Läsanvisning till Discrete matematics av Norman Biggs - 5B1118 Diskret matematik

Mats Boij

18 november 2001

13 Grupper

Det trettonde kapitlet behandlar *grupper*. Att formulera abstrakta begrepp som grupper har visat sig mycket kraftfullt. Man kan på det viset se vad som gäller för en mycket stor mängd till synes olika begrepp. Permutationer och modulär aritmetik visar sig på det viset ha något gemensamt.

Rekommenderade uppgifter

	lättare	svårare
13.1	1	
13.2	4	
13.3	1	3
13.4	1	
13.5	1	2
13.6	1	4
13.7	1,3	
13.8	2	
13.10	8	

13.1 Gruppaxiomen

Gruppbegreppet generaliserar flera av de saker vi sett tidigare. Mängden av alla permutationer under sammansättning bildar en grupp och heltalen under addition bildar en grupp, precis som heltalen modulo n under addition. Det definieras vad som menas med en *binär operation* på en mängd. Det är en regel som tar två element och ger tillbaka ett element. Exempel på binära operationer är addition, subtraktion och multiplikation av heltal, reella tal, eller något annat slags tal. Ett annat exempel är sammansättning av funktioner från en mängd till sig själv, speciellt permutationer.

Av de fyra gruppaxiomen som benämns **G1**, **G2**, **G3** och **G4** kan det första ibland uteslutas eftersom det kan anses vara en del av definitionen av vad en binär operation är. Det andra axiomet, *associativiteten* säger att vi kan utelämna parenteser när vi upprepar gruppoperationen, med andra ord kan vi definiera sammansättning av en hel följd element.

Det tredje säger att det finns ett element, e, som är neutralt för gruppoperationen. Detta element kallas *identitetselementet*, och man kan visa att det bara finns ett sådant element i en grupp. Ibland kan man även säga *enhetselement* (*eng. unit*).

Det fjärde axiomet säger att alla element i gruppen är inverterbara, dvs för a kan vi hitta a^{-1} så att $a * a^{-1} = e$ och $a^{-1} * a = e$.

Ordningen för en grupp är antalet element i gruppen. Detta skall inte blandas ihop med begreppet *multiplikativ ordning*, eller *ordningen av ett gruppelement* som betyder den minsta positiva potens av ett element som ger identitetselementet. Om gruppen är oändlig sägs den ha *oändlig ordning*.

Översättningar

group *grupp*
binary operation *binär operation*
closure *slutenhet*
associativity *associativitet*
identity *identitet*
inverse *invers*
order *orning*
infinite order *oändlig ordning*

13.2 Exempel på grupper

Symmetriska gruppen S_n har vi stött på tidigare. Det är mängden av permutationer av en mängd med n element och gruppoperationen är sammansättning. Ordningen av S_n är $n!$.

En annat exempel på grupper är *symmetrigrupper* för geometriska objekt. Det är *stelkroppsrotationer* som återför objektet på sig självt. Ett objekt som inte har någon symmetri har en *trivial* symmetrigrupp, dvs bara identitetselementet. I avnittet introduceras triangelgruppen G_Δ som är symmetrigruppen för en liksidig triangel. Den visar sig ha ordning sex.

Det andra exemplet använder sig av matriser. Eftersom matriser introduceras först i Matematik II kan det vara lika bra att hoppa över detta exempel. Annars kan man glömma bort matrisnotationen och bara tänka sig par av element i $\mathbf{Z}_3$, (a, b), där $a \neq 0$. Multiplikationen ges av $(a, b) * (c, d) = (ac, ad + b)$. Det visar sig att detta ger en grupp av ordning 6 med identitetselement $(1, 0)$.

Översättningar

symmetric group *symmetriska gruppen*
symmetries *symmetrier*
equilateral triangle *liksidig triangel*
group table *grupptabell*
matrix *matris*

13.3 Grundläggande algebra i grupper

Avsnittet bahendlar några grundläggande räkneregler i grupper. Det första som nämns är att man ofta inte skriver ut gruppoperationen som $*$ utan använder multiplikativ notation istället.

Sats 13.3.1 säger att vi alltid kan använda kancellering i grupper, både till vänster och till höger. I grupper är det viktigt att skilja på höger och vänster, eftersom de i allmänhet inte är *kommutativa*, dvs det är inte alltid sant att $ab = ba$. Om $ab = ba$ för alla a och b i en grupp kallas gruppen *abelsk* eller *kommutativ*.

En annan viktig observation är att grupptabellen alltid är en *latinsk kvadrat*, dvs varje symbol förekommer precis en gång i varje rad och varje kolonn. Däremot är det inte sant att alla latinska kvadrater är grupptabeller. De flesta latinska kvadrater har inte den associativa egenskapen som krävs för att det skall vara en grupptabell.

Sats 13.3.2 säger att vi alltid har en *unik* lösning till ekvationer som $ax = b$ där a och b är givna element i en grupp. Här konstateras också att gruppens identitetselement är entydigt bestämt, dvs det finns bara ett sådant, och även inversen till ett element är entydigt bestämd. Observera att detta inte ingår bland gruppaxiomen, utan är en följd av dem.

Översättningar

abstract algebra *abstrakt algebra*
commute *kommuterar*
commutative *kommutative*
abelian *abelsk*
latin square *latinsk kvadrat*

13.4 Ordningen av ett gruppelement

Här definieras *ordningen av ett gruppelement*. Det handlar om att ta potenser av element. Förr eller senare kommer man att komma till identitetselementet, i alla fall om gruppen är ändlig. Den minsta positiva potensen som ger identitetselementet kallas elementets ordning och skrivs $o(x)$ för ett element x.

