

1. Bestäm graden, en bas och Galoisgruppen $G(L : \mathbb{Q})$ då L är sönderfallskroppen av polynomet $f(X) = X^{12} - 1$ över $\mathbb{Q}$. Bestäm också alla delkroppar till L .

Vi har $X^{12} - 1 = (X^6 - 1)(X^6 + 1) = (X^3 - 1)(X^3 + 1)(X^2 + 1)(X^4 - X^2 + 1) = (X - 1)(X^2 + X + 1)(X + 1)(X^2 - X + 1)(X^2 + 1)(X^4 - X^2 + 1)$. Genom att lösa ekvationen $X^{12} - 1 = 0$ finner vi nu att talen $\sqrt{3}$ och i genererar sönderfallskroppen dvs $L = \mathbb{Q}(\sqrt{3}, i)$. Alltså är graden $[L : \mathbb{Q}] = 4$. En bas är t ex $1, \sqrt{3}, i, i\sqrt{3}$. Galoisgruppen $G(L : K)$ har 4 element och dessa ges av alla funktioner $\sigma : L \rightarrow L$ sådana att $\sigma(\sqrt{3}) = \pm\sqrt{3}$ och $\sigma(i) = \pm i$. Låt $G(L : \mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, där $\sigma_1 = id$. Alla σ_i för $i = 2, 3, 4$ har ordningen 2 och $G(L : K)$ har 5 delgrupper: $\langle id \rangle$, $G(L : K)$ och $\{\sigma_i, \sigma_i\}$ för $i = 2, 3, 4$. Låt $\sigma_2(\sqrt{3}) = \sqrt{3}$, $\sigma_3(i) = i$ och $\sigma_4(\sqrt{3}) = -\sqrt{3}$, $\sigma_4(i) = -i$. Delkropparna motsvarande delgrupperna $\langle id \rangle$, $G(L : K)$ och $\{\sigma_i, \sigma_i\}$ för $i = 2, 3, 4$ (i denna ordning) är $L, \mathbb{Q}$ och $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(i), \mathbb{Q}(i\sqrt{3})$.

2. Låt $K \subset L$ vara en separabel kroppsutvidgning sådan att $[L : K] = 4$ och låt N vara normala höljet till L över K . Visa att $[N : L] \leq 6$. Vilka är möjliga värden av $[N : L]$? Ge exempel på respektive kroppar $K \subset L \subseteq N$ för två av dessa värden.

L är separabel över K . Alltså finns det $\alpha \in L$ så att $L = K(\alpha)$. Låt $f \in K[X]$ vara minimalpolynomet för α över K . Då är N en sönderfallskropp av f över K . Alltså är N en sönderfallskropp av $g(X) = f(X)/(X - \alpha)$ över $L = K(\alpha)$. Men $g(X)$ har grad 3 så att N som dess sönderfallskropp har som mest grad 6 över L . Möjliga värden av $[N : L]$ är 1, 2, 3, 6. Det första fallet inträffar då alla nollställena till g ligger i L , det andra då g har exakt ett nollställe i L , medan det tredje och det fjärde då g är irreducibelt över L .

Exempel: $f(X) = (X^5 - 1)/(X - 1) = X^4 + X^3 + X^2 + X + 1$ är irreducibelt över $\mathbb{Q}$ och om ε är ett av dess nollställena, så är $L = \mathbb{Q}(\varepsilon)$ en Galoisutvidgning av $\mathbb{Q}$. Alltså är $N = L$ och $[N : L] = 1$. $f(X) = X^4 - 2$ och $\alpha = \sqrt[4]{2}$ ger $L = \mathbb{Q}(\sqrt[4]{2})$. I detta fall är normala höljet $N = \mathbb{Q}(\sqrt[4]{2}, i)$ och $[N : L] = 2$.

3. (a) Låt $K \subset L$ vara en kroppsutvidgning av ändliga kroppar sådan att $[L : K] = 12$. Bestäm antalet kroppar M sådana att $K \subseteq M \subseteq L$. Ge exakta motiveringar!

(b) Låt d vara ett naturligt tal. Motivera att vinkeln d grader kan konstrueras med passare och linjal då och endast då $3 \mid d$ (Du får hänvisa till kända satser – uppgiften är inte svår).

