Alg3
Andet sæt obligatoriske opgaver

Rasmus Sylvester Bryder

9. marts 2010

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

Opgave C2.1

Lad G være en endelig gruppe af orden $55055 = 5 \cdot 7 \cdot 11^2 \cdot 13$. Lad $P \in \mathrm{Syl}_{13}(G)$, $Q \in \mathrm{Syl}_{11}(G)$, $R \in \mathrm{Syl}_7(G)$, $S \in \mathrm{Syl}_5(G)$.

(1) *Vis, at $m_{11}(G) = 1$ og at $Q \lhd G$.*

Vi har, at $m_{11}(G) \mid |G : Q| = 5 \cdot 7 \cdot 13$ pr. en bemærkning i N, s. 30 og Lagranges indexsætning, N 1.38; altså er $m_{11}(G) \in \{1, 5, 7, 13, 35, 65, 91, 455\}$ – mængden af positive divisorer i 455.

Da vi endvidere har pr. Sylows tredje sætning, N 1.138, at $m_{11}(G) \equiv 1 \pmod{11}$, kan vi udelukke 5 (da $5 \equiv 5 \pmod{11}$), 7 (da $7 \equiv 7 \pmod{11}$), 13 (da $13 \equiv 2 \pmod{11}$), 35 (da $35 \equiv 2 \pmod{11}$), 65 (da $65 \equiv -1 \pmod{11}$), 91 (da $91 \equiv 3 \pmod{11}$) og 455 (da $455 \equiv 4 \pmod{11}$). Altså må $m_{11}(G) = 1$.

Lad $g \in G$ og betragt gQg^{-1}, som også er en Sylow-11-undergruppe pr. Sylows anden sætning, N 1.136; da der kun er én Sylow-11-undergruppe i G, må $gQg^{-1} = Q$. Da g var valgt vilkårligt, gælder pr. N 1.48, at $Q \lhd G$.

(2) *Vis, at G/Q er cyklisk.*

Vi har, at $|G/Q| = |G : Q| = 5 \cdot 7 \cdot 13$ (pr. N 1.60). Sæt nu $p_1 = 5$, $p_2 = 7$ og $p_3 = 13$, så $|G/Q| = p_1 p_2 p_3$ – det er let at se, at de er primtal! Da vi har, at $5 \nmid 7 - 1$, $5 \nmid 13 - 1$ og $7 \nmid 13 - 1$, er betingelserne i N 1.214 opfyldt, og der findes dermed kun én gruppe af orden $5 \cdot 7 \cdot 13$ op til isomorfi.

For ethvert $n \in \mathbb{N}$ har vi mindst én gruppe af orden n, nemlig C_n (jf. N s. 49). Da der kun findes én gruppe af orden $5 \cdot 7 \cdot 13 = 455$ op til isomorfi, må denne altså være cyklisk. Da $|G/Q| = 455$, må G/Q altså være cyklisk.

(3) *Brug forrige resultat til at vise, at PQ, QR, QS og QRS er normale undergrupper i G.*

Da $Q \lhd G$, gælder pr. N 1.55, at QP, QR og QS er undergrupper i G. Vi får dermed pr. N 1.46, at $QP = PQ$, hvorpå PQ er en undergruppe i G.

Vi danner nu den kanoniske epimorfi $\kappa : G \to G/Q$, idet $Q \lhd G$, hvorpå G/Q er en gruppe (jf. N 1.60). Vi får nu pr. Noethers anden isomorfisætning, N 1.86, at der er en 1-1-korrespondance mellem undergrupper i G, der indeholder Q, og undergrupper i G/Q, og denne opfylder $K \lhd G \Leftrightarrow \kappa(K) \lhd G/Q$. Vi har derfor, da PQ, QR og QS er undergrupper i G og da Q er indeholdt i dem alle tre, at $\kappa(PQ)$, $\kappa(QR)$ og $\kappa(QS)$ er undergrupper i G/Q.