Sats 13.4 säger att det följer att alla andra potenser som är lika med enhetelementet är multipler av ordningen, dvs $x^m = e$ medför att m är delbart med $o(x)$.

Översättningar

powers *potenser*
order *ording*
infinite order *oändlig ording*

13.5 Isomorfi av grupper

Isomorfi är ett viktigt begrepp inte bara för grupper. Det kommer att komma upp när det gäller både *ringar* i kapitel 15 och *grafer* i kapitel 10. Att två abstrakt definierade objekt är *isomorfa* betyder att de egentligen är exakt likadana. Det enda som skiljer dem är namnen på elementen.

När vi skall beskriva detta matematiskt blir det i form av en *bijektion*, f som dessutom *bevarar gruppstrukturen*, dvs uppfyller

$$f(a * b) = f(a) * f(b)$$

för alla a och b i G. En sådan bijektion kallas *isomorfi* av grupper.

Exemplet på isomorfi som ges i avsnittet bygger på de två exemplen från avsnitt 13.2. Det skulle också gå att byta ut matrisexemplet mot symmetriska gruppen S_3, eftersom den också är isomorf med triangelgruppen.

Översättningar

isomorphism *isomorfi*
isomorfic *isomorfa*

13.6 Cykliska grupper

Den första och viktigaste byggstenen när det gäller att konstruera grupper är de *cykliska grupperna*. Vi har stött på dem som de additiva grupperna $\mathbf{Z_n}$, men också genom cykliska permutationer. Om vi tar en cyklisk permutation av n element och dess potenser får vi en cyklisk grupp av ordning n.

Ett viktigt begrepp som kommer in är *generator*. Ett element a är en generator till en cyklisk grupp om gruppen består av alla potenser av a.

När vi pratar om potenser i grupper är det bra att komma ihåg att gruppoperationen inte alltid är multiplikation. Om gruppoperationen är addition motsvarar potenser multipler.

När vi sedan skall bygga upp något med de cykliska grupperna använder vi först *direkt produkt*. Det betyder att vi bildar en ny grupp $G \times H$ från två grupper G och H genom att ta produktmängden och använda gruppoperationerna oberoende av varandra på de olika komponenterna.

Exemplet visar vad som händer när vi bildar produkter av några olika cykliska grupper. Ibland visar det sig att resultatet blir en cyklisk grupp, ibland inte. Sats 13.6 talar om att vi kan få en isomorfi mellan en cyklisk grupp och en produkt av två cykliska grupper om ordningarna för faktorerna är relativt prima.

Översättningar

cyclic *cyklisk*
generate *generera*
infinite cyclic group *oändlig cyklisk grupp*
direct product *direkt produkt*

13.7 Delgrupper

När vi ska gå närmare in på strukturen hos grupper stöter vi på begreppet *delgrupp*. Det är en delmängd av en grupp som dessutom bildar en grupp med samma gruppoperation som den ursprungliga gruppen.

Sats 13.7 talar om att det finns två kriterier som tillsammans bildar nödvädniga och tillräckliga villkor för när en delmängd av en grupp skall vara en delgrupp. Det ena är att delmängden skall vara sluten under gruppoperationen, det andra är att den skall vara sluten under invers.

Om gruppen är ändlig räcker det första för att det skall vara en delgrupp, eftersom inversen av ett element då alltid är en potens av samma element.

Varje gång vi tar ett element a i en grupp så får vi en cyklisk delgrupp som genereras av a genom att ta mängden av potenser av a. Observera att vi även måste ta med de negativa potenserna om a har oändlig ordning. Ordningen av den delgrupp som genereras av a är lika med ordningen av a.

Översättningar

subgroup *delgrupp, undergrupp*
sufficient conditions *tillräckliga villkor*
centre *center*
cyclic subgroup *cyklisk delgrupp*

13.8 Sidoklasser och Lagranges sats

Lagranges sats visar styrkan i gruppbegreppet genom att det ger ett väldigt klart krav på ordningen för delgrupper i grupper. Från Lagranges sats följer sedan exempelvis Eulers sats.

Lagranges sats (Sats 13.8.2) säger att ordningen för en delgrupp måste dela gruppens ordning. Idén med beviset är att bilda en partition av gruppen i delar som alla är lika stora som delgruppen. Delarna i denna partition kallas *sidoklasser* och är i sig ett nyttigt begrepp. Eftersom gruppoperationen inte alltid är kommutativ skiljer vi på höger- och vänstersidoklasser.

Sats 13.4.3 är em följdsats, eller ett korollarium, till Lagranges sats, och den säger att gruppelementens orgningar måste dela gruppens ordning och att därmed $a^{|G|} = e$, för alla a i en ändlig grupp G. Det är detta som direkt ger Eulers sats när vi ser på gruppen av inverterbara element i $\mathbf{Z}_n$ som är en grupp av ordning $\phi(n)$.

Sats 13.4.4 är en annan följdsats som säger att det för varje primtal p bara finns en grupp upp till isomorfi, nämligen C_p. Alla grupper av ordning p är alltså cykliska.

Det sista exemplet, med delgrupperna till den alternerande gruppen A_4, visar att man kan ordna upp delgrupperna i ett *lattice*.

Översättningar

coset *sidoklass*
left coset *vänstersidoklass*
right coset *högersidoklass*
Lagrange's Theorem *Lagranges sats*
distinct *distinkta, olika*
index *index*
lattice *lattice, gitter*