GÖTEBORGS UNIVERSITET
MATEMATIK 1, MMG200, HT2016
INLEDANDE ALGEBRA

Övningshäfte 6:

Syftet med övningen är att

- utforska strukturen hos talsystemen under addition respektive multiplikation samt sambandet mellan den additiva och multiplikativa strukturen.
- introducera grupper, ringar och kroppar.

Övning N

1. Skriv upp ALLA formler och egenskaper du/ni känner till som handlar om addition, subtraktion, multiplikation och division. (Tillsammans bör ni komma på många!) Exempel på formler är $a + 0 = a$, $-(-a) = a$ och $a(b + c) = ab + ac$ där a, b och c betecknar tal ur någon talmängd.

   Vilka talmängder känner du till? Vad skiljer dessa talmängder åt? Vad är egentligen ett "tal"? Vad är addition, subtraktion, multiplikation och division?

2. Alla formler är inte oberoende av varandra. Försök att härleda ett par av de formler du fann ur några av de övriga.

Övning O

I denna uppgiften ska vi studera den additiva strukturen hos talmängder. Låt M vara en talmängd vilken som helst som har addition och antag att denna addition uppfyller följande fyra formler (axiom):

$$
\begin{aligned}
&(1) \quad \forall a, b \in M \ : \ a + b = b + a \\
&(2) \quad \forall a, b, c \in M \ : \ (a + b) + c = a + (b + c) \\
&(3) \quad \exists 0 \in M \, \forall a \in M \ : \ a + 0 = a \\
&(4) \quad \forall a \in M \, \exists - a \in M \ : \ a + (-a) = 0
\end{aligned}
$$

Med andra ord så antar vi att operatorn '+' är kommutativ, associativ, har identitet 0 och att ett godtyckligt element a har en invers $-a$.

Ur dessa formler kan vi t ex visa följande:

$$(5) \quad \forall a \in M \ : \ 0 + a = a$$

(6) $\forall a \in M \ : \ (-a) + a = 0$

(7) $\forall a, x, y \in M \ : \ a + x = a + y \Longrightarrow x = y$

(8) $\forall a \in M \ : \ -(-a) = a$

(9) $\forall a, b \in M \ : \ $ ekvationerna $a + x = b$ och $x + a = b$ har entydig lösning x.

(10) $\forall a, b \in M \ : \ -(a + b) = (-a) + (-b)$

1. Bevisa att formlerna (5)—(10) följer ur ENBART formlerna (1)—(4). Ange i varje steg vilken/vilka formler ni använder.

   De formler som ni nu bevisat utgör *satser* i en *teori* som har formlerna (1)—(4) som *axiom*. En mängd M med en operator '+' som uppfyller (1)—(4) kallas för en (kommutativ) grupp.

2. (a) Hur skulle man i denna teori kunna definiera subtraktion $a - b$ där $a, b \in M$?

   (b) Vad är skillnaden mellan minustecknet i de två olika sammanhangen $-a$ och $a - b$?

   (c) Diskutera formeln $a - b = a + (-b)$. Är detta en sats eller en definition?

Övning P

I denna uppgiften ska vi istället studera den multiplikativa strukturen hos talmängder. Låt M vara en talmängd vilken som helst som har multiplikation och antag att denna multiplikation uppfyller följande fyra formler (axiom):

$(1)'$ $\forall a, b \in M \ : \ a \cdot b = b \cdot a$

$(2)'$ $\forall a, b, c \in M \ : \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$

$(3)'$ $\exists 1 \in M \, \forall a \in M \ : \ a \cdot 1 = a$

$(4)'$ $\forall a \in M \setminus \{0\} \, \exists a^{-1} \in M \ : \ a \cdot a^{-1} = 1$

Med andra ord så antar vi att operatorn '$\cdot$' är kommutativ, associativ, har identitet 1 och att ett godtyckligt element $a \neq 0$ har en invers a^{-1}. Observera den stora likheten med den additiva strukturen.

Ur dessa formler kan vi t ex visa följande:

$(5)'$ $\forall a \in M \ : \ 1 \cdot a = a$

$(6)'$ $\forall a \in M \setminus \{0\} \ : \ a^{-1} \cdot a = 1$

$(7)'$ $\forall a \in M \setminus \{0\} \, \forall x, y \in M \ : \ a \cdot x = a \cdot y \Longrightarrow x = y$

$(8)'$ $\forall a \in M \setminus \{0\} \ : \ (a^{-1})^{-1} = a$

$(9)'$ $\forall a, b \in M \ : \ $ om $a \neq 0$ så har ekvationerna $a \cdot x = b$ och $x \cdot a = b$ entydig lösning x.

