

MAT220 HANDBOOK

4. juni 2015

Grupper

For aa være gruppe må et sett oppfylle 3 aksiomer:

G_1 : For alle $a, b, c \in G$ har vi at $(a * b) * c = a * (b * c)$ (Assositivitet)

G_2 : Det finnes et element e i G slik at for alle $x \in G$ saa $e * x = x * e = x$ (Identitets-elementet)

G_3 : Til hver element $a \in G$ finnes det et element a' i G slik at $a * a' = a' * a = e$ (Inversen til a)

Abelian: $ab = ba$

Non-abelian: $ab \neq ba$.

Normal Subgroup

Oppfyller en av disse kravene:

La $H \subset G$

H er da en normal subgruppe dersom $gHg^{-1} = H$, som er ekvivalent med at $gH = Hg^{-1}$

Factor groups / Quotient Groups

Dersom en subgruppe er normal vil cosetene danne en faktor gruppe.

En faktorgruppe er ett sett der elementene er sett. Dvs. at hvert element i settet er igjen et sett.

Isomorfisme

En gruppe $Z_m \times Z_n$ er syklisk og isomorfisk til Z_{mn} bare dersom m og n er relativt primsk. Altså dersom $\gcd(m, n) = 1$. (teorem 11.5, se side 106)

To sykliske grupper med samme orden er isomorfisk til hverandre. Det samme gjelder for to primtalls grupper av samme orden, der en primtalls gruppe er en gruppe der ordenen til gruppen er et primtall.

Order

Order i en gruppe

Order vil være antall elementer i en gruppe.

Sagt på en annen måte; det er antall ganger en må gå framover før en når identitets elementet.

Dermed, når en skal finne ordenen til et element i en gruppe er det du spør om hvor mange ganger du er nødt til å utføre gruppeoperasjonen på denne for å komme til identitets elementet.

Kort om order, fint forklart fra stackexchange:

The order of an element g in a group G is the smallest number of times that you need to apply the group operation to g to obtain the identity.

Let G be cyclic of order 35. That means that there is an element $g \in G$ with $g^{35} = e$, and that $g^k \neq e$ for all $1 < k < 35$. Now, consider $h = g^5$. Then $h^7 = (g^5)^7 = g^{35} = e$, but $h^k \neq e$ for all $1 < k < 7$, thus h has order 7. Similarly, the element g^7 has order 5.

Remark: Cauchy's theorem (which perhaps you did not see yet) states that if p is a prime dividing $|G|$, then G has an element of order p . Thus, the only finite groups where all elements except the identity have the same order are p -groups, namely groups whose order is a power of a fixed prime p . A group of size 35 is not a p -group.

Finn order til x i gruppe A

Formel: $\frac{\text{Order of}(A)}{\gcd(x, \text{Order of}(A))}$

Finn alle abelske grupper av orden X

Primtallfaktoriser X . Lagranges theorem brukes. Dette sier at ordenen til alle subgrupper til G vil kunne dividere ordenen til G .

Dermed vil alle grupper satt sammen av primtallene til X lage grupper av orden X .

Eksempel: Gi alle abelske grupper av orden 8:

Primtallfaktoriserer først $8 = 2 \times 2 \times 2$

Alle abelske grupper med orden 8 vil da være:

1. $Z_2 \times Z_2 \times Z_2$
2. $Z_4 \times Z_2$
3. Z_8

Hva er ordenen til (x,y) i $Z_a \times Z_b$

Finn ordenen til x i Z_a . Dvs, $\frac{a}{\gcd(x,a)}$. Finn saa ordenen til y i Z_b . Dvs, $\frac{b}{\gcd(y,b)}$
 Finn til slutt lcm av svarene.