Vi fandt i **(2)**, at G/Q var cyklisk. Specielt er G/Q abelsk, og pr. N 1.50 er alle undergrupper normale i G/Q; altså får vi, at $\kappa(PQ) \lhd G/Q$, $\kappa(QR) \lhd G/Q$ og $\kappa(QS) \lhd G/Q$, og pr. Noethers anden isomorfisætning har vi, at $PQ \lhd G$, $QR \lhd G$, $QS \lhd G$.

Da $QR \lhd G$, må QRS være en undergruppe i G jf. N 1.55. Da $Q \subseteq QRS$, har vi, at $\kappa(QRS)$ er en undergruppe i G/Q; da G/Q er abelsk, er $\kappa(QRS)$ normal i G/Q, og Noethers anden isomorfisætning giver nu slutteligt, at $QRS \lhd G$.

(4) *Hvilke af undergrupperne PQ, QR, QS og QRS er nødvendigvis abelske?*

Vi betragter undergruppen PQ. Vi har, at $|P| = 13$ og $|Q| = 11^2$.

Lad $g \in P \cap Q$. Da $|g| \mid 13$ og $|g| \mid 11^2$ pr. N 1.39, må $|g| \mid (13, 11^2) = 1$. Altså må $|g| = 1$, og dermed er $g = e$; altså vil $P \cap Q \subseteq \{e\}$. Da $P \cap Q$ er en undergruppe (jf. N 1.14), må $e \in P \cap Q$ (jf. N 1.12), og dermed er $P \cap Q = \{e\}$. Vi får nu pr. N 1.43, at $|PQ| = |P||Q||P \cap Q|^{-1} = 13 \cdot 11^2$.

Da $Q \subseteq PQ \subseteq G$ og $Q \lhd G$, må $Q \lhd PQ$ (jf. N 1.48). Da P er en undergruppe i PQ af orden 13, thi $P \subseteq PQ$ og P er en undergruppe i G, må P være en Sylow-13-undergruppe i PQ, thi $13 \nmid 11^2$, jf. N 1.128.

Vi har pr. bemærkningen N s. 30, at $m_{13}(PQ) \mid |PQ : P| = 11^2$, hvorpå altså $m_{13}(PQ) \in \{1, 11, 121\}$. Da $121 \equiv 4 \pmod{13}$ og $11 \equiv 11 \pmod{13}$, må gælde pr. Sylows tredje sætning, N 1.138, at $m_{13}(PQ) = 1$.

Da er P altså Sylow-13-undergruppen i PQ, og dermed er $P \lhd PQ$. Vi får altså pr. N 1.145, at $PQ \simeq P \times Q$. Vi har pr. N 1.210, da $|P| = 13$, at $P \simeq C_{13}$, hvorpå P specielt er abelsk, og pr. N 1.112, da $|Q| = 11^2$, at Q er abelsk. Da må $P \times Q$ selv være abelsk (hvilket let indses ved den koordinatvise komposition), hvorfor PQ nødvendigvis er abelsk.

På stort set samme måde kan vises, at QR er abelsk.

Lades nemlig $g \in Q \cap R$, må $|g| \mid (7, 11^2) = 1$, så $|g| = 1$ og $g = e$. Da $Q \cap R$ er en undergruppe selv (jf. N 1.14), må $e \in Q \cap R$ (jf. N 1.12). Altså er $Q \cap R = \{e\}$, og $|QR| = 7 \cdot 11^2$ jf. N 1.43.

Da $Q \subseteq QR \subseteq G$ og $Q \lhd G$, må $Q \lhd QR$ (jf. N 1.48). Vi har endvidere – da R er en undergruppe i QR af orden 7, fordi $R \subseteq QR$ og R er en Sylow-7-undergruppe i G – at R må være en Sylow-7-undergruppe i QR, thi $7 \nmid 11^2$, jf. N 1.128.

