MAT220 HANDBOOK

27. mai 2015

Grupper

For aa vaere gruppe maa 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 $e * x = x * e = x$ (Identitetselementet) G_3: Til hver element $a \in G$ finnes det et elemen a' i G slik at $a * a' = a' * a = e$ (Inversen til a)

Abelian: $ab = ba$
Non-abelian: $ab \neq ba$.

Normal Subgroup

Skriv om dette!!

Factor groups

Skriv om dette!

Order

Order i en gruppe

Order vil vaere antall elementer i en gruppe.
Sagt paa en annen maate; det er antall ganger en maa gaa framover foer en naar identidets elementet.
Dermed, naar en skal finne orderen til et element i en gryppe er det du spoer om hvor mange ganger du er noddt til aa utfore gruppeoperasjonen paa denne for aa komme til identietselementet.

Kort om order, fint forklart fra stackexchange:
The order of an elements 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 $gk \neq e$ for all $1 < k < 35$. Now, consider $h = g^5$. Then $h^7 = (g^5)^7 = g^{35} = e$, but$hk \neq e$for all $1 < k < 7$, thus h has order 7. Similarly, the element g7 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: $\frac{Orderof(A)}{gcd(x,Orderof(A)}$

Finn alle abelske grupper av orden X

Primtallfaktoriser X. Lagranges theorem brukes. Dette sier at orderen til alle subgrupper til G vil kunne dividere orderen 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 forst $8 = 2 \times 2 \times 2$
Alle abelske grupper med order 8 vil da vaere:
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: $(10, 21)iZ_{12} \times Z_{30}$ Orderen til 10 i Z_12 vil vaere:
$\frac{12}{gcd(10,12)} = \frac{12}{2} = 6$
Videre er orderen til 21 i Z_{30} lik:
$\frac{30}{gcd(21,30)} = \frac{30}{3} = 10$
Orderen til $(10, 21)$ i $Z_{12} \times Z_{30}$ er dermed $lcm(10, 6) = 30$

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 k^p.
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-subgroupäv 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 opphoyes i noe hoyere enn 1.

Theorem 2

La G vaere en endelig gruppe med order n og la p vaere 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 primske) og la s vaere antall Sylow p-subgrupper av G. Da vil $s|m$ og $s \equiv 1(mod\ p)$

Folger av dette

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

La G vaere 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 $n \neq 1(mod\ p)$ men $n^q \equiv 1(mod\ p)$.

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

http://bit.ly/1ciHUTD
Fasit: http://bit.ly/1LJ2IjW

Ringer/Rings

En ring $< R, +, * >$ 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 vaere en ring maa disse tre aksiomene oppfylles:
R_1: ¡R, +¿ 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 nodvendigvis trenger aa oppfylle folgende 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 folgende:
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 vaere lik $20 \text{mod}(10) = 0$. 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

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 R og Q. Da disse oppfyller alle integral domain kravene, men ogsaa oppfyller kravet om at alle elementer har en invers (sett bort ifra 0). 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.

Adjoint Field

Et adjoint field er naar en allerede har et ferdig field, si Q, og oensker aa legge til et nytt element, si $\sqrt{2}$, men onsker at det forsatt 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. sorge for at alle tall som allerede er i Q skal kunne adderes me $\sqrt{2}$ og fortsatt eksistere i settet.
I tillegg vil vi ogsaa at alle tall i Q skall kunnes multipliseres me $\sqrt{2}$ og likevel eksistere i settet. Disse to egenskapene kan vi kombinere og vi faar da settet: $Q(\sqrt{2}) = \{a + b\sqrt{2}|a, b \in Q\}$.
Legg merke til at dette ikke er en generell losning. Hvis vi ser p $Q(\sqrt[3]{5})$ ser vi at $\sqrt[3]{5} * \sqrt[3]{5} = \sqrt[3]{5}^2$ som vi ikke kan uttrykke med elementer fra Q.(gitt at vi bare kan multiplisere og addere). Dermed maa denne ogsaa legges til:
$Q(\sqrt[3]{5}) = \{a + b\sqrt[3]{5} + c\sqrt[3]{5}^2\}$
Generelt: Legg til nye ledd (Multipliser med en konstant), der hvert ledd er tallet som skal legges til i fielden opphyd i en storre enn den forrige, helt til dette tallet blir noe som allerede finnes i fielden.

Polynomer og saant

Vis at polynomet p er irreducible over Q

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

Eisenstein's criterion: Polynomet er irreducibel dersom disse tre kravene er oppfyllt (dette vil som regel vaere 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 hyest opphyning. I $5x^4 + 2x - 3$ er f.eks. 5 den ledende koeffesienten)
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 irredusibelt over Z_n vil det bety at det ogsaa er irreducibelt over Z.
Eks: $t^4 - 15t + 7 \; mod(5) = t^4 + 2$. Dette skal da kunne reduseres til to faktorer der den ene er polynom grad 1 og det andre med grad 3.(Setter t utenfor)
Dvs: $(t - x)(t^3....)$
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 faktorieser p denne mten.(Det hadde vaert nok dersom polynomet var av grad 3) Det kan fortsatt faktoriseres med to polynomer med grad 2:
$(t^2....)(t^2...)$. Denne er litt mer tricky. For aa finne ut dette bruk metoden som blir beskrevet i denne videoen omtrent fra minutt 12
https://youtu.be/ebwp4eqrOfg?t=12m32s

Vis at polynom p(x) er irreducible i Z_y

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

Burnsides formel

Basically, det den gjor, er aa 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 maa en finne hvor mange elementer totalt som forblir fiksert naar en gjor disse operasjonene. En tar saa summen av dette og deler paa alle de ulike rotasjonene. Veldig godt forklart i denne korte videoen: https://youtu.be/wdDF7_vfLcE