LEKTION 04-26

Idag definierar vi några algebraiska strukturen: Grupper, Ringer och kropp.

De alla består av en mängd med en *binära operation* som motsvarar några egenskaper.

Definition 0.1. Låt A vara en mängd. En binär operation $*$ på A ër en funktion:

$$* : A \times A \to A$$

Exempel:

- $+, \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.
- Låt $M_k(\mathbb{R})$ vara mängden av $n \times n$ matriser med reella koefficienter. Matris multiplikationen definierar en binära operation.

$$\cdot : M_k(\mathbb{R}) \times M_k(\mathbb{R}) \to M_k(\mathbb{R})$$

- Additionen och multiplikationen modulo n definierar binära operationer på $\mathbb{Z}_n$.

$$+, . : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$

- Divisionen INTE definierar en binär operation på $\mathbb{Z}$.
- Låt $S(A) = \{f : A \to A \text{ så att } f \text{ är surjektiv}\}$. Sammansättning

$$\circ : S(A) \times S(A) \to S(A)$$

definierar en binär operation. Vi ska visa att $\circ$ definiera en binär operation på $S(A)$, dvs att sammansättning av två surjektiva funktioner är surjektiva. Låt f, g vara två surjektiva funktioner och betrakta $a \in A$. Vi ska visa att det finns $b \in A$ så att $f(g(b)) = a$. Eftersom f, g är surjektiva finns det $c \in A$ så att $a = f(c)$ och $b \in A$ så att $c = g(b)$.

Det följer att $\circ$ definierar en binär operation på $S(A)$.

Definition 0.2. En *grupp* definieras som ett par $(G, *)$ där G är en mängd och $*$ är en binär operation med följande tre egenskaper:

(G1) Operationen är **associativ**:

$$(a * b) * c = a * (b * c) \text{ for varje } a, b, c \in G$$

(G2) Det finns ett **noll** element:

$$\text{det finns ett element } 0 \in G \text{ så att } 0 * g = g * 0 = g \text{ for varje } g \in G$$

(G3) varje element har en **invers**:

for varje element $g \in G$ det finns ett element $g' \in G$ så att $g * g' = g' * g = 0$

Exempel:

- $(\mathbb{Z}, +)$ är en grupp. $(\mathbb{Z}, \cdot)$ INTE är en grupp. Låt $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, då är $(\mathbb{Q}^*, \cdot)$ en grupp. Är $(\mathbb{Z}^+, +)$ en grupp?
- $(M_k(\mathbb{R}), \cdot)$ är en grupp. Noll elementet är den identitet matrisen, I_n, och inversen av en matris, M, är den inversmatris M^{-1}.
- $(\mathbb{Z}_n, +)$ är en grupp. Noll element är klassen $[0]$ och invers av element $[x]$ är klassen $[n - x]$.

  Betrakta nu $\mathbb{Z}_n$ med multiplikationen. Är den en grupp? Man kan hytta en nollelement, nämlingen $[1]$. Men man kan hytta en invers bara till inverterbara element, d.v.s $[a] \in \mathbb{Z}_n$ där $gcd(a, n) = 1$.

  Man ser att alla element blir inverterbara när n är ett primtal. Dessutom vi ska ta borta element $[0]$, den har ingen invers. Låt $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, då är $(\mathbb{Z}_p^*, \cdot)$ en grupp för varje primtal p.
- Betrakta mängden $S(A)$ med den sammansättning operationen. (G1) gäller. Identitet funktionen id_A är en noll-element, då gäller (G2). Finns det en inversfunktion till alla funktioner?

  Vi har tidigare visat att bara injektiva funktioner har en invers. Det betyder att $(S(A), \circ)$ är inte en grupp.

  Kan vi definiera en grupp genom att betrakta en delmängd av $F(A)$?

  Låt $B(A) = \{f : A \to A$ så att f är bijektiv$\}$. Är $\circ$ en binär operation på $I(A)$? Vi ska visa att sammansättningen at två injektiva funktioner är fortforande injektiv. Anta att f, g är injektiva och att $f \circ g(a) = f \circ g(b)$. Det betyder att $f(g(a)) = f(g(b))$ och då, eftersom f är injektiv, $g(a) = g(b)$. Men g är också injektiv så att $a = g$.

  Det följer att $(B(A), \circ)$ är en grupp.

Definition 0.3. En grupp $(G, *)$ kallas en *abelska grupp* om operationen är kommutativ, dvs

$$\text{(G4) } a * b = b * a \text{ för alla } a, b \in G$$

Exempel.

