb{Q}(i, \epsilon)$ där $\epsilon = e^{\frac{2\pi i}{5}}$;

g) T.ex. $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$;

h) Konstruera som i f) (utnyttja b));

i) T.ex. 7.4 c);

j) T.ex. 7.3 f);

k) T.ex. splittringskroppen för $X^4 - 2X - 2$ över $\mathbb{Q}$;

l) T.ex. splittringskropparna för $X^4 + X + 3/4$ över $\mathbb{Q}$.

7.11 Utnyttja Dirichlets sats: För varje naturligt tal n finns det ett naturligt tal k sådant att $nk+1$ är ett primtal.

7.12 Nej. Ge ett motexempel!

7.13 $G(L : M_1M_2) = H_1 \cap H_2$; $G(L : M_1 \cap M_2) =$ den minsta undergrupp till $G(L : K)$ som innehåller både H_1 och H_2.

7.14 $K(\alpha) \supseteq K$ är en Galoisutvidgning.

* * *

8.2 Visa utan att lösa ekvationerna!

8.3 a) se kursboken.

8.4 T.ex. $X^{n-5}f(X)$, där $n \geq 5$ och f är polynomet ur 8.3 b).

8.5 Diskutera alla möjliga Galoisgrupper och utnyttja $8.T_1$. Alternativt visa hur man löser sådana ekvationer.

8.6 Betrakta splittringskroparna för $f(X)$ och $f(X^n)$.

8.7 a) $p = x_1x_2 + x_2x_3 + x_3x_1, \quad q = -x_1x_2x_3$.

b) Polynomet $g(X) = (X^3 + pX + q)/(X - x_1)$ har sina koefficienter i $K(\sqrt{\Delta}, x_1)$. Utnyttja det att både $g(x_1)$ och $\sqrt{\Delta}$ tillhör $K(\sqrt{\Delta}, x_1)$.

8.8 b) Bestäm koefficienten a i faktoruppdelningen i $L[x]$: $f(x) = (x^2 + ax + b)(x^2 + cx + d)$.

* * *

9.2 a) $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

b) Man måste kunna konstruera punkten $(\cos 20°, \sin 20°)$. Ur $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$ får man att $\cos 20°$ uppfyller ekvationen $4x^3 - 3x = \frac{1}{2}$. Visa att $[\mathbb{Q}(\cos 20°) : \mathbb{Q}] = 3$.

c) Man måste kunna konstruera punkten $(0, \sqrt{\pi})$. Motivera att $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$.

9.3 a) Ja. Radien av den nya cirkeln är $\sqrt{r_1^2 + r_2^2}$, där r_1 och r_2 är radierna av de två givna cirkelskivorna.

b) Ibland. Radien av den nya kulan uppfyller ekvationen $X^3 - r_1^3 - r_2^3 = 0$, där r_1 och r_2 är radierna av de två givna kulorna. Om t.ex. $r_1 = r_2 = 1$ är konstruktionen inte möjlig, men om $r_1 = 1, r_2 = \sqrt[3]{7}$ så är den möjlig.

9.4 Ja. Kvadratens sida $x = \sqrt{\frac{1}{2}ah}$, där a är triangelns bas och h motsvarande höljd – både a och h är givna.

9.5 Nej. Kubens sida $x = \frac{1}{\sqrt[6]{62}}$.

9.6 b) Det finns heltal a och b sådana att $1 = ak + bl$ dvs $\frac{1}{kl} = a\frac{1}{l} + b\frac{1}{k}$. Alltså är vinkeln $\frac{2\pi}{kl}$ konstruerbar om vinklarna $\frac{2\pi}{k}$ och $\frac{2\pi}{1}$ är konstruerbara. Resten följer ur a).

d) Om vinkeln $\frac{2\pi}{p^2}$ är konstruerbar, så är punkten $(\cos\frac{2\pi}{p^2}, \sin\frac{2\pi}{p^2})$ konstruerbar. Alltså är $[L : \mathbb{Q}]$ en potens av 2, där $L = \mathbb{Q}(\cos\frac{2\pi}{p^2}, \sin\frac{2\pi}{p^2}, i) \supseteq \mathbb{Q}(\epsilon), \epsilon = \cos\frac{2\pi}{p^2} + i\sin\frac{2\pi}{p^2}$. Men $[\mathbb{Q}(\epsilon) : \mathbb{Q}] = p(p-1)$ är inte en potens av 2.

e) Vinkeln $\frac{2\pi}{p}$ är konstruerbar då och endast då punkten $P = (\cos\frac{2\pi}{p}, \sin\frac{2\pi}{p})$ är konstruerbar. Punkten P är konstruerbar då och endast då $[L : \mathbb{Q}]$ är en potens av 2, där $L = \mathbb{Q}(\cos\frac{2\pi}{p}, \sin\frac{2\pi}{p}, i) = \mathbb{Q}(\epsilon, i), \epsilon = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ (utnyttja $9.T_1$ och $9.T_2$ samt observera att $\epsilon^{-1} = \cos\frac{2\pi}{p} - i\sin\frac{2\pi}{p}$). Men $[\mathbb{Q}(\epsilon) : \mathbb{Q}] = p - 1$ dvs P är konstruerbar då och endast då $p = 2^T + 1$. Om nu $T = 2^t u$, där u är ett udda tal, så är $2^T + 1$ ett sammansatt tal då $u > 1$. Alltså är $T = 2^t$.

9.7 a) $\cos 72^\circ = \frac{\sqrt{5}-1}{4}$; b) och c): Utnyttja a) och 9.6 b).

9.8 a) $1^\circ = \frac{2\pi}{360}$ kan inte konstrueras enligt 9.6, ty $360 = 2^3 \cdot 3^2 \cdot 5$;
b) $3^\circ = \frac{2\pi}{120}$ kan konstrueras enligt 9.6, ty $120 = 2^3 \cdot 3 \cdot 5$;
c) $5^\circ = \frac{2\pi}{72}$ kan inte konstrueras enligt 9.6, ty $72 = 2^3 \cdot 3^2$.

9.9 T.ex. $\alpha = \frac{2\pi}{7}$. Utnyttja 9.6 och likheten $\frac{\alpha}{3} = 2(\frac{\pi}{3} - \alpha)$.