Pr. N s. 30 fås, at $m_7(QR) \mid |QR : R| = 11^2$, hvorpå $m_7(QR) \in \{1, 11, 121\}$. Da $121 \equiv 2 \pmod{7}$ og $11 \equiv 4 \pmod{7}$, har vi pr. N 1.138, at $m_7(QR) = 1$. R er dermed Sylow-7-undergruppen i QR, så $R \lhd QR$. N 1.145 giver, at $QR \simeq Q \times R$. Pr. N 1.210 er $R \simeq C_7$, hvorpå R er abelsk. Da indses igen, at $Q \times R$ selv er abelsk, hvorpå QR nødvendigvis er abelsk.

Derimod er QS og QRS ikke nødvendigvis abelske i G. For at vise dette, finder vi en gruppe A af orden 55055, hvori vi lader $Q_A \in \mathrm{Syl}_{11}(A)$, $R_A \in \mathrm{Syl}_7(A)$ og $S_A \in \mathrm{Syl}_5(A)$ og derpå viser, at $Q_A S_A$ og $Q_A R_A S_A$ *ikke* er abelske.

Betragt gruppen $A = C_7 \times C_{11} \times C_{13} \times H$, hvor H er en ikke-abelsk gruppe af orden 55: denne findes, thi $55 = 5 \cdot 11$, $5 \mid 11 - 1$, hvorpå vi kan benytte N 1.212 og betragte gruppen $H = F(11, 5)$.

Det er klart, at A har orden $5 \cdot 7 \cdot 11^2 \cdot 13 = 55055$, hvorpå vi kan benytte de foregående resultater for G på A. Lad $Q_A \in \mathrm{Syl}_{11}(A)$, $R_A \in \mathrm{Syl}_7(A)$ og $S_A \in \mathrm{Syl}_5(A)$. Alt hvad gælder for Q i de foregående resultater, gælder altså for Q_A her, etc.

Vi ønsker at vise, at der findes en ikke-abelsk undergruppe i $Q_A S_A$. Betragt $J = \{e\} \times \{e\} \times \{e\} \times H \subseteq A$; det ses let, at J er isomorf med H og en undergruppe i A; J er altså ligeledes en ikke-abelsk gruppe af orden 55. Lad $a \in J$; vi vil vise, at $a \in Q_A S_A$. Da er $|a|$ enten 1, 5 eller 11 (var $|a| = 55$, var J cyklisk og dermed abelsk), jf. N 1.39.

Hvis $|a| = 1$, er $a = e \in Q_A S_A$, thi $Q_A S_A$ er en undergruppe.

Hvis $|a| = 5$, kan vi betragte $\langle a \rangle$. Da $|\langle a \rangle| = 5 \nmid 11011$, har vi, at $\langle a \rangle$ er en Sylow-5-undergruppe i A (jf. N 1.128). Vi har nu, at $S_A = f\langle a \rangle f^{-1}$ for et $f \in A$ pr. Sylows anden sætning, hvorpå $f^{-1} S_A f = \langle a \rangle$.

Altså fås, at $Q_A\langle a \rangle = Q_A f^{-1} S_A f = f^{-1} Q_A S_A f = Q_A S_A$ jf. N 1.48, da Q_A og $Q_A S_A$ er normale i A, hvorpå $a \in Q_A\langle a \rangle = Q_A S_A$.

Hvis endelig $|a| = 11$, følger at $\langle a \rangle = b Q_A b^{-1}$ for et $b \in A$, hvorpå vi får, at $S_A\langle a \rangle = S_A b Q_A b^{-1} = S_A Q_A b b^{-1} = S_A Q_A = Q_A S_A$ jf. N 1.46 og jf. N 1.48, da $Q_A \lhd A$.

Altså vil $a \in Q_A S_A$ i alle tilfælde, hvorpå $J \subseteq Q_A S_A$. Altså er $Q_A S_A$ ikke abelsk, thi den indeholder en ikke-abelsk undergruppe J.

Da $Q_A S_A \subseteq Q_A R_A S_A$, er $Q_A R_A S_A$ heller ikke abelsk.

