Abstrakt algebra för gymnasister

Veronica Crispin Quinonez

Sammanfattning. Denna text är föreläsningsanteckningar från föredraget Abstrakt algebra som hölls under Kleindagarna på Institutet Mittag-Leffler 15-17 juni 2012.

1. Introduction

Vad betyder ordet "abstrakt" i uttrycket "abstrakt algebra"?

Enligt [**NE**] är *Abstraktion, en tankeprocess ... i vilken man bortser från vissa egenskaper ... och i stället uppmärksammar en eller några få egenskaper.* Den i detta sammanhang bästa beskrivningen finner jag dock hos Rydelius [**R**] när jag söker på ordet i Svenska Akademiens ordbok: *Genom det man bortlemnar kännemärken, (kan man) ifrån lägre begrepp uppstiga till högre, hvilket kallas logisk Abstraktion."* (Inom psykologin anser man att barnets förmåga till abstrakt tänkande börjar utvecklas vid elvaårsåldern.)

Med andra ord drar man ut (aritmetiska) egenskaper som en viss (tal-)mängd besitter, arbetar bara med dessa egenskaper, varefter de erhållna resultaten tillämpas på många fler mängder än bara de ursprungliga (tal-)mängderna.

2. Mängder och operationer

De vanligaste oändliga talmängderna är $\mathbb{N}$ − de naturliga talen (inklusive noll), $\mathbb{Z}$ − heltalen, $\mathbb{Q}$ − de rationella talen, $\mathbb{R}$ − de reella talen och $\mathbb{C}$ − de komplexa talen. Vi kan bilda andra mängder med hjälp av dessa, såsom $\mathbb{R} \setminus \{0\}$ − alla reella tal utom noll eller $\mathbb{Q}^+$ − alla de positiva rationella talen.

De första operationer som definieras i skolan är addition, subtraktion, multiplikation och division, även om man i själva verket arbetar med betydligt fler operationer men utan att vara medveten om dem.

DEFINITION 2.1. En mängd M sägs vara *sluten* under operationen $*$ om för varje elementpar a, b, där $a \in M$ och $b \in M$, så är resultatet av operationen $a * b$ återigen ett element i M.

EXEMPEL 2.2. Av mängderna som nämns i början av det här avsnittet är:

(1) alla utom $\mathbb{R} \setminus \{0\}$ slutna under addition;
(2) $\mathbb{N}$ och $\mathbb{Q}^+$ de enda som inte är slutna under subtraktion;
(3) alla slutna under multiplikation;
(4) bara $\mathbb{R} \setminus \{0\}$ och $\mathbb{Q}^+$ slutna under division; i mängderna $\mathbb{Q}$, $\mathbb{R}$ och $\mathbb{C}$ finns det ett enda element som gör att talmängden inte uppfyller kravet på slutenhet, men i $\mathbb{N}$ och $\mathbb{Z}$ kan man hitta oändligt många elementpar som ställer till det.

ÖVNING 1. Visa varför var och en av mängderna som nämns tidigare är eller inte är sluten under given operation.

Nedanstående exempel beskriver aritmetiska egenskaper hos de jämna talen, som vi lär oss ganska tidigt i grundskolan, med den abstrakta algebrans språk.

EXEMPEL 2.3. De jämna talen är slutna under addition, subtraktion och multiplikation, dock inte under division då, till exempel, $\frac{6}{2}$ är udda, $\frac{2}{6}$ icke är heltal och $\frac{2}{0}$ inte är definierat.

Följande exempel generaliserar exemplet i ett visst fall.

EXEMPEL 2.4. Låt S vara de heltal som får rest 1 vid division med 3, dvs tal på formen $x = 3n + 1$, där $n \in \mathbb{Z}$. S är då sluten under multiplikation, ty $(3n + 1)(3m + 1) = 9nm + 3n + 3m + 1 = 3(3nm + n + m) + 1$ får också rest 1 vid division med 3.

Naturliga frågor som en algebraiker då vill ställa är, bland annat:

(1) Givet en mängd M och en operation $*$, är M sluten under $*$?
(2) Om M inte är sluten under $*$, hur kan vi ändra på M för att göra den sluten under $*$?
(3) Givet M, vilka operationer finns det sådana att M är sluten under dem?