- $(\mathbb{Z}, +), (\mathbb{Q}^*, \cdot)$ är abelska grupper.
- $(M_k(\mathbb{R}), \cdot)$ INTE är en abelsk grupp.
- $(\mathbb{Z}_n, +)$ är en abelsk grupp.

Vi ska nu definiera vad betyder att en grupp H kan tänkas som en delgrupp av en grupp G.

Definition 0.4. Låt $(G, *)$ vara en grupp. En *delgrupp* av G består av ett par $(H, *)$ där:

- $H \subseteq G$ är en delmängd.
- Operationen $*$ är "sluten" på H :

  $$* : H \times H \to H, \text{ dvs att } h_1 * h_2 \in H \text{ för varje } h_1, h_2 \in H$$

  och $(H, *)$ är en grupp

Exempel

- $(\mathbb{Q}_+, \cdot)$ är en delgrupp till $(\mathbb{Q}^*, \cdot)$.
- Låt $(G, *)$ vara en grupp och $g \in G$. Man kan definiera en delgrupp från g, den kallas den *delgruppen som genereras av* g:

$$< g >= \{g^n | n \in \mathbb{Z}\}$$

Här $g^n = g * g * ... * g$ n gånger.

Säkert är $< g >$ en dälmängd av G, varje potens av g finns i G enligt binär operationen. Man ska visa att operationen $*$ är sluten på $< g >$. Låt g^n, g^m vara två element i $< g >$, vi har att

$$g^n * g^m = g^{n+m} \in < g >$$

Definition 0.5. En grupp $(G, *)$ är ändlig om G är en ändlig mängd.

Grupperna $(\mathbb{Z}_n, +)$ och $(\mathbb{Z}_p^*, \cdot)$ är bland de viktigaste ändliga grupper.

Definition 0.6. En grupp $(G, *)$ kallas en *cyklisk grupp* om den genereras av ett element: $G =< g >$.

Exempel.

- $(\mathbb{Z}, +) =< 1 >=< -1 >$
- Om $G = (< g >, *)$ är en ändlig cyklisk grupp då måste det finnas ett tal n sådan att $g^n = 1$, där 1 är nollelement i gruppen.

$$G = \{1, g, g^2, g^3, ..., g^{n-1}\}$$

Det betyder att $|G| = n$. Heltalet n kallas *ordningen* av element g, $ord(g)$.

Betrakta gruppen $(\mathbb{Z}_n, +)$. Den är en cyklisk ändlig grupp:

$$(\mathbb{Z}_n, +) = (< [1] >, +) \text{ och } ord([1]) = n$$

- Betrakta gruppen $(\mathbb{Z}_6, +)$. Hur många delgrupper finns?

  Eftersom denna ër en cyklisk grupp vi ska bästemma alla möjliga cykliska delgrupper.
  - $H_0 =< [0] >= \{[0]\}$, $ord([0]) = 1$;
  - $< [1] >= \mathbb{Z}_6$, $ord([1]) = 6$;;
  - $H_2 =< [2] >= \{[2], [4], [0]\}$, $ord([2]) = 3$;
  - $H_3 =< [3] >= \{[3], [0]\}$, $ord([3]) = 2$;
  - $< [4] >= H_2$, $ord([4]) = 3$;
  - $< [5] >= \mathbb{Z}_6$, $ord([5]) = 6$;

Om vi fixar en delgrupp, t.ex. $(H, *) \subset (G, *)$ kan vi definiera dess *sydokalsser* for varje $g \in G$:

$$g * H = \{g * h | h \in H\}$$

Sydoklasser av H_2 i $\mathbb{Z}_6$ är

- $0 + H_2 = 2 + H_2 = 4 + H_2 = \{[4], [0], [2]\} = H_2$;

- $1 + H_2 = \{[3], [5], [1]\} = 3 + H_2 = 5 + H_2$

Vi ser att $\mathbb{Z}_6 = (0 + H) \cup (1 + H)$.

Det kan man visa för all grupper:

$$G = H \cup g_1 * H \cup ... \cup g_k * H \text{ för några } g_1, ..., g_k \in G$$

där unionen består av disjunkta mängder (dvs att denna är en partition av mängden G). Dessutom är alla dessa sydoklasser like stora,

$$|H| = |g_i * H| \text{ för alla } i = 1, ..., k$$

Det följer att:

LAGRANGES SATS Om H är en delgrupp av gruppen G då måste kardinaliteten av H, $|H|$, dela kardinaliteten av G, $|G|$.

Exempel Enligt Lagranges Sats har $(\mathbb{Z}_p, +)$ bara två delgrupper:

$$< [1] >= \{[1]\} \text{ och } \mathbb{Z}_p =< [n] > \text{, för } n = 2, ..., p - 1$$