MA2201 - ØVING 9

OLE FREDRIK BREVIG

Avsnitt 37

Oppgave 5. Vi vil vise at det ikke finnes noen simple grupper av orden $96 = 3 \cdot 2^5$. Vi ser på antall Sylow 2-undergrupper n. Har da at $n \equiv 1 \pmod 2$ og $n|96$. Følgelig er $n = 1$ eller $n = 3$. Vi antar 3, og da finnes to ulike Sylow 2-undergrupper H og K, slik at $|H| = |K| = 2^5$. Lemma 37.8 gir da at

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{2^{10}}{|H \cap K|} < 3 \cdot 2^5.$$

Hvorfor det? HK er kun en mengde!

Da vi har at $|H \cap K| \leq |H| = |K|$ er eneste mulighet at $|H \cap K| = 2^5$. Men da følger det at $H = K$. Antalgelsen om at vi har to ulike Sylow 2-undergrupper er derfor gal, og vi har kun en. Følgelig, ved andre Sylowteorem er denne normal. $\square$

Siden $H \neq K$ må $|H \cap K| = 2^4$ $\Rightarrow$ $H \cap K$ normal i H og i K $\Rightarrow N[H \cap K] = G$ ↯

Oppgave 7. Vi vil vise at hver gruppe G av orden ~~105~~ 30 har en undergruppe av orden 15. Jeg tror ikke min metode er akkurat det som er tiltenkt, men jeg klarer ikke finne noen feil i argumentasjonen. Dersom H og K er undergrupper av G, og H er normal vil mengden

$$HK = \{hk | h \in H \wedge k \in K\}$$

være en undergruppe av G. Dette holder da $kH = Hk$, for alle $k \in K$, da H er normal. Av eksempel 37.12 vet vi at vi har (minst) en undergruppe av orden 5 og (minst) en undergruppe av orden 3, hvor en av disse er normal. La H være den normale undergruppen, og K den andre. Lemma 37.8 gir

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{15}{|H \cap K|}.$$

Anta $a \in H$ og $a \in K$. Da må a ha orden 3 og 5 (da H og K har primtallsorden), som ikke er mulig. Altså har H og K kun identiteten til felles. Følgelig har vi at $|HK| = 15$, altså har vi funnet en undergruppe av orden 15. Bra!

Alternativt:
H normal i G
$|H| = 3 \Rightarrow |G/H| = \frac{|G|}{|H|} = 10$
Cauchy sier da at $\exists K \leq G/H$ der $|K| = 5$
$\gamma^{-1}[K] \leq G$
og $|\gamma^{-1}[K]| = 15$ osv..

Avsnitt 18

Oppgave 5. Vi vil beregne $(2, 3)(3, 5)$ i $\mathbb{Z}_5 \times \mathbb{Z}_9$. Vi har $2 \cdot 3 \equiv 1 \pmod 5$ og $3 \cdot 5 \equiv 6 \pmod 9$. Følgelig har vi at $(2, 3)(3, 5) = (1, 6)$.

Oppgave 6. Vi ønsker å beregne $(-3, 5)(2, -4)$ i $\mathbb{Z}_4 \times \mathbb{Z}_{11}$. Vi har at $-3 \cdot 2 \equiv 2 \pmod 4$ og $5 \cdot (-4) \equiv 2 \pmod{11}$, så har vi $(-3, 5)(2, -4) = (2, 2)$.

Oppgave 8. Vi vil undersøke om $\mathcal{R} = (\mathbb{Z}^+, +, \cdot)$, der $+$ og $\cdot$ er de vanlig addisjon og multiplikasjon. Vi vet at $(\mathbb{Z}^+, +)$ ikke er en gruppe, så følgelig er ikke $\mathcal{R}$ en ring.

Oppgave 11. Vi har $M = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Z}\}$ og vil undersøke om $\mathcal{R} = (M, +, \cdot)$ er en ring. Vi ser at $(M, +)$ er en abelsk gruppe, og da $a, b \in \mathbb{Z}$ vet vi multiplikasjon er assosiativitet, kommutativ og distributiv over addisjon. Følgelig er $\mathcal{R}$ en kommutativ ring med enhet $\mathbf{1} = 1 \in \mathbb{Z}$. Det er ikke en kropp da vi ikke har multiplikativ invers til f.eks. $a = 2$.