(5) *Hvordan udledes det af (4), at $P \lhd G$ og $R \lhd G$?*

Vi har, at $P \subseteq PQ$ og $R \subseteq QR$.

Vi udledte i **(4)**, at $P \lhd PQ$. Da $|PQ| = 13 \cdot 11^2$ og $(13, 11^2) = 1$, fås pr. N 1.124, da $P \lhd PQ$, at P char PQ.

Vi udledte ligeledes, at $R \lhd QR$, og da $|QR| = 11^2 \cdot 7$ og $(11^2, 7) = 1$, fås pr. N 1.124, da $R \lhd QR$, at R char QR.

Vi har nu med **(3)**, at P char $PQ \lhd G$ og R char $QR \lhd G$. Vi får nu med N 1.119, at $P \lhd G$ og $R \lhd G$.

Opgave C2.2

Lad α være et algebraisk tal af ulige grad over $\mathbb{Q}$. Vis, at α og α^2 har samme grad over $\mathbb{Q}$.

Vi lader $\mathbb{L}$ betegne et legeme, som indeholder α og $\mathbb{Q}$, hvorpå det også indeholder α^2, da det er stabilt under multiplikation. Da $\mathbb{Q}(\alpha)$ er et dellegeme af $\mathbb{L}$, der indeholder α og $\mathbb{Q}$, indeholder det specielt α^2, hvorpå $\mathbb{Q}(\alpha^2) \subseteq \mathbb{Q}(\alpha)$, da $\mathbb{Q}(\alpha^2)$ er det *mindste* dellegeme af $\mathbb{L}$, som indeholder $\mathbb{Q}$ og α^2; således får vi, at $\mathbb{Q} \subseteq \mathbb{Q}(\alpha^2) \subseteq \mathbb{Q}(\alpha)$.

Da vi har disse legemsinklusioner, får vi med transitivitetssætningen, N 2.47, at $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)][\mathbb{Q}(\alpha^2) : \mathbb{Q}]$, da $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$, thi α var algebraisk over $\mathbb{Q}$. Viser vi $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] = 1$, er vi færdige.

Betragt derfor homomorfien $\Phi : \mathbb{Q}(\alpha^2)[x] \to \mathbb{Q}(\alpha^2)[\alpha]$ givet ved $\Phi(f) = f(\alpha)$. Lad $f(x) = x^2 - \alpha^2$; det ses, at $f \in \mathbb{Q}(\alpha^2)[x]$. Da $f \neq 0$ og $f(\alpha) = 0$, får vi, at $\ker \Phi \neq 0$, hvorpå $\mathbb{Q}(\alpha^2)[\alpha] = \mathbb{Q}(\alpha^2)(\alpha)$.

Graden af $\mathrm{Irr}(\alpha, \mathbb{Q}(\alpha^2))$ er den laveste positive grad, som et polynomium med koefficienter i $\mathbb{Q}(\alpha^2)$ og α som rod kan have. Vi har derfor, at

$$2 = \deg f \geq \deg \mathrm{Irr}(\alpha, \mathbb{Q}(\alpha^2)) = [\mathbb{Q}(\alpha^2)(\alpha) : \mathbb{Q}(\alpha^2)] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)],$$

thi $\mathbb{Q}(\alpha^2)(\alpha) = \mathbb{Q}(\alpha^2, \alpha) = \mathbb{Q}(\alpha)$ jf. 2.14, idet inklusionen $\mathbb{Q}(\alpha^2, \alpha) \supseteq \mathbb{Q}(\alpha)$ er klar, og idet $\alpha^2 \in \mathbb{Q}(\alpha)$, hvorpå $\mathbb{Q}(\alpha^2, \alpha) \subseteq \mathbb{Q}(\alpha)$.

Hvis $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] = 2$, er dette i modstrid med, at α var af ulige grad, da der så ville gælde, at $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ var lige; altså må vi have, at $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] = 1$, hvilket var, hvad vi ønskede.