$(10)'$ $\forall a, b \in M \setminus \{0\} \ : \ (a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$

1. Bevisa att formlerna $(5)'$—$(10)'$ följer ur ENBART formlerna $(1)'$—$(4)'$. Ange i varje steg vilken/vilka formler ni använder. Observera att detta är helt analogt med uppgift 1 i Övning O.

2. Hur kan man definiera division a/b där $a, b \in M$ med $b \neq 0$? Varför får inte $b = 0$? Jämför med diskussionen i uppgift 2 i Övning O. Vilka likheter och skillnader finns det?

3. För vilka av talmängderna $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ och $\mathbb{C}$ gäller formlerna (1)—(4) respektive $(1)'$—$(4)'$?

4. Bland de formler som vi betraktat i samband med den additiva och den multiplikativa strukturen saknas vissa typer av formler. Vilka? (Vi har ju bara studerat dem *var för sig*.)

Övning Q

I denna uppgift ska vi introducera det viktiga algebraiska begreppet *grupp*. Kom ihåg att '$\star$' var en (binär) operator (man säger också att den är en operation) på en mängd M om det för alla $a, b \in M$ gäller att $a \star b \in M$. Vi gör nu följande definition:

Definition: En mängd M med en (binär) operator $\star$ kallas för en (kommutativ) *grupp* om operatorn är kommutativ, associativ, har en identitet (eller neutralt element) e och varje element i M har en invers, d v s:

$$
\begin{aligned}
&(1) \quad \forall a, b \in M \ : \ a \star b = b \star a \\
&(2) \quad \forall a, b, c \in M \ : \ (a \star b) \star c = a \star (b \star c) \\
&(3) \quad \exists e \in M \, \forall a \in M \ : \ a \star e = e \star a = a \\
&(4) \quad \forall a \in M \setminus \{0\} \, \exists a' \in M \ : \ a \star a' = a' \star a = 1.
\end{aligned}
$$

Vi kommer att skriva $\langle M, \star \rangle$ för att beteckna mängden M med operatorn $\star$.

Anmärkning: Normalt definierar man en grupp utan att kräva att operatorn är kommutativ. Vi kommer bara att titta på grupper där operatorn är kommutativ och kalla detta för en grupp. En grupp som är kommutativ brukar oftast kallas för en *abelsk grupp* efter den store norske matematikern Niels Henrik Abel.

1. Låt M vara någon av talmängderna $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ respektive $\mathbb{C}$.

   (a) På vilka av dessa talmängder är addition, subtraktion, multiplikation respektive division en operator.

   (b) För vilka av dem är $\langle M, + \rangle$ en grupp? Vilket element är identitet (neutralt element)? Vad innebär inverst element?

2. Vi ska nu titta på kongruenser modulo ett tal n och additionen som vi definierade tidigare. Vi ska beteckna mängden av klasserna modulo n med $\mathbb{Z}_n$, så att t ex är $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$. Ta fram tabellerna för addition modulo 5 och 6 som ni gjorde i en tidigare övning.

   (a) Man kan "direkt" ur tabellerna se att additionen uppfyller axiomen (1), (3) och (4) i definitionen av en grupp. Hur då?

(b) Hur skulle man kunna verifiera att den också uppfyller axiomet (2)? Försök göra detta.

(c) Ni har visat att $\langle \mathbb{Z}_5, + \rangle$ och $\langle \mathbb{Z}_6, + \rangle$ är grupper, eller hur? Gäller detta för alla $\langle \mathbb{Z}_n, + \rangle$? Hur skulle man kunna bevisa det?

3. Visa att följande satser alltid är sanna i en grupp $\langle M, + \rangle$:

   (1) $\forall a, x, y \in M \ : \ a \star x = a \star y \Longrightarrow x = y$

   (2) $\forall a \in M \ : \ (a')' = a$

   (3) $\forall a, b \in M \ : \ $ ekvationerna $a \star x = b$ och $x \star a = b$ har entydig lösning x.

   (4) $\forall a, b \in M \ : \ (a \star b)' = a' \star b'$

   Ange i varje steg vilka axiom ni använder. Obs: Jämför med bevisen ni gjorde i uppgift 1 i Övning O och Övning P. Det är i princip samma bevis!

4. Visa att identiteten (neutrala elementet) i en grupp är unikt.

5. Visa att för varje element i en grupp så är inversen unik.

6. (a) Visa att talmängderna $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ och $\mathbb{C} \setminus \{0\}$ är grupper med operatorn multiplikation.

   (b) Varför har vi tagit bort nollan?

   (c) Vilket element är identitet?

   (d) Vad innebär det inversa elementet?

   (e) Visa att $\mathbb{Z} \setminus \{0\}$ inte är en grupp.

Övning R

I denna uppgift ska vi introducera de viktiga algebraiska begreppen *ring* och *kropp*.