3. Binära operationer

I förra avsnittet har vi talat om operationer utan att egentligen ha definierat begreppet. Faktum är att vi bara har pratat om en typ av operationer som vi definierar på följande sätt.

DEFINITION 3.1. En *binär operation* på en mängd M är en regel som till varje ordnat par av element $a, b \in M$ tilldelar ett element i M, betecknat $a * b$.

De fyra grundläggande aritmetiska operationerna är så klart binära, men för att ge en bättre känsla för begreppet bör man alltid ge motexempel. I definitionen är några ord understrukna, och vi ska visa varför de är så väsentliga genom att ge exempel på operationer som inte är binära om vart och ett av de understrukna kraven inte uppfylls.

EXEMPEL 3.2. Det är viktigt att operationen är definierad för varje par. Betrakta mängden av alla ändliga vektorer och operationen addition. Då kan man inte addera två vektorer av olika storlek, säg, $(1, 2, 3)+(1, 2)$. För att fixa det, kan man i stället betrakta alla vektorer av samma storlek.

EXEMPEL 3.3. Ordningen av elementen är viktig, eftersom $3 + 4 \neq 4 + 3$.

EXEMPEL 3.4. Ordet binär indikerar just att det alltid rör sig om ett par element som man gör något med. En unär operation skulle kunna vara "kvadratroten ur" $\sqrt{}$ eller "fakulteten av" !, då man bara behöver ett enda tal för att dra roten ur det eller beräkna fakulteten av.

EXEMPEL 3.5. Låt $*$ definieras via $a * b$ = {ett heltal som är större än a och b}. Då kan vi ha både $2 * 3 = 4$ och $2 * 3 = 5$ och andra värden, och det finns inte ett enda bestämt värde på $2 * 3$, vilket gör operationen ganska omöjlig att arbeta med algebraiskt. Vi kan rätta till definitionen genom att tillägga "... det minsta heltal som är större ... ".

EXEMPEL 3.6. Det sista villkoret att resultatet av operationen ska återigen vara ett element i M är slutenhet. Varför den är viktig har vi sett tidigare.

Här följer exempel på binära operationer, som är mer eller mindre "naturliga".

EXEMPEL 3.7. .

(1) $\mathbb{N}$ och $a * b = \min(a, b) = \{$det minsta talet av a och $b\}$
(2) $\mathbb{N}$ och $a * b = a = \{$det första talet i talparet$\}$
(3) Mängden M bestående av alla funktioner, som är definierade på $\mathbb{R}$ och har värdemängd i $\mathbb{R}$, och operationen $+$ eller $\cdot$
(4) $\mathbb{N}^+$ och $a * b = a^b$ (varför är det viktigt att mängden bara består av positiva heltal?)

(5) $\mathbb{N}^+$ och $a * b = a \cdot b - a$
(6) $\mathbb{N}^+$ och $a * b = a \cdot b - 1$.

4. Egenskaper hos binära operationer

Nu är det dags att titta på fler begrepp som vi bekantade oss med redan i grundskolan: kommutativitet och associativitet.

DEFINITION 4.1. En binär operation $*$ på en mängd M kallas *kommutativ* om $a * b = b * a$ för alla $a, b \in M$.

EXEMPEL 4.2. Betrakta Exempel 3.7 (1). Operationen är kommutativ, eftersom det minsta talet är bestämt oavsett ordningen som talparet är presenterat i.

Operationen i Exempel 3.7 (2) är inte kommutativ, eftersom $3*5 = 3$ men $5 = 5 * 3$.

ÖVNING 3. Kontrollera alla de övriga operationerna i Exempel 3.7 med avseende på kommutativitet.

En binär operation kan naturligtvis appliceras flera gånger och då på fler än bara två element, men kan man göra det hursom helst? Vi vet att $(3+4)+2 = 3+(4+2)$, dvs att det inte spelar roll i vilken ordning vi summerar två tal i taget i en flertalssumma så länge ordningen mellan alla talen är densamma. Å andra sidan känner vi också till att $\frac{\frac{24}{6}}{3} \neq \frac{24}{\frac{6}{3}}$.