Opgave C2.3

Lad $\mathrm{GF}(5) = \mathbb{Z}_5$ *være legemet med 5 elementer.*

(1) *Vis, at polynomiet* $p(x) = x^3 + x^2 + 1 \in \mathrm{GF}(5)[x]$ *er irreducibelt over* $\mathrm{GF}(5)$.

$\mathrm{GF}(5)$ er et integritetsområde, thi det er et legeme. Da p er monisk af grad 3, har vi pr. øvelse 2.8, at det er nok at vise, at p ikke har nogen rødder i $\mathrm{GF}(5)$, hvorfor p derpå er irreducibel.

Vi prøver derfor elementerne i $\mathrm{GF}(5)$ igennem: Da $0^3 + 0^2 + 1 = 1$, $1^3 + 1^2 + 1 = 3$, $(-1)^3 + (-1)^2 + 1 = 1$, $2^3 + 2^2 + 1 = 3$ og $(-2)^3 + (-2)^2 + 1 = 2$, har p ingen rødder i $\mathrm{GF}(5)$, hvorpå p er irreducibel.

(2) *Vis, at* $\mathrm{GF}(125)$ *er et spaltningslegeme for* p *over* $\mathrm{GF}(5)$.

Lad $\mathbb{L}$ være et legeme, som indeholder $\mathrm{GF}(5)$, og antag, at $\alpha \in \mathbb{L}$ er rod i p. Betragt nu $\mathrm{GF}(5)(\alpha)$, og dan homomorfien $\Phi : \mathrm{GF}(5)[x] \to \mathrm{GF}(5)[\alpha]$ givet ved $\Phi(f) = f(\alpha)$. Da $p \neq 0$ og $p(\alpha) = 0$, har vi, at $\ker \Phi \neq 0$, hvorpå $\mathrm{GF}(5)(\alpha) = \mathrm{GF}(5)[\alpha]$. $\ker \Phi$ er frembragt af et irreducibelt monisk polynomium med koefficienter i $\mathrm{GF}(5)$ – $\mathrm{Irr}(\alpha, \mathrm{GF}(5))$. Graden af dette er mindre end lig 3, thi vi ved, at $p(\alpha) = 0$.

Graden er nu ikke 0, da $\mathrm{Irr}(\alpha, \mathrm{GF}(5))$ da ville være invertibelt, hvilket er i modstrid med irreducibiliteten. Hvis graden var 1 eller 2, ville $\mathrm{Irr}(\alpha, \mathrm{GF}(5))$ være et første- eller andengradspolynomium med koefficienter i $\mathrm{GF}(5)$ med α som rod, og dette ville nødvendigvis være en divisor i p, thi $\ker \Phi$ er et hovedideal i $\mathrm{GF}(5)[x]$. Det ville medføre, at p havde en ikke-triviel faktorisering $p = g \cdot \mathrm{Irr}(\alpha, \mathrm{GF}(5))$, hvilket er i modstrid med, at p er irreducibel. Altså er $[\mathrm{GF}(5)(\alpha) : \mathrm{GF}(5)] = \deg \mathrm{Irr}(\alpha, \mathrm{GF}(5)) = 3$, og da p er af grad 3, monisk og irreducibel i $\mathrm{GF}(5)[x]$ med α som rod, må $p = \mathrm{Irr}(\alpha, \mathrm{GF}(5))$ jf. N s. 2.13.