Eksempel: $(10, 21)$ i $Z_{12} \times Z_{30}$ Ordenen til 10 i Z_{12} vil vaere:

$$\frac{12}{\gcd(10,12)} = \frac{12}{2} = 6$$

Videre er ordenen til 21 i Z_{30} lik:

$$\frac{30}{\gcd(21,30)} = \frac{30}{3} = 10$$

Ordenen til $(10, 21)$ i $Z_{12} \times Z_{30}$ er dermed $\text{lcm}(6, 10) = 30$

Homomorfisme og kernel

En mapping er homomorfisk dersom $\sigma(ab) = \sigma(a)\sigma(b)$ i multiplikativ notasjon og $\sigma(a + b) = \sigma(a) + \sigma(b)$ i additiv notasjon.

La G vaere en gruppe som blir mappet til H gjennom σ
 Kernel σ er da $\{g \in G | \sigma(g) = e_H\}$. Dvs alle elementer i G som mapper til identitets elementet til H .

Sylow Theoremer

Theorem 1

La G vaere en endelig gruppe. Dersom p er et primtall slik at p^k er en divisor for $|G|$ for en $k \geq 0$, vil G ha en subgruppe som har order p^k .

Eks: S_5 har order $5! = 5 * 4 * 3 * 2 * 1 = 5 * 2 * 2 * 3 * 2 = 5 * 3 * 2^3$. Det betyr at den inneholder 3 subgrupper med order 5, 3 og $2^3 = 8$.

Definisjon 1

La G vaere en endelig gruppe og la p vaere et primtall. En subgruppe P av G kalles ä Sylow p -subgroup ä G dersom $|P| = p^k$ for en integer $k \geq 1$ slik at p^k er en divisor for $|G|$ men p^{k+1} er ikke.

Eks: Vi tar igjen for oss $|S_5| = 5 * 3 * 2^3$. Denne har da en Sylow 2-subgruppe ettersom 2 er det eneste primtallet som opphøyes i noe høyere enn 1.

Theorem 2

La G være en endelig gruppe med order n og la p være et primtall.

Alle Sylow p -subgrupper av G er konjugate (http://en.wikipedia.org/wiki/Conjugacy_class) og enhver p -subgruppe av G finnes i en Sylow p -subgruppe.

Theorem 3

La $n = mp^k$ der $\gcd(m, p) = 1$ (dvs. at m og p er relativt primiske) og la s være antall Sylow p -subgrupper av G . Da vil $s|m$ og $s \equiv 1 \pmod{p}$ (n må kunne dele ordenen til den originale gruppe, dvs. bestaa av de andre primtallene i G . Dette betyr igjen at m er satt sammen av andre primtall i G .)

Det holder å sjekke om primtallene ulike fra p (altsaa de som er relativt primiske til p) kan settes sammen til noe som blir $1 \pmod{p}$. Da vil denne sammensetningen være antall p -grupper.

Folger av dette

La $p > 2$ være et primtall, og la G være en gruppe med order $2p$. Da er G enten syklisk eller isomorfisk til dihedral gruppen D_p av order $2p$.

La G være en gruppe av order pq hvor $p > q$ er primtall:

Dersom q ikke er en divisor av $p - 1$ s er G syklisk.

Dersom q er en divisor av $p - 1$ saa er enten G syklisk ellers er G generert av to elementer a og b som tilfredstiller disse kravene:

$a^p = e$, $b^q = e$, $ba = a^n b$ der $n \not\equiv 1 \pmod{p}$ men $n^q \equiv 1 \pmod{p}$.

Fin oppgave for å se dette i praksis er oppgave 4 i dette settet

<http://bit.ly/1ciHUTD>

Fasit: <http://bit.ly/1LJ2IjW>

Ringer/Rings

En ring $\langle R, +, * \rangle$ er bare et set R som har to operasjone istedenfor bare en (Slik grupper har). Kaller dem i framtidige eksempler for addering og multiplikasjon. For aa være en ring maa disse tre aksiomene oppfylles:

R_1 : $\langle R, + \rangle$ er en abelian gruppe (Det vil si at den maa oppfylle alle gruppe aksiomene under addisjon).

R_2 : Multiplikasjon er assosiativt.

R_3 : For alle $a, b, c \in R$ saa holder $a * (b + c) = (a * b) + (a * c)$ og $(a + b) * c = (a * c) + (b * c)$.