DEFINITION 4.3. En binär operation $*$ på en mängd M kallas *associativ* om $(a * b) * c = a * (b * c)$ för alla $a, b, c \in M$. För en sådan operation är uttrycket $a * b * c$ väldefinierat även utan parenteser.

EXEMPEL 4.4. För en godtycklig oändlig talmängd, låt $a * b = \frac{ab}{2}$. Det är lätt att se att operationen är kommutativ. Den är även associativ, eftersom $(a * b) * c = (\frac{ab}{2}) * c = \frac{\frac{ab}{2} \cdot c}{2} = \frac{abc}{4}$ och $a * (b * c) = a * (\frac{bc}{2}) = \frac{a \cdot \frac{bc}{2}}{2} = \frac{abc}{4}$. Observera att denna operation $*$ är baserad på den gamla bekanta multiplikationen och divisionen, och att vi använde deras egenskaper i vårt bevis.

EXEMPEL 4.5. Betrakta Exempel 3.7 (6). Enligt Övningen 3 är operationen $a * b = ab - 1$ kommutativ.

Vi ska visa att den inte är associativ, dvs att $(a*b)*c \neq a*(b*c)$. Vi har $(a * b) * c = (ab - 1) * c = ((ab - 1)c) - 1 = abc - c - 1$ men $a * (b * c) = a * (bc - 1) = (a(bc - 1)) - 1 = abc - a - 1$, vilket skulle bevisas.

Ett annat exempel på en kommutativ och icke-associativ operation är $a * b = 2^{ab}$. Visa det!

Två operationer som varken är kommutativa eller associativa hittar vi i Exempel 3.7 (4,5).

Ett givet exempel från universitetsmatematiken på en icke-kommutativ men associativ operation är matrismultiplikation, men kan vi hitta ett enklare exempel? Exempel 3.7 (2) är ett sådant. Det kan kännas konstruerat vid första anblicken, men hur kan man beskriva operationen "Ange x-koordinaten för en given punkt i xy-planet" med matematiska symboler? Jo, exakt så.

SATS 4.6. *Om $*$ är en associativ binär operation, så kommer operationen applicerad på fyra eller fler element ge samma resultat oavsett hur man placerar parenteserna.*

BEVIS. Satsen gällande fyra element säger att inga parenteser behövs i uttrycket $a * b * c * d$ eftersom associativiteten ger

$\big((a * b) * c\big) * d = [\text{ ty } (a * b) * c = a * (b * c)\ ] =$
$\big(a * (b * c)\big) * d = [\text{ låt } b * c = b'\ ] = a * \big((b * c) * d\big) =$
$a * \big(b * (c * d)\big) = [\text{ låt } c * d = c'\ ] = \big(a * b\big) * (c * d).$ □

Grupper

DEFINITION 4.7. En mängd G tillsammans med en binär operation $*$ kallas *grupp*, betecknat $\langle G, *\rangle$ om följande villkor är uppfyllda:

G_1 : $*$ är associativ
G_2 : det finns ett *identitetselement* $e \in G$ sådant att $e*x = x*e = x$ för alla $x \in G$
G_3 : till varje element $x \in G$ finns en *invers* $x' \in G$ sådan att $x * x' = x' * x = e$.

ANMÄRKNING 4.8. Man kan visa att identitetselementet är unikt liksom inversen till ett element.

EXEMPEL 4.9. Några välkända grupper är:

(1) $\langle \mathbb{Z},\ + \rangle$ med identitetselementet 0 och där inversen till ett tal är det motsatta talet
(2) $\langle \mathbb{R} \setminus \{0\},\ \cdot \rangle$ med identitetselementet 1 och där inversen till ett tal x är den multiplikativa inversen $\frac{1}{x}$
(3) $\langle \{\text{matriser av storlek } m\text{x}n\},\ + \rangle$ med identitetselementet nollmatrisen.

