Alg3
Tredje sæt obligatoriske opgaver

Rasmus Sylvester Bryder

23. marts 2010

Henvisninger på formen N $\star$ er til forelæsningsnoterne, og AT refererer til afsnit i "Algebra" af Anders Thorup.

Opgave C3.1

Betragt polynomiet $g(x) = x^3 + 2x + 2$ *over* $\mathbb{Q}$.

(1) *Vis, at* g *er irreducibel i* $\mathbb{Q}[x]$.

Da g har heltallige koefficienter, og da der findes et primtal p, så p går op i alle koefficienter pånær den ledende og p^2 ikke går op i konstantleddet, nemlig $p = 2$, er g irreducibel pr. Eisensteins irreducibilitetskriterium, N 2.36.

(2) *Vis, at* g *har præcis én reel rod.*

Det følger af algebraens fundamentalsætning, at g har tre rødder a, b, c i $\mathbb{C}$. Da g er monisk, har vi i $\mathbb{C}[x]$, at

$$\begin{aligned} g(x) &= (x-a)(x-b)(x-c) \\ &= x^3 - (a+b+c)x^2 + (ab+ac+bc)x - abc. \end{aligned}$$

Da må $a + b + c = 0$, $ab + ac + bc = 2$ og $abc = -2$. Vi får deraf, at

$$0 = (a+b+c)^2 = a^2 + b^2 + c^2 + 2(ab+ac+bc) = a^2 + b^2 + c^2 + 4.$$

Vi ser, at a, b, c ikke alle tre kan være reelle, da deres kvadrater derpå alle ville være større end lig 0, hvilket ville føre til modstrid med ovenstående. Altså må mindst én rod være kompleks; lad denne være a. Den konjugerede til denne rod er ligeledes en rod pr. regneregler for konjugerede, da g har reelle koefficienter; sæt da $b = \overline{a}$. Da $a + b = 2\mathrm{Re}a$, må $c = -(a+b) \in \mathbb{R}$, hvoraf g har én reel rod og to komplekse.

(3) *Lad* M *være spaltningslegemet for* g *over* $\mathbb{Q}$. *Vis, at* $M/\mathbb{Q}$ *er normal og bestem Galois-gruppen* $\mathrm{Gal}(M/\mathbb{Q})$.

Da g er irreducibel i $\mathbb{Q}[x]$, følger af N 2.70, at g er separabel. N 3.26 giver nu, at $M/\mathbb{Q}$ er normal.

Endvidere giver N 3.40, da g ikke har multiple rødder i M jf. N 2.67, at $3 \mid [M:\mathbb{Q}] \mid 6$.

Lad β være den ene reelle rod for g og lad α være en kompleks rod for g (jf. **(2)**); det er klart, at $\beta, \alpha \in M$. Da vi nu har, at $\mathbb{Q} \subseteq \mathbb{Q}(\beta)$ og $\mathbb{Q}(\beta) \subseteq M$, da M indeholder $\mathbb{Q}$ og alle rødder for g, får vi jf. N 2.47, at

$$[M:\mathbb{Q}] = [M:\mathbb{Q}(\beta)][\mathbb{Q}(\beta):\mathbb{Q}].$$

Da $g \in \mathbb{Q}[x]$ er irreducibelt og monisk, samt har β som rod, må $g = \mathrm{Irr}(\beta, \mathbb{Q})$, hvorpå $[\mathbb{Q}(\beta):\mathbb{Q}] = \deg g = 3$.

Nu må $[M:\mathbb{Q}(\beta)] \leq 2$. Antag, at $[M:\mathbb{Q}(\beta)] = 1$. Da vil $M = \mathbb{Q}(\beta) \subseteq \mathbb{R}$, i modstrid med, at M indeholder $\alpha \in \mathbb{C}$. Altså må $[M:\mathbb{Q}(\beta)] = 2$, så $[M:\mathbb{Q}] = 6$. Galois-teoriens fundamentalsætning N 3.32 giver, at $|\mathrm{Gal}(M/\mathbb{Q})| = 6$. Da N 3.40 gav, at $\mathrm{Gal}(M/\mathbb{Q})$ var isomorf med en undergruppe af S_3 af orden 6, må der gælde, at $\mathrm{Gal}(M/\mathbb{Q}) \simeq S_3$.

Opgave C3.2

Lad M være spaltningslegemet for polynomiet $f(x) = (x^3-2)(x^4-2)$ over $\mathbb{Q}$.