Legg merke til at en ring IKKE nødvendigvis trenger aa oppfylle følgende krav

- 1) Multiplisering kommutativ, dvs: $a * b = b * a$.
- 2) Multipliserings identitet
- 3) Multipliserings inverser.

Subring

For aa bevise at S er en subring av R maa en bevise følgende:

- 0) Vise at S faktisk er et subset av R (Er ofte obvious).
- 1) S er lukket under addisjon.
- 2) S er lukket under multiplikasjon.
- 3) S inneholder det adderende identitetselementet (0).
- 4) Alle elementer i S har en invers i S .

Protip: For aa bevise at noe er en ring kan en ofte kun bevise det som trengs for aa bevise at det er en subring, og dersom det da er et subset av noe en vet er en ring er det nok aa bevise.

Zero divisors og Integral domain

Zero divisor er tall ulik 0 som, naar de multipliseres, er lik 0 . Eks:

Hvis vi ser paa Z_{10} saa vil 5×4 være lik $20 \bmod(10) = 0$. Da, til tross for at hverken 5 eller 4 er 0 er resultatet 0 . 5 og 4 er da, sammen, zero divisors i Z_{10} .

Videre finnes det ringer der dette aldri skjer. (F.eks. R , Q og Z). Her kan aldri to elementer multiplisert sammen bli 0 . Disse ringene kalles INTEGRAL DOMAIN. Dette er den offisielle definisjonen:

En kommutativ ring med enhetselement og ingen zero divisors.

Subnote: Legg ogsaa merke til at alle Z_c der c ikke er et primtall har zero divisors, mens Z_p der p er et primtall er et integral domain.

Field (Kropp)

Et field er bare et integral domain hvor hvert non-zero element er en unit. En unit er hvilket som helst element som har en invers (multipliserende invers that is).

Eksempler paa field er \mathbb{R} og \mathbb{Q} . Da disse oppfyller alle integral domain kravene, men ogsaa oppfyller kravet om at alle elementer har en invers (sett bort ifra 0). \mathbb{Z} er ikke et field, da denne ikke inneholder noen multiplikativ invers for sine elementer.

Protip(theorem): Et endelig integral domain er alltid ett field.

Protip 2: La R vaere en ring og I vaere et maksimalt ideal for denne ringen. R/I er da en kropp/field.

Adjoint Field

Et adjoint field er naar en allerede har et ferdig field, si \mathbb{Q} , og oensker aa legge til et nytt element, si $\sqrt{2}$, men onsker at det fortsatt skal forbli et field. Da maa man ogsaa legge til flere elementer slik at aksiomene for field ikke brytes.

I dette eksempelet maa en f.eks. sørge for at alle tall som allerede er i \mathbb{Q} skal kunne adderes me $\sqrt{2}$ og fortsatt eksistere i settet.

I tillegg vil vi ogsaa at alle tall i \mathbb{Q} skall kunnes multipliseres me $\sqrt{2}$ og likevel eksistere i settet. Disse to egenskapene kan vi kombinere og vi faar da settet: $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$.

Legg merke til at dette ikke er en generell losning. Hvis vi ser p $\mathbb{Q}(\sqrt[3]{5})$ ser vi at $\sqrt[3]{5} * \sqrt[3]{5} = \sqrt[3]{5^2}$ som vi ikke kan uttrykke med elementer fra \mathbb{Q} . (gitt at vi bare kan multiplisere og addere). Dermed maa denne ogsaa legges til:

$$\mathbb{Q}(\sqrt[3]{5}) = \{a + b\sqrt[3]{5} + c\sqrt[3]{5^2}\}$$

Generelt: Legg til nye ledd (Multipliser med en konstant), der hvert ledd er tallet som skal legges til i fielden opphyd i en større enn den forrige, helt til dette tallet blir noe som allerede finnes i fielden.

Polynomer og saant

Vis at polynomet p er irreducible over \mathbb{Q}

Gauss' Lemma forteller oss for vise at et polynom er irreducible over \mathbb{Q} er det nok vise at det er irreducible over \mathbb{Z} . =i Vis at p er irreducible over \mathbb{Z} , da vil det vaere nok bevis for \mathbb{Q} .