EXEMPEL 4.10. Nu ska vi konstruera en grupp. Vi tar $\mathbb{R}$ och hittar på operationen $a * b = a + b + ab$. För att avgöra om $\langle \mathbb{R}, * \rangle$ är en grupp behöver vi kontrollera alla tre villkoren.

G_1 : Algebraiska beräkningar visar att $*$ är associativ.

G_2 : För att hitta identitetselementet e löser vi ekvationen $e*x = x$, det vill säga $e * x = x \Leftrightarrow e + x + ex = x \Leftrightarrow e + ex = 0 \Leftrightarrow e(1 + x) = 0 \Rightarrow e = 0$ eftersom ekvationen ska gälla för alla x.

G_3 : Nu när vi vet att identitetselementet är 0, är det dags att hitta inversen till ett godtyckligt element x, dvs x' sådant att $x * x' = 0 \Leftrightarrow x + x' + xx' = 0 \Leftrightarrow x'(1 + x) = -x \Leftrightarrow x' = -\frac{x}{1+x}$. Det betyder att inversen till -1 med avseende på $*$ inte kan beräknas. Detta hinder fixar vi till genom att helt enkelt ta bort talet ur mängden.

Alltså, har vi konstruerat gruppen $\langle \mathbb{R} \setminus \{-1\},\ * \rangle$, där $a * b = a + b + ab$.

Några exempel på "icke-grupper" är:

$\langle \mathbb{N}, * \rangle$ där $a * b = ab - 1$ eftersom operationen inte är associativ enligt Exempel 4.5,

$\langle \mathbb{R} \setminus \{0\}, + \rangle$ eftersom identitetselementet saknas,

$\langle \mathbb{N}, + \rangle$ där alla positiva element saknar invers.

5. Gruppisomorfier

Två grupper $\langle G, * \rangle$ och $\langle H, \circ \rangle$ kallas isomorfa om elementen i den ena är precis elementen i den andra (möjligen med andra namn) och operationen $*$ motsvaras av operationen $\circ$. Med andra ord är grupperna identiska utom namnen på elementen och operationerna. Då finns det en så kallad bijektion, dvs en avbildning som bara byter namn på elementen, mellan grupperna.

Följande villkor kännetecknar en bijektion mellan två mängder. Man tänker sig att avbildningen går från den ena mängden till den andra mängden. I så fall motsvaras *varje* element i den andra mängden ett *unikt* element i den första mängden.

Exempel 5.1. Grupperna $\langle \mathbb{R}, + \rangle$ och $\langle \mathbb{R}^+, \cdot \rangle$ är isomorfa. Vi låter bijektionen, "namnbytesfunktionen", från $\langle \mathbb{R}, + \rangle$ till $\langle \mathbb{R}^+, \cdot \rangle$ definieras via $f(x) = e^x$. Vi behöver kontrollera att f verkligen är en bijektion:

(1) Om $x \neq y$ så är $f(x) = e^x \neq e^y = f(y)$. Alltså, två olika element $\mathbb{R}$ avbildas på två olika element i $\mathbb{R}^+$. Detta säkerställer villkoret "unikt".

(2) Givet ett $t \in \mathbb{R}^+$, är $t = e^{ln(t)} = f\big(\ln(t)\big)$, dvs "varje" element i $\mathbb{R}^+$ motsvaras av ett element i $\mathbb{R}$.

På vilket sätt motsvaras $+$ av $\cdot$? Först tar vi $x, y \in \mathbb{R}$ och tittar på deras motsvarigheter $e^x, e^y \in \mathbb{R}^+$. Om vi tar summan $x + y \in \mathbb{R}$, vilket element motsvarar den i $\mathbb{R}^+$? Vi har $f(x+y) = e^{x+y} = e^x e^y = f(x)f(y)$. Alltså motsvaras summan $\langle \mathbb{R}, + \rangle$ av en produkt i $\langle \mathbb{R}^+, \cdot \rangle$.

EXEMPEL 5.2. Gruppen $\langle \mathbb{Z}, + \rangle$ är isomorf med gruppen $\langle n\mathbb{Z}, 0 \rangle$, där n är ett positivt heltal, via bijektionen $f(x) = nx$.