Vi har hittills studerat additiva och multiplikativa strukturer var för sig. För att t ex få vårt vanliga talsystem så måste vi koppla ihop de båda strukturerna. Detta sker med hjälp av den *distributiva lagen*.

Vi gör följande definition:

Definition: En mängd M med en operatorerna '$+$' och multiplikation '$\cdot$' är en (kommutativ) *ring* om

- $\langle M, + \rangle$ är en grupp med identitet 0.
- Multiplikationen är kommutativ, associativ och det finns en identitet 1.
- Distributiva lagen gäller:

$$\forall a, b, c \in M \ : \ a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

Vi betecknar att M har båda operatorerna med $\langle M, +, \cdot \rangle$.

Anmärkning: Normalt definierar man en ring utan att kräva att additionen är kommutativ. Vi kommer bara att titta på ringar där additionen är kommutativ och kalla detta för en ring

Observera att vi INTE kräver att det ska finnas inverser med avseende på multiplikation. Det är alltså inte givet att man kan "dividera" i en ring. Om man ökar på kraven ytterligare och kräver att alla element utom 0 ska ha invers med avseende på multiplikation så får man en *kropp*:

Definition: En mängd M med en operatorerna addition '$+$' och multiplikation '$\cdot$' är en *kropp* om den är en ring och alla element i $M \setminus \{0\}$ har en invers med avseende på multiplikation.

1. Direkt från definitionerna följer det att en kropp också är en ring. Varför det?
2. Vilka av talmängderna $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ och $\mathbb{C}$ är ringar? Vilka är kroppar?
3. Motivera att $\langle \mathbb{Z}_n, +, \cdot \rangle$ är en ring oavsett vad n är. (Här är additionen och multiplikationen så som vi definierat dem i tidigare avsnitt.) Vad är det man måste kontrollera? Kolla speciellt att den distributiva lagen gäller.
4. Visa att i en ring gäller följande satser:
   - $\forall a \in M \ : \ a \cdot 0 = 0$
   - $(-1) \cdot (-1) = 1$
   - $\forall a \in M \ : \ -(-a) = a$
   - $\forall a, b \in M \ : \ (-a) \cdot b = -(a \cdot b)$
   - $\forall a, b \in M \ : \ (-a) \cdot (-b) = a \cdot b$

   Markera i varje steg vilket axiom som används.
5. Visa att i en ring med minst två element så gäller att $0 \neq 1$. (Tips: Utnyttja den första satsen i förra uppgiften för något $a \neq 0$.)
6. Visa att om $\langle M, +, \cdot \rangle$ är en kropp så är $\langle M \setminus \{0\}, \cdot \rangle$ en grupp. (Inga räkningar behövs.)
7. Antag nu att $\langle M, +, \cdot \rangle$ är en godtycklig kropp. Då kan vi definiera de *inversa operationerna* subtraktion och division genom:

   $$a - b = a + (-b) \text{ och } \frac{a}{b} = a \cdot b^{-1}.$$

   Visa att följande gäller:

   (a) $(a - b) + (c - d) = (a + c) - (b + d)$

   (b) $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$ om $b, d \neq 0$

   (c) $(a - b) - (c - d) = (a + d) - (b + c)$

   (d) $\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a \cdot d}{b \cdot c}$ om $b, c, d \neq 0$

(e) $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$ om $b, d \neq 0$

Glöm inte att i varje steg ange vilket/vilka axiom som används.

8. Jämför i förra uppgiften de två första formlerna med varandra och den tredje med den fjärde. Vad ser ni? Är de relaterade på något sätt?

9. (a) Visa att $\langle \mathbb{Z}_6, +, \cdot \rangle$ inte är en kropp.

   (b) Visa att $\langle \mathbb{Z}_5, +, \cdot \rangle$ är en kropp.

   (c) För vilka n gäller det att $\langle \mathbb{Z}_n, +, \cdot \rangle$ är en kropp? Hur bevisar man det?

10. (a) Motivera att
$$R = \mathbb{Z}\left[\sqrt{2}\right] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$$
är en ring.

Vad är det man behöver kontrollera? Jo, att $0, 1 \in R$, att det finns en additiv invers i R till varje element i R och inte minst att addition och multiplikation är operatorer på R.

(b) Motivera att
$$\mathbb{Z}\left[\sqrt{2}\right] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$$
INTE är en kropp.

(c) Motivera att
$$\mathbb{Q}\left[\sqrt{2}\right] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$
är en kropp.

(d) Kan ni generalisera era bevis för att bevisa motsvarande resultat med 2 utbytt mot ett godtyckligt (positivt) heltal n?

Uppgifter ur boken som rekommenderas för självstudier:

Kapitel 8: 1abcdef, 7abd, 19abcd.