Eisenstein's criterion: Polynomet er irreducibel dersom disse tre kravene er oppfylt (dette vil som regel være den som brukes oftest)

Dersom vi kan finne et primtall integer q slik at:

1. q er en faktor for hver ikke ledende koeffisient (dvs. alle konstanter som ikke er foran den x 'en med høyest opphøyning. I $5x^4 + 2x - 3$ er f.eks. 5 den ledende koeffisienten)
2. q er IKKE en faktor i den ledende koeffisienten
3. q^2 er ikke en faktor i konstanten.

Reduksjon mod(n): Dersom en modulerer polynomet over en viss n og viser at de da er irreducibelt over Z_n vil det bety at det også er irreducibelt over Z .

Eks: $t^4 - 15t + 7 \bmod(5) = t^4 + 2$. Dette skal da kunne reduseres til to faktorer der den ene er polynom grad 1 og den andre med grad 3. (Setter t utenfor)

Dvs: $(t - x)(t^3 \dots)$

Trenger da bare sjekke for alle tall a i Z_5 . $x \in Z_5$ er en rot. Dersom ingen av disse blir 0 finnes det ikke en rasjonell rot (det betyr et rasjonalt tall for x slik at polynomet = 0). Ser raskt at det ikke finnes en rot i Z_5 for $t^4 + 2$. Men dette beviser kun at det ikke kan faktoriseres på denne måten. (Det hadde vært nok dersom polynomet var av grad 3) Det kan fortsatt faktoriseres med to polynomer med grad 2:

$(t^2 \dots)(t^2 \dots)$. Denne er litt mer tricky. For å finne ut dette bruk metoden som blir beskrevet i denne videoen omtrent fra minutt 12

<https://youtu.be/ebwp4eqrOfg?t=12m32s>

Intuitiv forståelse av irreducible

At et polynom er irreducible i en viss gruppe betyr simpelthen at løsningen for x ikke finnes i gruppen. F.eks. hvis en ser på $x^2 - 3$ i $\mathbb{Q}[x]$ kan en raskt se at $\sqrt{3}$ er løsningen, noe som ikke er et rasjonalt tall ($\mathbb{Q}[x]$). Dermed er det irreducible.

Vis at polynom $p(x)$ er irreducible i Z_y

Dersom $p(a) \neq 0$ for alle $a \in Z$ er p irreducibelt.

(Dersom en modulerer polynomet med en integer m er det nok vise at formelen ovenfor da stemmer med dette nye polynomet i Z_m .)

Er $p(x)$ en generator for et maksimal ideal for $\mathbb{Q}[x]$

Dersom $p(x)$ er irreducibel i $\mathbb{Q}[x]$ betyr dette at $p(x)$ er en generator for et maksimal ideal.

Burnsides formel

Basically, det den gjør, er å finne antall orbits i en gruppe. Dersom G er en gruppe som inneholder ulike rotasjoner som: fiksert, roter 90 grader, roter 180, roter 170 grader, speil horisontal, vertikalt, begge diagonale. For hver av disse rotasjonene må en finne hvor mange elementer totalt som forblir fiksert når en gjør disse operasjonene. En tar så summen av dette og deler på alle de ulike rotasjonene. Veldig godt forklart i denne korte videoen: https://youtu.be/wdDF7_vfLcE

Formel som kan brukes:

Gitt ett alfabet med n bokstaver, og ett sirkelord med lengde m s finner en antall forskjellige sirkelord ved først finne gcd til alle tall i Z_m og m . S dersom $m=3$ s m en finne $\gcd(0,3) = x$, $\gcd(1,3) = y$, $\gcd(2,3)=z$. Deretter setter en disse verdiene som opphøyere for hver sin n , i denne:

$$\frac{1}{m}(n^x + n^y + n^z).$$

Fermats teorem

Dersom p er et primtall som ikke deler et heltall n vil p dele: $n^{p-1} - 1$