(a) Som vi vet är $K \subset L$ en Galoisutvidgning med cyklisk Galoisgrupp av ordningen 12. Enligt Galoissteorins huvudsats svarar mellankropparna mot delgrupperna av Galoisgruppen $G(L : K)$. Denna grupp som cyklisk har exakt lika många delgrupper som delare till dess ordning 12 dvs 6 delgrupper (ty 12 har 6 delare: 1, 2, 3, 4, 6, 12). Alltså finns det 6 kroppar M sådana att $K \subseteq M \subseteq L$.

(b) Vinkeln 1° är konstruerbar (med passare och linjal) då och endast då en regelbunden 360-hörning är konstruerbar. Men $360 = 2^3 \cdot 3^2 \cdot 5$ och primtalet 3 förekommer 2 gånger som faktor, vilket innebär att 360-hörning inte är konstruerbar (enligt Gauss sats). Vinkeln 2° är konstruerbar då och endast då en regelbunden 180-hörning är konstruerbar. Men $180 = 2^2 \cdot 3^2 \cdot 5$, vilket leder till samma resultat dvs 180-hörning är inte konstruerbar så att 2° är inte konstruerbar. Vinkeln 3° är konstruerbar då och endast då en regelbunden 120-hörning är konstruerbar. Nu är $120 = 2^3 \cdot 3 \cdot 5$, vilket innebär att 120-hörning är konstruerbar och således vinkeln 3° . Det är klart att varje multipel av denna vinkel är konstruerbar dvs varje vinkel d° då $d = 3k$, k ett naturligt tal. Men varje vinkel d° , där $d = 3k + 1$ eller $d = 3k + 2$ är inte konstruerbar därför att konstruerbarheten av en sådan vinkel skulle innebära att vinkeln med måttet $d - 3k = 1$ eller 2 grader skulle vara konstruerbar.

4. Låt $\alpha = \sqrt{a + b\sqrt{d}}$, där a, b, d är heltal och antag att $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Formulera ett villkor som garanterar att $L = \mathbb{Q}(\alpha)$ är en Galoisutvidgning av $\mathbb{Q}$. Vilken Galoisgrupp har då L över $\mathbb{Q}$ – cyklisk eller "Kleinsfyra"? Ge två exempel.

Först finner vi lätt att α är ett nollställe till polynomet $X^4 - 2aX^2 + (a^2 - db^2)$ som måste vara irreducibelt i $\mathbb{Q}$ beroende på att $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Detta polynom har 4 nollställena: $\pm\sqrt{a \pm b\sqrt{d}}$.

Beteckna $\beta = \sqrt{a - b\sqrt{d}}$. Utvidgningen $L \supset \mathbb{Q}$ är Galois då och endast då $\beta \in L$ ty då och endast då alla fyra nollställena $\pm\alpha, \pm\beta \in L$. Detta villkor kan också uttryckas så att $\alpha\beta = \sqrt{a^2 - db^2} \in L$. (Vi skall precisera detta villkor nedan – det är inte nödvändigt för presentationen av lösningen).

Låt oss beskriva Galoisgruppen $G(L : \mathbb{Q})$ då L är Galois över $\mathbb{Q}$. Låt σ vara en automorfism av L sådan att $\sigma(\alpha) = \beta$ (en sådan automorfism måste finnas). Då är $\sigma(\alpha^2) = \beta^2$ så att $\sigma(b\sqrt{d}) = -b\sqrt{d}$ ty $\sigma(a) = a$. Men $b \neq 0$ ty annars $L = \mathbb{Q}(\sqrt{a})$ har grad 2 över $\mathbb{Q}$. Alltså är $\sigma(\sqrt{d}) = -\sqrt{d}$ ty $\sigma(b) = b$. Detta betyder att $\sigma^2 \neq id$ och således är ordningen av σ i Galoisgruppen lika med 4. Alltså är $G(L : \mathbb{Q})$ cyklisk.