(1) *Vis, at M indeholder spaltningslegemerne L_1 og L_2 for hhv. $f_1(x) = x^3-2$ og $f_2(x) = x^4-2$ over $\mathbb{Q}$.*

Da alle rødderne for f_1 og f_2 tydeligt er rødder for f over $\mathbb{Q}$, må rødderne for f_1 og f_2 være indeholdt i M. Dermed kan f_1 og f_2 opspaltes i lineære faktorer i M (da $M[x]$ indeholder alle lineære faktorer i faktoriseringen af f_1 og f_2), hvorpå L_1 og L_2 er indeholdt i M, thi L_1 og L_2 er minimale med hensyn til den egenskab.

(2) *Vis, at M er kompositet L_1L_2 af L_1 og L_2 og at $L_1 \cap L_2 = \mathbb{Q}$.*

Da L_1L_2 er det mindste legeme, der indeholder både L_1 og L_2, samt $L_1 \subseteq M$ og $L_2 \subseteq M$ (jf. **(1)**), må $L_1L_2 \subseteq M$. M er det mindste legeme, der indeholder $\mathbb{Q}$ og rødderne i f. Vi har, at $\mathbb{Q} \subseteq L_1 \subseteq L_1L_2$. Da alle rødder for f enten er rødder for f_1 eller for f_2, og alle rødder i f_1 og f_2 ligger i L_1L_2, må alle rødderne for f ligge i L_1L_2. Altså vil $M \subseteq L_1L_2$, og dermed $M = L_1L_2$.

Vi har nu, at $L_1 \cap L_2$ er et legeme, og at $\mathbb{Q} \subseteq L_1 \cap L_2 \subseteq L_i$, $i = 1, 2$. Altså vil gælde pr. N 2.47, at $[L_1 \cap L_2 : \mathbb{Q}] \mid [L_i : \mathbb{Q}]$, $i = 1, 2$. Eksemplerne N 3.42 samt N 3.44 giver, at $[L_1:\mathbb{Q}] = 6$ og $[L_2:\mathbb{Q}] = 8$. Altså vil $[L_1 \cap L_2 : \mathbb{Q}]$ gå op i den største fælles divisor i 6 og 8, nemlig 2; altså vil $[L_1 \cap L_2 : \mathbb{Q}] \leq 2$.

Vi ønsker at vise, at $[L_1 \cap L_2 : \mathbb{Q}] = 1$. Antag derfor, at $[L_1 \cap L_2 : \mathbb{Q}] = 2$. Da $L_1 \cap L_2$ er et dellegeme af L_2 med dimension 2 over $\mathbb{Q}$, giver Galois-teoriens fundamentalsætning N 3.37 og eksempel N 3.44, at $L_1 \cap L_2$ må være et af de tre dellegemer af L_2 med dimension 2 over $\mathbb{Q}$; altså

$$L_1 \cap L_2 \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2}i)\}.$$

Lad ε være den tredje enhedsrod. Vi har, at $L_1 = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\varepsilon, \sqrt[3]{2}\varepsilon^2)$ pr. definition, som er lig $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$, thi $\varepsilon = \sqrt[3]{2}\varepsilon(\sqrt[3]{2})^{-1}$. Da ε er rod i $x^2+x+1 \in \mathbb{Q}[x]$ og $\varepsilon \notin \mathbb{Q}$, må $[\mathbb{Q}(\varepsilon):\mathbb{Q}] = 2$. Da $\mathrm{Gal}(L_1/\mathbb{Q}) \simeq S_3$ pr. N 3.42 og da der kun er én

undergruppe af orden 3 i S_3 (nemlig $\langle 1\,2\,3\rangle$), ser vi, at der kun er én undergruppe af orden 3 og index 2 i $\mathrm{Gal}(L_1/\mathbb{Q})$, hvormed der kun er ét dellegeme af L_1, hvis dimension er 2 over $\mathbb{Q}$; dette må være $\mathbb{Q}(\varepsilon)$, thi $\mathbb{Q}(\varepsilon) \subseteq L_1$, så $L_1 \cap L_2 = \mathbb{Q}(\varepsilon)$. Altså vil $\mathbb{Q}(\varepsilon) \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2}i)\}$.

Da ε er kompleks og $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$, må ε ligge i enten $\mathbb{Q}(i)$ eller $\mathbb{Q}(\sqrt{2}i)$. Men da ε har en entydig fremstilling $\varepsilon = -1/2 + \sqrt{3}/2i$, kan ε ikke ligge i $\mathbb{Q}(i)$, thi det ville kræve, at $\sqrt{3}$ var rational. Altså må $\varepsilon \in \mathbb{Q}(\sqrt{2}i)$. ε er nu på formen $\varepsilon = a + b\sqrt{2}i$ (thi $\sqrt{2}i$ er rod for $x^2 + 2$), så der findes $b \in \mathbb{Q}$, så $b\sqrt{2} = \sqrt{3}$ og altså $b = \sqrt{3/2}$. Dette $b \in \mathbb{Q}$ løser altså ligningen $2x^2 - 3$, men de eneste mulige rationale rødder til denne er på formen a/b, hvor $a \in \{\pm 1, \pm 3\}$ (går op i konstantleddet) og $b \in \{\pm 1, \pm 2\}$ (går op i den ledende koefficient), og det ses let, at ingen af disse muligheder er rødder for $2x^2 - 3$. Altså har ligningen $2x^2 - 3$ ingen rationale rødder, hvilket er en modstrid (vi har her vist, at $\sqrt{3/2}$ er irrational).

