

Tentamenlösningar i Galoisteori, MAN 630

Varje uppgift ger 3 poäng. För Godkänd krävs minst 12 poäng, varav minst 7 på problemdelen 1—5 (bonuspoäng tillgodoräknas här).

1. Låt $L = \mathbb{Q}(\sqrt[6]{5})$.

- (a) Polynomet $X^6 - 5$ är irreducibelt enligt Eisensteinskriteriet med $p = 5$, så det är ett minimalpolynom för $\alpha = \sqrt[6]{5}$ med $L = \mathbb{Q}(\alpha)$ och $[L : \mathbb{Q}] = 6$. En bas för $L \supset \mathbb{Q}$ ges av $\{1, \alpha, \alpha^2, \dots, \alpha^5\}$.
- (b) De andra nollställen till $X^6 - 5$ i en splittringskropp är $j\alpha, j^2\alpha, -\alpha, -j\alpha, -j^2\alpha$, med $j \neq 1, j^3 = 1$ varav bara $-\alpha$ tillhör L ty $L \subset \mathbb{R}$ och de andra rötterna inte är reella. Därför är $L : \mathbb{Q}$ ingen normalutvidgning, och Galoisgruppen $G = \text{Gal}(L : \mathbb{Q}) = \{1, \sigma\} \simeq \mathbb{Z}/2\mathbb{Z}$ där $\sigma(\alpha) = -\alpha$.
- (c) *fixkroppen* $L^G \subset L$: Vi ser att $\sigma(\alpha^2) = \alpha^2$ så $\mathbb{Q}(\alpha^2) \subset L^G$. Då ger $[L : \mathbb{Q}(\alpha^2)] \leq 2 = [L : L^G]$ (ty α är nollställe till $X^2 - \alpha^2$) att $\mathbb{Q}(\alpha^2) = L^G$.
- (d) *det normala höljet* N till $L : \mathbb{Q}$, *and dess grad* : N är splittringskroppen till $X^6 - 5$. Alltså är $N = \mathbb{Q}(\alpha, j)$ av grad $6 \cdot 2 = 12$ över $\mathbb{Q}$.
- (e) *Kroppen* L *innehåller* $\sqrt[6]{5}$ *men inte alla andra nollställen till polynomet* $X^6 - 5$. *Medför det att* L *inte är normal över sig själv? Varför?*

Nej, polynomet är inte irreducibelt över L , ty den har α som nollställe. Minimalpolynomet för α är bara $X - \alpha$. Varje kropp är normal över sig själv!

2. Låt $L = \mathbb{F}_2(\alpha)$, där $\mathbb{F}_2$ är en kropp med två element och α är ett nollställe till polynomet $X^4 + X^3 + 1 \in \mathbb{F}_2[X]$. Motivera att Galoisgruppen $G(L, \mathbb{F}_2)$ innehåller en delgrupp H med två element och bestäm $\beta \in L$ så att fixkroppen $L^H = \mathbb{F}_2(\beta)$.

Vi kollar först att polynomet är irreducibelt över $\mathbb{F}_2$. Det har inga linjära faktorer ty 0 och $1 \in \mathbb{F}_2$ är inte nollställe. Det har inte heller några kvadratiske faktorer ty det enda irreducibla kvadratiske polynomet över $\mathbb{F}_2$ är $X^2 + X + 1$ och det i kvadrat är inte lika med $X^4 + X^3 + 1$. (De andra kvadratiske polynom: $X^2, X^2 + 1, X^2 + X$ är reducibla). Så $X^4 + X^3 + 1$ är irreducibelt och utvidgningen har grad 4. Alla ändliga utvidgningar av ändliga kroppar är normala. (Dessutom är Galoisgruppen cyklisk, genererad av Frobenius-elementet. I vårt fall är L splittringskropp för $X^{2^4} - X$ över $\mathbb{F}_2$, med $2^4 = 16$ element.)