Två exempel. Tag $\alpha = \sqrt{2 + \sqrt{2}}$. Då är $\beta = \sqrt{2 - \sqrt{2}}$ och $\alpha\beta = \sqrt{2} \in L$, där $L = \mathbb{Q}(\alpha)$ ty $\alpha^2 - 2 = \sqrt{2} \in L$. Man kan också välja $\alpha = \sqrt{5 + \sqrt{5}}$ (kontrollera att $\alpha\beta \in L$ då $\beta = \sqrt{5 - \sqrt{5}}$). Av resonemanget nedan följer att $\alpha = \sqrt{3 + \sqrt{3}}$ inte duger.

Nu analyserar vi närmare villkoret $\alpha\beta \in L$ (den delen är inte nödvändig för att besvara frågor i uppgiften). Det faktum att Galoisgruppen är cyklisk implicerar att L endast har en delkropp av grad 2 över $\mathbb{Q}$ som är $\mathbb{Q}(\sqrt{d})$. Vi har $\alpha\beta = \sqrt{a^2 - db^2} \in L$. Beteckna $\sqrt{a^2 - db^2} = r$. Vi påstår att $r \notin \mathbb{Q}$. Om vi antar motsatsen dvs att $r \in \mathbb{Q}$ så ger $\beta = r/\alpha$ att $\sigma(\beta) = r/\sigma(\alpha) = r/\beta = \alpha$. Men $\sigma(\alpha) = \beta$ och $\sigma(\beta) = \alpha$ ger att $\sigma^2 = id$, vilket strider mot att σ har ordning 4 i Galoisgruppen. Alltså är $r = \sqrt{a^2 - db^2} \notin \mathbb{Q}$, vilket innebär att $\mathbb{Q}(\sqrt{a^2 - db^2})$ är en kvadratisk utvidgning av $\mathbb{Q}$. Men det finns endast en sådan i L , så att $\mathbb{Q}(\sqrt{a^2 - db^2}) = \mathbb{Q}(\sqrt{d})$. Vi har visat att $L = \mathbb{Q}(\alpha)$ är Galois över $\mathbb{Q}$ då och endast då $\mathbb{Q}(\sqrt{a^2 - db^2}) = \mathbb{Q}(\sqrt{d})$. Detta villkor är mycket enkelt att kontrollera. Tag t ex $\alpha = \sqrt{3 + \sqrt{3}}$. Då är $a^2 - db^2 = 6$ och $\mathbb{Q}(\sqrt{6}) \neq \mathbb{Q}(\sqrt{3})$ dvs $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3 + \sqrt{3}})$ är inte Galois över $\mathbb{Q}$.

- 5. Låt $L = K(\alpha)$ och låt $f(X)$ vara minimalpolynomet av α över K . Låt $K \subseteq M \subseteq L$, där M är en kropp. Visa att om $K \subseteq L$ är en Galoisutvidgning så har alla irreducibla faktorer av $f(X)$ i polynomringen $M[X]$ samma grad.**

Låt β beteckna ett annat nollställe till $f(X)$ i L ($f(X)$ är en produkt av linjära faktorer i $L[X]$ ty L är normal över K). Då är $L = K(\alpha) = K(\beta)$ ty $f(X)$ är irreducibelt över K . Låt nu $g(X)$ och $h(X)$ vara två irreducibla faktorer av $f(X)$ i $M[X]$. Låt vidare α vara ett nollställe till $g(X)$ och β ett nollställe till $h(X)$. Då är $L = M(\alpha) = M(\beta)$ ty $L = K(\alpha) = K(\beta)$. Alltså är $\text{grad } g = [M(\alpha) : M] = [M(\beta) : M] = \text{grad } h$ dvs två godtyckliga irreducibla faktorer av f över M har samma grad.

- 6. Visa att en utvidgning $K \subseteq L$ är ändlig då och endast då den är algebraisk och ändligt genererad.**
- 7. Låt G vara en ändlig grupp av automorfismer av en kropp L . Visa en av olikheterna $[L : L^G] \geq |G|$ eller $[L : L^G] \leq |G|$.**
- 8. Låt K vara en kropp av karakteristiken 0 och låt $a \in K$. Visa att Galoisgruppen för sönderfallskroppen av polynomet $X^n - a$ över K är lösbar.**

För 6,7,8 se kursboken eller stencilen med bevisen av satser.