

Ugeseddel 2.

Program. I den anden uge, 10/2-14/2, er overskriften „Grupper“, med materiale fra TAL6 og GRP1. Ugens øvelser er TAL2: 5, 9, 10, 12, 13, 14; TAL3: 2, 4, 6, 7, 10, 12. De markerede opgaver er til skriftlig aflevering til instruktorene.

I den første uge gennemgik jeg TAL 1-6, excl. (6.14)-(6.15). TAL3 og TAL6 er egentligt eksamenspensum, resten er kursorisk. Af kursorisk opgivet stof forudsættes kendskab til resultaterne, men ikke kendskab til beviser og bevismetoder.

Nøgleord: komposition, kommutative lov, associative lov, inverst element, distributive lov, nul-reglen, relation, symmetrisk, asymmetrisk, transitiv, reflexiv, irreflexiv, Velordningsprincippet, Induktionsprincippet, Princippet om fuldstændig induktion, divisor, multiplum, division med rest, største fælles divisor, Euklid's algoritme, primisk, printal, primdivisor, primopløsning, ækvivalensrelation, klassesdeling, kongruens modulo n , restklasser, principal rest.

Kommentar. Det er jo et helt overvældende antal nøgleord, men du kender vist de fleste i forvejen.

Kuglerne.

• *Samtlige divisorer* kan man let bestemme, når n er primopløst, $n = p_1^{v_1} \cdots p_r^{v_r}$. De positive er netop tallene af formen $d = p_1^{\delta_1} \cdots p_r^{\delta_r}$, hvor $0 \leq \delta_i \leq v_i$.

• *En primisk restklasse*, for et givet n , er en restklasse $A = [a]_n$, hvor $(a, n) = 1$. De primiske restklasser er netop de invertible restklasser, dvs de restklasser A for hvilke der findes en restklasse X med $AX = [1]_n$. Med \mathbb{Z}/n betegnes mængden af restklasser modulo n , og med $(\mathbb{Z}/n)^*$ betegnes delmængden bestående af primiske restklasser.

• *Euler's φ -funktion* $\varphi(n)$ tæller antallet af primiske restklasser. Det er antallet af tal a , med $0 \leq a < n$, som er primiske med n , og altså lig med elementantallet i mængden $(\mathbb{Z}/n)^*$.

• *Den kinesiske restklassesætning* fortæller, at det at give en restklasse A modulo $364 = 52 \cdot 7$ er det samme som at give et par (A_1, A_2) , hvor A_1 er en restklasse modulo 7 og A_2 er en restklasse modulo 52. „Er det samme som“ udtrykker, at der er en naturlig bijektiv forbindelse mellem de to slags ting, givet ved en bijektiv afbildning fra $\mathbb{Z}/364$ til $\mathbb{Z}/52 \times \mathbb{Z}/7$. Afbildningen er bestemt ved $[a]_{364} \mapsto ([a]_{52}, [a]_7)$. Den er bijektiv fordi 7 og 52 er primiske, $(7, 52) = 1$.

• *Grupper findes overalt.* Det er simpelthen formålet med GRP1 at bevise denne påstand. Du kender formodentlig definitionen på en gruppe. Her er nogle af de grupper, man møder i GRP1:

- (1) $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+, \mathbb{C}^+$,
- (2) $\mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$,
- (3) $\mathbb{Z}_+^*, \mathbb{Q}_+^*, \mathbb{R}_+^*, \mathbb{C}_+^*$ (næh, den sidste går ikke!),
- (4) \mathbb{U} er gruppen af komplekse enheder,
- (5) $C_1 = \{e\}$ og $C_2 = \{\pm 1\}$ er grupper med ét og to elementer,

10. februar 2003

- (6) \mathbb{Z}/n af orden n , $(\mathbb{Z}/n)^*$ af orden $\varphi(n)$, S_n af orden $n!$, C_n af orden n ,
- (7) $GL_n(\mathbb{R})$ er den generelle lineære gruppe af invertible $n \times n$ -matricer med reelle koefficienter; beslægtede grupper: $GL_n(\mathbb{Q})$, $GL_n(\mathbb{C})$, og(?) $GL_n(\mathbb{Z})$,
- (8) og $SL_n(\mathbb{C})$, $SL_n(\mathbb{R})$, \dots , $O_n(\mathbb{R})$, $O_n(\mathbb{Q})$, \dots ,
- (9) og hvad med $GL_n(\mathbb{Z}/k)$, $SL_n(\mathbb{Z}/k)$, $O_n(\mathbb{Z}/k)$,
- (10) diedergruppen D_n består af symmetrierne af en regulær n -kant,
- (11) $\text{Perm}(X)$ eller S_X , gruppen af permutationer, eller transformationer, af en given mængde X ,
- (12) og V , *Klein's Vierer-gruppe*.

Er du klar over hvad notationen dækker?

Klein's Vierer-gruppe V omtales overalt i bogen som Vier-gruppe, men Klein sagde faktisk 'der Vierer'. Det er en gruppe af orden 4, hvor alle elementerne har sig selv som det inverse. Den møder man som den som den multiplikative gruppe $(\mathbb{Z}/8)^*$ bestående af restklasserne af 1, 3, 5, 7 modulo 8.

Hvornår var det nu det var? Leonhard Euler 1707-83, Christian Klein 1849–1925.

På sigt: I den tredie uge, 17/2-21/2, er overskriften „Permutationer og cykliske grupper“, fra GRP2-3. Ugens øvelser er: TAL3: 5, 11, 14; TAL6: 5, 6, 7, 10*; GRP1: 5, 9, 11, 12, 13, 14.

Opgaven med * er ugens *nød*.

Anders Thorup