Ibland är det svårt att hitta en bijektion, men det betyder inte att två grupper inte är isomorfa. Om man misstänker att två grupper inte är isomorfa, kan man försöka leta efter egenskaper som ena gruppen besitter, men inte den andra.

EXEMPEL 5.3. Grupperna $\langle \mathbb{R}, + \rangle$ och $\langle \mathbb{R} \setminus \{0\}, \cdot \rangle$ är inte isomorfa. I den första har ekvationen $x + x = a$ alltid en lösning $x = \frac{a}{2}$ för ett godtyckligt $a \in \mathbb{R}$. I den andra saknar ekvationen $x \cdot x = a$ lösning för exempelvis $a = -1$.

Om två eller flera grupper har samma egenskaper räcker det att studera ena gruppen. Genom att "dra ut" vissa egenskaper, som kanske många mängder har gemensamt, och arbeta med dem enbart kan man sedan tillämpa de resultat man får på alla mängderna utan att behöva studera varje mängd för sig.

För vidare läsning kan jag varmt rekommendera min första kursbok i abstrakt algebra [**F**].

6. Tillämpningar

Galoisteori är studie av så kallade Galoisgrupper. I den bevisar man bland annat att det inte går att hitta nollställen till ett polynom av femte och högre grad genom att bara använda de fyra aritmetiska operationerna och rötter av tal.

I gruppen Rubiks kub är elementen alla möjliga vridningar på en Rubiks kub. Om E är ursprungsläget och U är att vrida toppskiktet 90° medsols, då är $U * U * U * U = E$. Om D är att vrida bottenskiktet 90° medsols, så betyder $D * U$ att man först vrider toppskiktet och sedan bottenskiktet. Observera ordning som kommer från funktionsläran, jämför med $g(f(x))$, där man först applicerar funktionen f och sedan g. Läs gärna mer på
http://en.wikipedia.org/wiki/Rubik's_Cube_group

Inom kemi kan man studera symmetrier hos molekyler. Ett antal symmetriska rörelser eller vridningar tillsammans bildar en grupp. Läs mer på
http://en.wikipedia.org/wiki/Molecular_symmetry

Det är faktiskt även möjligt att addera punkter på en viss typ av kurvor, som kallas *elliptiska*, utan att blanda in koordinater. Denna addition går ut på att dra räta linjer mellan två punkter eller genom en punkt på kurvan. Sedan tittar man på om den räta linjen skär kuran i ytterligare en punkt på kurvan eller ej. Läs mer om detta på

http://en.wikipedia.org/wiki/Elliptic_curve#The_group_law

7. Övningar

Här kommer en mängd olika binära operationer att arbeta med på olika sätt: hitta mängder som är slutna under en given operation, avgöra om operationen är associativ etc.

(1) $a * b = a^b$
(2) $a * b = \frac{b}{a}$
(3) $a * b = \sqrt[b]{a}$
(4) $a * b = ab + a + b$
(5) $a * b = \frac{a+b}{2}$
(6) $a * b = \mid ab \mid$
(7) $a * b = \mid a + b \mid$
(8) $a * b = \mid a \mid \cdot b$
(9) $a * b = \sqrt{ab}$
(10) $a * b = \pi(a + b)$
(11) $a * b = \sqrt{a^2 + b^2}$
(12) $a * b = \pi b + a$
(13) $a * b = ab - 1$
(14) $a * b = \sqrt{a + b}$
(15) $a * b = \sqrt{b}$ Man kan undra om denna operation är unär, då man i praktiken bara arbetar med ett element, men eftersom det alltid finns två ingångsvärden, är operationen binär, även om man bortser från ena ingångsvärdet vid operationens utförande.

Referenser

[NE] Nationalencyklopedin http://www.ne.se
[F] Fraleigh, John B. *A First Course in Abstract Algebra, 7th Edition.*, Addison-Wesley 2003.
[R] Rydelius, Andreas. *Nödiga förnufftz öfvningar. 2 uppl. 1-5*, Linköping 1737.

Matematiska institutionen, Uppsala universitet
E-mail address: veronica.crispin@math.uu.se