0 **Oppgave 13.** Mengden av alle rene imaginære tall ir, $r \in \mathbb{R}$ er en kropp. Dette følger direkte av at $\mathbb{R}$ er en kropp. ikke en ring!

$i \cdot i = -1$ ikke på formen $x \cdot i$, $x \in \mathbb{R}$

Oppgave 23. La $\phi : \mathbb{Z} \to \mathbb{Z}$ være en avbildning. For at dette skal være en ringhomomorfi må følgende oppfylles:

pr. def. så er $\varphi(1) = 1$ (def. av ring avbildning) og ergo er det kun en avbildning

(i) ϕ er en surjektiv.
(ii) ϕ er injektiv.
(iii) $\phi(a \cdot b) = \phi(a)\phi(b)$.
(iv) $\phi(a + b) = \phi(a) + \phi(b)$.

Vi ser på $\phi(x) = ax + b$. For at disse skal oppfylles må $b = 0$ og $|a| = 1$. Altså er mulighetne $\phi(x) = x$ og $\phi(x) = -x$. merk $\underbrace{\varphi(1)}_{=-1} = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) = (-1)^2 = 1$ motsigelse

Oppgave 28. Vi har ligningen $x^2 + x - 6 = (x-2)(x+3) = 0$ i $\mathbb{Z}_{14}$. Da må $x \equiv 2 \pmod{14}$ eller $x \equiv -3 \equiv 11 \pmod{14}$. Altså har vi løsningene $x_1 = \overline{2}$ og $x_2 = \overline{11}$. Hva med $x=4$ og $x=9$??

Oppgave 34. Vi lar $F = \{f : \mathbb{R} \to \mathbb{R}\}$. La $f, g, h \in F$. Vi har definert multiplikasjon ved $(fg)(x) = f(x)g(x)$. Vi vil vise at dette oppfyller visse ringaksiomer.

($\mathcal{R}_2$) Vi har at

$$((fg)h)(x) = (fg)(x)h(x) = f(x)g(x)h(x) = f(x)(gh)(x) = (f(gh))(x),$$

så multiplikasjonen er assosiativ.

($\mathcal{R}_3$) Videre ser vi at

ok

$$(f(g+h))(x) = f(x)(g(x) + h(x)) = f(x)g(x) + f(x)h(x) = (fg)(x) + (fh)(x).$$

Helt tilsvarende kan vi vise at $((f+g)h)(x) = (fh)(x) + (fg)(x)$.

Oppgave 35. Vi har $F = \{f : \mathbb{R} \to \mathbb{R}\}$, mengden av alle funksjoner fra de reelle tall til de reelle tall. Vi har også definert multiplikasjon ved $(fg)(x) = f(x)g(x)$. Så har vi avbildningen $\phi_a : F \to \mathbb{R}$ for $a \in \mathbb{R}$ ved $\phi_a(f) = f(a)$. Vi noterer at

$$\phi_a(fg) = (fg)(a) = f(a)g(a) = \phi_a(f)\phi_a(g),$$ ok

så ϕ_a oppfyller det multiplikative kravet til ringhomomorfier.

Oppgave 37. Vi lar U være samlingen av alle elementer med multiplikativ invers i en ring $(\mathcal{R}, +, \cdot)$ med enhet $\mathbf{1}$. Vi vil vise at $(U, \cdot)$ er en gruppe.

($\mathcal{G}_0$) La $a, b \in U$. Da har vi $a', b' \in \mathcal{R}$ slik at $aa' = \mathbf{1}$ og $bb' = \mathbf{1}$. Da vil

$$(ab)(b'a') = a(bb')a' = a\mathbf{1}a' = aa' = \mathbf{1}.$$

Følgelig har ab en multiplikativ invers i $\mathcal{R}$, og $ab \in U$. Altså er U lukket under $\cdot$.

($\mathcal{G}_1$) U er assosiativ da $\mathcal{R}$ er en ring.
($\mathcal{G}_2$) Da $\mathcal{R}$ har enhet $\mathbf{1}$ er $\mathbf{1} \in U$, og $e = \mathbf{1}$.
($\mathcal{G}_3$) La $a \in U$. Da $\exists a' \in \mathcal{R}$, den multiplikative invers, slik at $aa' = \mathbf{1} = a'a$. Men da er a den multiplikative inversen til a', og $a' \in U$, så alle inverser er med i U.