$\mathrm{GF}(5)(\alpha)$ er altså et legeme med $5^3 = 125$ elementer, hvor ethvert element er på formen $a_0 + a_1\alpha + a_2\alpha^2$, hvor $a_0, a_1, a_2 \in \mathrm{GF}(5)$. Sæt $\alpha_2 = 3\alpha + 2\alpha^2$ og $\alpha_3 = -1 - \alpha - \alpha_2 = -1 + \alpha - 2\alpha^2$ (pr. N 2.59). Da elementer i $GF(5)(\alpha)$ er entydigt bestemt ved deres koefficienter, er α, α_2 og α_3 forskellige elementer i

GF(5)(α). Vi har nu, at

$$\begin{aligned}
& (x-\alpha)(x-\alpha_2)(x-\alpha_3) \\
= \; & (x-\alpha)(x+2\alpha-2\alpha^2)(x+1-\alpha+2\alpha^2) \\
= \; & (x-\alpha)(x^2+x-\alpha x+2\alpha^2 x+2\alpha x+2\alpha-2\alpha^2 \\
& \quad -\alpha^3-2\alpha^2 x-2\alpha^2+2\alpha^3+\alpha^4) \\
= \; & (x-\alpha)(x^2+(1-\alpha+2\alpha^2+2\alpha-2\alpha^2)x+\alpha+\alpha+\alpha^2+\alpha^3+\alpha^4) \\
= \; & (x-\alpha)(x^2+(1+\alpha)x+\alpha(1+\alpha)) \\
= \; & x^3+(1+\alpha)x^2+\alpha(1+\alpha)x-\alpha x^2-\alpha(1+\alpha)x-\alpha^2(1+\alpha) \\
= \; & x^3+x^2-\alpha^3-\alpha^2 \;=\; x^3+x^2+1=p(x).
\end{aligned}$$

Vi betragter altså legemsudvidelsen GF(5)(α,α_2,α_3) = GF(5)(α) over GF(5). Vi har, at p spaltes i lineære faktorer over GF(5)(α)[x]. Lad nu M være et ægte dellegeme af GF(5)(α), som indeholder GF(5). Da GF(5)(α) består af 125 elementer, er det isomorft med ethvert legeme med 125 elementer og vi kan betegne det GF(125) = GF(5^3). Pr. N 2.81 fås nu, at hvis vi har et legeme, der er isomorft med et dellegeme af GF(5^3), må det enten være GF(5) eller GF(5^3) selv, thi 1 og 3 er eneste positive divisorer i 3.

Da M var antaget at være et ægte dellegeme af GF(5)(α) $\simeq$ GF(5^3), som indeholdt GF(5), må følgelig gælde, at $M \simeq$ GF(5). Da vi viste i **(1)**, at p havde ingen rødder over GF(5), har p altså ingen rødder over M, og dermed kan p ikke spaltes i lineære faktorer i noget ægte dellegeme af GF(125) $\simeq$ GF(5)(α), som indeholder GF(5). Da må GF(5)(α) $\simeq$ GF(125) være spaltningslegemet for p over GF(5).

(3) *Hvorfor gælder, at p er divisor i $x^{125}-x$ i* GF(5)[x]*?*

Betragt den multiplikative gruppe GF(5)(α)* = GF(5)(α) $\setminus \{0\}$; denne har 124 elementer, og ethvert element heri har en orden, der er divisor i 124, således at $b^{124}=1$ for alle $b \in$ GF(5)(α)*. Altså er $b^{124}-1=0$ for alle $b \in$ GF(5)(α) $\setminus \{0\}$; alle $b \in$ GF(5)(α) $\setminus \{0\}$ er altså rødder i polynomiet $x^{124}-1 \in$ GF(5)(α)[x]. Dette giver, at alle $b \in$ GF(5)(α) er rødder i polynomiet $x(x^{124}-1) = x^{125}-x \in$ GF(5)(α)[x], hvorpå altså $b^{125}-b=0$ for alle $b \in$ GF(5)(α).

Betragt nu polynomiet $g(x)=x^{125}-x \in$ GF(5)[x]. Med homomorfien Φ fra **(2)** får vi nu, at $\Phi(g)=g(\alpha)=\alpha^{125}-\alpha=0$, thi $\alpha \in$ GF(5)(α). Altså får vi, at $g \in \ker\Phi = (\mathrm{Irr}(\alpha, \mathrm{GF}(5))) = (p)$. Altså har vi, at $g=fp$ for et $f \in$ GF(5)[x], hvorpå p går op i g.