

Session 1-2.

Velkommen til Algebra 1. Kurset har en hjemmeside:

<http://www.math.ku.dk/kurser/2008-09/blok4/alg1/>

Her kan du finde oplysningerne om kurset. Med mellemrum, typisk inden hver uges undervisning, lægger jeg en ugeseddel – som denne – ud på nettet; de udleveres også ved forelæsningerne. De fortæller bl.a. lidt om hvad der lige er foregået, og om hvad der planlægges i den nærmeste fremtid. Videre fremhæves på sedlerne – lidt uformelt – nogle aktuelle hovedresultater fra noterne. Endelig vil der være diverse kommentarer og oplysninger. Jeg er i øvrigt Anders Thorup, og jeg kan træffes på H. C. Ørsted Institutet (lokale E209), tlf 35320749, e-mail: <thorup@math.ku.dk> — eller privat, tlf 44653153.

Program. Den første tirsdag, T21/4, har overskriften „Cyklisk gruppe, Sideklasse“, på baggrund af GRP1-4. Normalt slutes tirsdagene med en „prøv-dig-selv“-session, men denne første tirsdag bliver virkelig hård: Der er forelæsninger både kl 8.15–10.00 og kl 13.45–15.30. Dagens øvelser er GRP3: 1, 3, 4, 5, 8, 9, 10, 15, 16.

Fredagen, F24/4, har overskriften „Normal undergruppe, homomorfi, isomorfi“ fra GRP4-5. Nogle af sætningerne springer vi over. Dagens øvelser er GRP4: 1, 2, 4, 5, 7, 10, 11, 12, 13, 14, 21*

Nøgleord: Ugesedlen vil i reglen indeholde en liste over *nøgleord*. Det er ord, som dækker begreber, der har været omtalt. Det er en god og vigtig øvelse, at du ord for ord gennemgår listen: har du en klar fornemmelse af hvad ordet dækker, – eller kan du i det mindste genkende ordet? Her er en række nøgleord fra Dis1, dvs fra bogens kapitler om TAL, og GRP1-2. Det er sundt at gennemgå den, men den er godt nok lang!

Primisk restklasse, Euler's φ -funktion, Den kinesiske Restklassesætning, gruppe, neutralt element, inverst element, kommutativ eller abelsk, gruppes orden, multiplikativ og additiv notation, undergruppe, den trivielle gruppe, komplekse fortegn \mathbb{U} , enhedsrødder, den cykliske gruppe C_n , den identiske afbildning, transformationsgruppe, permutationsgruppe, generelle lineære gruppe GL_n , specielle lineære gruppe SL_n , ortogonal afbildning, ortogonale gruppe O_n , drejning, spejling, regulær n -kant, symmetri, diedergruppen D_n , kvaterniongruppen Q_8 . permutation, permutationsgruppe, identiteten, den symmetriske gruppe S_n , fixpunkt, disjunkte permutationer, p -cykel, cykelnotation, transposition, baner for permutation, cykelfremstilling, Cykelsætning, cykeltype, dobbelttransposition, fortegn, lige og ulige permutation, den alternerende gruppe A_n .

Kommentar. Cykliske grupper er de enkleste grupper: De består udover det neutrale element e af et element g og alle potenser g^n . Enhver gruppe G er fuld af cykliske undergrupper: Tag bare et element g ud af gruppen, og betragt alle g 's potenser. Og i enhver cyklisk gruppe C af orden n har man fuldt overblik over samtlige undergrupper: De er alle selv cykliske og der er præcis én af orden d for hver divisor d i n .

I GPR4 bruges det fundamentale tælleprincip: Når en mængde G er delt i klasser, kan man tælle elementerne i G ved at tælle antallet af elementer i klasserne og lægge disse antal sammen. Elementært, ikke? Men dette enkle princip er grundlaget for næsten al

17. april 2009

kombinatorik. Og i hvert fald er det grundlaget for Lagrange's Indexsætning og dermed for vores bevis for Fermat's lille Sætning og Euler's generalisering. Fermat's store sætning siger i øvrigt, at ligningen $x^n + y^n = z^n$, for en eksponent $n \geq 3$, ikke har løsninger med naturlige tal x, y, z .

Kuglerne.

- *Fortegnet* for permutationer, $\text{sign}: S_n \rightarrow \{\pm 1\}$ opfylder, at $\text{sign}(\sigma\mu) = \text{sign}(\sigma)\text{sign}(\mu)$ og at en p -cykel har fortegnet $(-1)^{p-1}$. Og så behøver man ikke at vide meget mere om fortegnet.
- *En lige cykel er ulige!* Hvad menes der mon med det? Og er det rigtigt?
- *Ordenen* af en potens bestemmes ved en formel: Hvis g har orden n , så har g^i orden $n/(n, i)$, hvor (n, i) er den største fælles divisor for n og i .
- *Om undergrupper* i en cyklisk gruppe af orden n ved man alt: De er selv cykliske, deres orden er divisor i n , og for hver divisor $d | n$ findes der præcis én af orden d .
- *Lagrange's Indexsætning.* $|G| = |G:H| \cdot |H|$. Konsekvens: ordenen af H er divisor i ordenen af G .
- *Der er kun én* gruppe af orden p , hvor p er et primtal, nemlig den cykliske gruppe C_p .
- *Korollar til Lagrange.* Med $n := |G|$ er $g^n = e$ for alle $g \in G$.
- *Euler's Sætning.* $(a, n) = 1 \implies a^{\varphi(n)} \equiv 1 \pmod{n}$.
Fx: $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$, så $2^8 = 256 \equiv 1 \pmod{15}$.
- *Fermat's lille sætning.* For et primtal p gælder: $p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$.
Fx: $2^{10} = 1.024 \equiv 1 \pmod{11}$.

Hvornår var det nu det var? Pierre de Fermat 1601–1665, Joseph-Louis Lagrange 1736–1813, Leonhard Euler 1707–1783,

På sigt: Tirsdag i næste uge, T28/4, er overskriften „Isomorfi, Struktursætning“, med materiale fra GRP5-6; øvelserne er GRP3: 12; GRP4: 8, 16, 24*; GRP5: 1, 2, 3, 5; GRP6: 1, 5. De markerede opgaver er til skriftlig aflevering til instruktoren.

Anders Thorup