Dermed må $[L_1 \cap L_2 : \mathbb{Q}] = 1$, hvorpå $L_1 \cap L_2 = \mathbb{Q}$.

(3) *Find dimensionen* $[M : \mathbb{Q}]$ *og bestem Galois-gruppen* $\mathrm{Gal}(M/\mathbb{Q})$.

Da f_1 og f_2 er irreducible pr. Eisenstein, er de separable, hvorpå $L_1/\mathbb{Q}$ og $L_2/\mathbb{Q}$ er endelige normale udvidelser jf. N 3.26. Da $L_1, L_2 \subseteq M$, $M = L_1L_2$ og $L_1 \cap L_2 = \mathbb{Q}$, giver N 3.47, at $\mathrm{Gal}(M/\mathbb{Q}) \simeq \mathrm{Gal}(L_1/\mathbb{Q}) \times \mathrm{Gal}(L_2/\mathbb{Q}) \simeq S_3 \times D_4$ jf. eksempler N 3.42 og N 3.44. Altså må gælde jf. N 3.37, at

$$[M : \mathbb{Q}] = |\mathrm{Gal}(M/\mathbb{Q})| = 3! \cdot 2 \cdot 4 = 48.$$

(4) *Lad* φ *være homomorfien beskrevet i N 3.40. Er* $\varphi(\mathrm{Gal}(M/\mathbb{Q}))$ *en transitiv undergruppe af* S_7*?*

Vi søger at vise, at $\mathrm{Gal}(M/\mathbb{Q})$ ikke er en transitiv undergruppe af S_7, hvorpå billedet heller ikke er det, thi φ er injektiv.

Rødderne for f er $\Omega = \{\sqrt[3]{2}, \sqrt[3]{2}\varepsilon, \sqrt[3]{2}\varepsilon^2, \sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}, -\sqrt[4]{2}i\}$; altså har f ingen multiple rødder. N 3.40 giver nu, at $\mathrm{Gal}(M/\mathbb{Q})$ er isomorf med en undergruppe af S_7.

M er udvidelsen af $\mathbb{Q}$, der indeholder alle rødderne for f. Enhver automorfi i $\mathrm{Gal}(M/\mathbb{Q})$ er entydigt bestemt ved sine værdier på disse rødder, og jf N 3.4 må billedet af enhver automorfi på en af rødderne igen være en rod for f; da det er en bijektion, udgør alle billederne af Ω hele Ω. Enhver automorfi i $\mathrm{Gal}(M/\mathbb{Q})$ kan altså betragtes som en bijektiv afbildning $\Omega \to \Omega$ og er dermed en entydigt bestemt permutation af rødderne i Ω, således, at $\mathrm{Gal}(M/\mathbb{Q}) \subseteq S(\Omega)$.

Dette inducerer en gruppevirkning af $\mathrm{Gal}(M/\mathbb{Q})$ på Ω ved blot at definere $\sigma.a := \sigma(a)$ for alle $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$ og $a \in \Omega$, jf. N s. 35. Vi vil vise, at der findes $a, b \in \Omega$, således at for alle $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$, vil $\sigma.a = \sigma(a) \neq b$.

Lad $\alpha \in L_1$ være rod for f_1. Det er klart, at $\alpha \notin \mathbb{Q}$, thi andet ville stride imod Eisenstein. Altså vil $\alpha \notin L_1 \cap L_2$, og dermed $\alpha \notin L_2$. Lader vi $\beta \in L_2$ være rod for f_2, vil vi tilsvarende få, at $\beta \notin L_1$. Vi husker, at $\alpha, \beta \in \Omega$.

Lad $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$. Da f_1 er et polynomium i $M[x]$, får vi jf. N 3.4, at $\sigma(\alpha)$ er en rod i f_1 og ligger i L_1. Da må gælde jf. ovenstående, at $\sigma(\alpha) \notin L_2$, så specielt vil $\sigma(\alpha) \neq \beta$ for alle $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$. Altså er $\mathrm{Gal}(M/\mathbb{Q})$ ikke en transitiv undergruppe af $S(\Omega) \simeq S_7$ jf. N 1.162, da $|\Omega| = 7$.