Følgelig er $(U, \cdot)$ en gruppe. ∎ ok

Oppgave 38. Vi vil vise at for $a,\, b \in \mathcal{R}$ holder likheten $a^2 - b^2 = (a+b)(a-b)$ hvis og bare hvis $\mathcal{R}$ er kommutativ. Vi noterer først at

$$(a+b)(a-b) = (a+b)\cdot a + (a+b)\cdot(-b) = a^2 + ab - ba - b^2. \tag{1}$$

Så har vi:

(i) Anta at $\mathcal{R}$ er kommutativ. Da har vi at $ab = ba$, for alle $a,\, b \in \mathcal{R}$. Følgelig, ved ligning (1) har vi

$$(a+b)(a-b) = a^2 + ab - ba - b^2 = a^2 + ab - ab - b^2 = a^2 - b^2.$$

(ii) Anta så at $a^2 - b^2 = (a+b)(a-b)$ for alle $a,\, b \in \mathcal{R}$. Da har vi, ved ligning (1) at

$$a^2 - b^2 = a^2 + ab - ba - b^2 \iff 0 = ab - ba \iff ab = ba,$$

og følgelig er $\mathcal{R}$ kommutativ.

$\square$

Oppgave 41. Vi vil vise at dersom p er et primtall og $a,\, b \in \mathbb{Z}_p$ har vi $(a+b)^p = a^p + b^p$. Da p er et primtall vet vi at $\mathbb{Z}_p$ er en kropp, så den er kommutativ. Da holder binomialteoremet i $\mathbb{Z}_p$. Videre noterer vi at for $n = 1, 2, \ldots, p-1$ vil $p \Big| \binom{p}{n}$. Følgelig vil $\binom{p}{n} \equiv 0 \pmod{p}$ for de samme n. Dette gir

$$(a+b)^p = \sum_{n=0}^{p} \binom{p}{n} a^{p-n} b^n \equiv \binom{p}{0} a^p + \sum_{n=1}^{p-1} 0 + \binom{p}{p} b^p = a^p + b^p \pmod{p}. \quad \square$$

Oppgave 43. La $\mathcal{R}$ være en ring med enhet $\mathbf{1}$, og $a \in \mathcal{R}$ være et element som har multiplikativ invers. Vi vil vise at denne er unik. Anta $b \neq b'$ er multiplikative inverser til a. Da har vi (spesielt) $ab = \mathbf{1}$ og $b'a = \mathbf{1}$. Dette gir at

$$b'(ab) = b'\mathbf{1} \implies (b'a)b = b' \implies \mathbf{1}b = b' \implies b = b',$$

så den multiplikative inversen er unik. $\square$

Oppgave 46. Vi lar $\mathcal{R}$ være en kommutativ ring og $a,\, b \in \mathcal{R}$ der $a^m = 0$ og $b^n = 0$. Da $\mathcal{R}$ er kommutativ holder binomialteoremet, og vi får

$$(a+b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^{m+n-k} b^k.$$

Anta det finnes et ledd i denne summen med potenser $a^r b^s$ der $r < n$ og $s < m$, men da vil $r + s < m + n$, som ikke stemmer da vi vet at $r + s = m + n - k + k = m + n$. Følgelig må enten $r \geq n$ og $s \geq m$, og følgelig er hvert ledd i summen 0, og vi har totalt 0. Altså er $(a+b)$ nullpotent dersom a og b er det. $\square$

Eksamen MA2201 vår 2006

Oppgave 3. Vi ser på $G = \mathrm{GL}(2, \mathbb{Q})$. Lar $r < s \in \mathbb{Q} - \{0\}$, og definerer

$$H_{r,\,s} = \{A \in G \mid \det(A) = r \text{ eller } \det(A) = s\}.$$

(a) Vi vil vise at $H_{r,\,s}$ er en undergruppe hvis og bare hvis $r = -1$ og $s = 1$. Vi har $e = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, og $\det(I_2) = 1$, så $r = 1$ eller $s = 1$. Anta $s = 1$. Da har vi B slik at $\det(B) = r > 1$, men dette impliserer at $\det(B^2) = r^2 \neq r$, da $r > 1$. Følgelig må $r = 1$. Anta så $\det(B) = s$. Da følger det (da inverser skal være med) at $\det(B^{-1}) = 1/s$. Da må $1/s = r$ eller $1/s = s$. Førstnevnte impliserer $r = s$ som ikke er mulig. Følgelig må $s = -1$. Altså har vi vist at eneste mulighet er $(r,\, s) = (-1,\, 1)$. Så må vi vise at dette faktisk gir en undergruppe.