Galoisgruppen har 4 element och de enda grupper med 4 element är abelska och har en delgrupp med 2 element. Så L har en delutvidgning $N = L^H$ av index 2.

Lägg märke till att $(X^4 + X^3 + 1)^2 = (X^4)^2 + (X^3)^2 + (1)^2 = (X^2)^4 + (X^2)^3 + 1$ så att kvadraten till ett nollställe är ett nollställe (eller använd Frobeniusautomorfin) för att inse att α^2, α^4 och α^8 är de andra nollställen till polynomet med $h(\alpha) = \alpha^4$ för det icke-triviala element $h \in H$. Så fixkroppen under $H = \{1, h\}$ innehåller $\mathbb{F}_2(\alpha + \alpha^4)$. Med $\beta = \alpha + \alpha^4 = \alpha^3 + \alpha + 1$ har vi $\mathbb{F}_2(\beta) = \mathbb{F}_2(\alpha^3 + \alpha)$ och β är ett nollställe till det enda irreducibla kvadratiske polynomet över $\mathbb{F}_2$ (kolla att $\beta^2 + \beta + 1 = 0$) så $\mathbb{F}_2(\beta) = \mathbb{F}_2(\alpha^3 + \alpha) = L^H$.

3. Ge exempel på följande :

- (a) *En icke-normal kroppsutvidgning*: $\mathbb{Q}(\sqrt[6]{5})$, se uppgift 1, eller $\mathbb{Q}(\sqrt[3]{7})$ som i uppgift 8. (se exempel i kursen, kapitel om normala utvidgningar)
- (b) *En icke-separabel kroppsutvidgning*: Se Stewart s.84, eller ta specialfallet $p = 2$, där irreducibilitet är lättare att bevisa.

- (c) Fem primtal p sådana att en regelbunden p -hörning kan konstrueras med passare och linjal. $p = 2, 3, 5, 17, 257$ se Stewart, sats 17.11 (Gauss). Om man inte tycker om 2-hörningar kan man fortsätta med $2^{2^4} + 1 = 65537$.

4. *Konstruera en Galoisutvidgning $K \supset \mathbb{R}(X)$ vars Galoisgrupp har 4 element.*

Kroppen $\mathbb{C}[\sqrt{X}]$ passar. Den är splittringskropp till $(T^2 + 1)(T^2 - X)$ över $\mathbb{R}(X)$. Utvidgningen har Galoisgrupp isomorf med $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Kroppen $\mathbb{R}[\sqrt{X}, \sqrt{X+1}]$, splittringskropp till $(T^2 - X)(T^2 - X - 1)$ passar också.

5. *Ge ett exempel på en kropp $K \supset \mathbb{Q}$ med exakt 5 äkta delutvidgningar.*

Här gäller det att hitta en grupp med 5 äkta delgrupper. Sedan hittar man en utvidgning av $\mathbb{Q}$ med den som Galoisgrupp. De 5 delgrupper ger 5 motsvarande delkroppar.

Grupper som skrivs som direktprodukt av cykliska grupper har många delgrupper (titta på delgrupperna genererade av varena element i gruppen). Inga av de små grupper vi känner har 5 delgrupper. Cykliska grupper har exakt en delgrupp för varje delare till gruppens ordning, så det räcker att hitta ett tal med 5 äkta delare, till exempel p^6 för något primtal p .

Vi tar $p = 2$ och vill hitta en utvidgning av $\mathbb{Q}$ med grupp $\mathbb{Z}/64\mathbb{Z}$. En sådan finns som delutvidgning till varje cyklotomisk utvidgning av $\mathbb{Q}$ vars grad är ett primtal kongruent med 1 modulo 64. Vi kan till exempel ta $193 = 3 \cdot 64 + 1$. Splittringskroppen till $X^{193} - 1$ över $\mathbb{Q}$ har cyklisk Galoisgrupp av ordning 192 och har en delutvidgning av begärd form: fixkroppen under verkan av delgruppen av ordning 3.