($\mathcal{U}_1$) Vi ser at dersom A, $B \in H_{-1,1}$ har vi

$$\det(AB) = \det(A) \cdot \det(B) = (\pm 1)(\pm 1) = \pm 1,$$

så $AB \in H_{-1,1}$, så denne er lukket.

($\mathcal{U}_2$) Vi har allerede notert at $I_2 \in H_{-1,1}$.

($\mathcal{U}_3$) La $A \in H_{-1,1}$. Det er

$$\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{\pm 1} = \pm 1,$$

så følgelig er $A^{-1} \in H_{-1,1}$.

Følgelig er $H_{-1,1}$ en undergruppe.

(b) Vi vil vise at $H = H_{-1,1}$ er normal. La $A \in G$ og $X \in H$. Da har vi

$$\det(AXA^{-1}) = \det(A)\det(X)\frac{1}{\det(A)} = \det(X) = \pm 1.$$

Følgelig er $AXA^{-1} \in H$ for alle $A \in G$ og $X \in H$ og denne er normal. Vi vil så vise at faktorgruppen G/H er isomorf med gruppen $(\mathbb{Q}^+, \cdot)$. Vi vil altså finne en surjektiv homomorfi $\phi : G \to \mathbb{Q}^+$ der $\ker(\phi) = H$. Vi vet at $e \in \mathbb{Q}^+$ er $e = 1$. Følgelig vil det være naturlig å definere $\phi(A) = |\det(A)|$. Vi noterer denne er veldefinert, da $A \in G \implies |\det(A)| > 0$. Videre ser vi at for alle $k \in \mathbb{Q}^+$ eksisterer $M = \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}$, der $\phi(M) = |\det(M)| = k$, så ϕ er surjektiv. Videre noterer vi at

$$\phi(AB) = |\det(AB)| = |\det(A)\det(B)| = |\det(A)| \cdot |\det(B)| = \phi(A) \cdot \phi(B).$$

Følgelig er ϕ en homomorfi. Men da har vi at $G/\mathrm{Ker}(\phi) \simeq \mathrm{Im}(\phi)$ gir dette $G/H \simeq \mathbb{Q}^+$.

Oppgave 6. La G være en gruppe av orden $105 = 3 \cdot 5 \cdot 7$. Vi vil vise at G har en normal undegruppe. Ved Sylows tredje toerem har vi 1 eller 21 Sylow 5-grupper (av orden 5), og 1 eller 15 Sylow 7-undergrupper (av orden 7). Vi antar at vi har både 21 Sylow 5-undergrupper og 15 Sylow 7-undergrupper. Identiteten e er det eneste element som er med i mer enn én av disse gruppene.

- Anta $a \neq e$ er med i to Sylow 5-undergrupper. Da disse har orden 5 er de isomorfe med $\mathbb{Z}_5$ og derfor sykliske. Følgelig må de to undergruppene være like, da a er en generator for begge. Følgelig kan ikke a være med i to Sylow 5-undergrupper. Tilsvarende holder for Sylow 7-undergruppene.
- Anta $a \neq e$ er med i en Sylow 5-undergruppe og en Sylow 7-undergruppe. Da disse er sykliske må a ha orden 5 og 7, som ikke er mulig.

Følgelig har vi minst

$$1 + 21 \cdot (5-1) + 15 \cdot (7-1) = 175$$

elementer i G. Men dette er ikke mulig da $|G| = 105$. Følgelig må vi enten ha kun én Sylow 5-undergruppe eller én Sylow 7-undergruppe. Ved Sylows andre teorem vet vi at alle Sylow p-grupper er konjungerte. Altså, om H er en Sylow p-undergruppe vil $gHg^{-1} = H'$ være en Sylow p-undergruppe for alle $g \in G$. Men da vi bare har en slik gruppe H (for $p = 5$ eller $p = 7$), må $gHg^{-1} = H$ for alle $g \in G$, og følgelig er H normal.