6. *Normala utvidgningar och splittringskroppar* Se Stewart s.82

7. *Beskrivning av enkla kroppsutvidgningar* : Se Stewart s.38.

8. *Låt K vara en kropp med karakteristik 0, $n \in \mathbb{N}$, $a \in K$. Låt L vara en splittringskropp för polynomet $X^n - a$ över K . Visa att Galoisgruppen $G(L : K)$ är lösbar. Beskriv Galoisgruppen i fall $K = \mathbb{Q}$, $n = 3$ och $a = 7$.*

Visa först att L innehåller de n -te enhetsrötter : Låt ζ_n vara ett nollställe till polynomet $X^n - 1 \in K[X]$ och låt $\alpha \in L$ vara ett nollställe till $P_{n,a}(X) = X^n - a$. Då är $(\alpha\zeta_n)^n = \alpha^n = a$, så $\alpha' = \alpha\zeta_n$ är också nollställe till $P_{n,a}$ och därmed element i L ty L är splittringskropp för $P_{n,a}$, så att $\zeta_n = \alpha'/\alpha$ tillhör L och L innehåller splittringskroppen N för polynomet $X^n - 1$ över K .

Vi tittar på utvidgningarna $K \subset N \subset L$ och motsvarande Galoisgrupper $\{1\} \subset \text{Gal}(L : N) \subset \text{Gal}(L : K)$. Eftersom $N : K$ är en normalutvidgning är $\text{Gal}(L : N)$ en normal delgrupp i $\text{Gal}(L : K)$ och $\text{Gal}(L : K)/\text{Gal}(L : N) \simeq \text{Gal}(K : N)$. Men $\text{Gal}(K : N)$ består av morfismer som avbildar ζ_n på andra enhetsrötter ζ_n^i , och sådana kommuterar med varandra $((\zeta_n^i)^j = (\zeta_n^j)^i = \zeta_n^{ij})$ så gruppen är abelsk (isomorf med gruppen av inverterbara element i $\mathbb{Z}/n\mathbb{Z}$).

Som ovan märker vi att alla $\alpha\zeta$, där $\zeta^n = 1$, är nollställe till $P_{n,a}$ och det finns n olika sådana ζ så att alla n olika nollställena till $P_{n,a}$ är av den formen och varje automorfism i $\text{Gal}(L : N)$ avbildar α till en $\alpha\zeta$. Men $\alpha\zeta\zeta' = \alpha\zeta'\zeta$ så $\text{Gal}(L : N)$ är också abelsk.

Alltså är $\{1\} \subset \text{Gal}(L : N) \subset \text{Gal}(L : K)$ en kedja av delgrupper till $\text{Gal}(L : K)$ med abelska kvot som visar lösbarhet av $\text{Gal}(L : K)$.

I fallet $K = \mathbb{Q}$, $n = 3$, $a = 7$ har vi kedjan $\{1\} \subset \mathbb{Z}/3\mathbb{Z} \subset S_3$ som motsvarar kropparna $\mathbb{Q} \subset \mathbb{Q}(\sqrt{-3}) \subset \mathbb{Q}(\sqrt{-3}, \sqrt[3]{7})$. Lägg märke till att $\mathbb{Q}(\sqrt[3]{7}) : N$ inte är en normalutvidgning och har som konjugatkroppar de $\mathbb{Q}(j\sqrt[3]{7})$ där $j^3 = 1, j \neq 1$, alltså är $\text{Gal}(L : \mathbb{Q}(\sqrt[3]{7}))$ inte normal i $\text{Gal}(L : N)$ och $\text{Gal}(L : N)$ är inte abelsk.

Mer allmänt, för $n = p$ ett udda primtal, $a \in \mathbb{Q}$ kvadratfri får vi $\{1\} \subset \mathbb{Z}/(p-1)\mathbb{Z} \subset \text{Gal}(L : \mathbb{Q})$, med $\text{Gal}(L : \mathbb{Q}) = \langle a, b : a^{p-1} = 1 = b^p, ba = ab^{p-1} \rangle$