Algebra
Cheatsheet

20094480 - Roberto Trifiletti

13. juni 2012

Indhold

Talteori (1) **10**

Mængderne $\mathbb{N}$ og $\mathbb{Z}$ (1.1) . . . 10
Division med rest (1.2) . . . 10
Entydig rest . . . 10
Def. 1.2.2 . . . 10
Restklasse . . . 10
Kongruenser (1.3) . . . 10
Kongruens . . . 10
Prop. 1.3.2 . . . 10
Prop. 1.3.4 . . . 11
Reference (1.2) . . . 11
Supp. Noter 1.3 . . . 11
"Repeated squaring" . . . 11
Største fælles divisor (1.4) . . . 11
Lemma 1.4.2 . . . 11
Største fælles divisor . . . 11
Euklids algoritme (1.5) . . . 11
Prop. 1.5.1 . . . 11
Lemma 1.5.7 . . . 12
Indbyrdes primisk . . . 12
Kor. 1.5.10 . . . 12
Generalisering af Kor. 1.5.11 (supp. noter) . . . 12
Den kinesiske restklassesætning (1.6) . . . 12
Def. 1.6.1 . . . 12
Lemma 1.6.3 . . . 13
Den kinesiske restklassesætning . . . 13

Eulers phi-funktion (1.7) . . . 13
Prop. 1.7.1 . . . 13
Eulers sætning . . . 13
Primtal (1.8) . . . 14
Primtal . . . 14
Lemma 1.8.1 . . . 14
Euklids sætning . . . 14
Def. Tvillingeprimtal . . . 14
Lemma 1.8.3 . . . 14
Entydig primtalsfaktorisering . . . 14
Bemærkning 1.8.6 . . . 14
RSA (1.9) . . . 15
Prop. 1.9.1 . . . 15
Fermats lille sætning . . . 16
Pseudoprimtal . . . 16
Lemma 1.9.4 . . . 16
Stærkt pseudoprimtal . . . 16
Prop. 1.9.6 . . . 17
Sætning 1.9.7 (Rabin) . . . 17
Kvadratiske rester (1.11) . . . 17
Kvadratisk rest . . . 17
Bemærkning ang. restklasser . . . 17
Prop. 1.11.3 . . . 17
Sætning 1.11.1 . . . 17
Kor. 1.11.5 . . . 18
Prop. 1.11.6 . . . 18
Lemma 1.11.10 . . . 18
Kor. 1.11.11 . . . 18
Loven for kvadratiske reciprokker . . . 18
Metode til at udregne $\left(\frac{a}{p}\right)$ . . . 18

Grupper (2) **20**

Indledende gruppeteori (2.1) . . . 20
Komposition . . . 20
Gruppe . . . 20
Def. 2.1.7 . . . 20
Finde inversen til et produkt . . . 20
Kompositionstabel (2.1.2) . . . 20

Gruppen S_3 . . . 20
Multiplikation med $g \in G$ er bijektiv . . . 21
Prop. 2.1.2 . . . 21
Undergrupper (2.2) . . . 21
Undergruppe . . . 21
Prop. 2.2.3 . . . 22
Sideklasse . . . 22
Lemma 2.2.6 . . . 22
Kor. 2.2.7 . . . 22
Lagranges sætning . . . 23
Index . . . 23
Normale undergrupper (2.3) . . . 23
Komposition for delmængder af en gruppe . . . 23
Prop. 2.3.1 . . . 23
Normal undergruppe . . . 23
Kor. 2.3.3 . . . 23
Kvotientgruppe . . . 24
Lemma 2.3.6 . . . 24
Kvotientgruppen $\mathbb{Z}/n\mathbb{Z}$ . . . 24
Primiske restklasser $(\mathbb{Z}/n\mathbb{Z})^*$ . . . 24
Supplement til 2.3. Lemma 1 . . . 24
Supplement til 2.3. Lemma 2 . . . 25
Gruppehomomorfier (2.4) . . . 25
Gruppehomomorfi . . . 25
Prop. 2.4.9 . . . 25
Gruppeisomorfi . . . 25
Isomorfisætningen . . . 25
Orden af et element i en gruppe (2.6) . . . 26
Prop. 2.6.1 . . . 26
Ordnen af et element . . . 26
Prop. 2.6.3 . . . 26
Supplement til 2.6 . . . 26
Cykliske grupper (2.7) . . . 27
Cyklisk gruppe . . . 27
Prop 2.7.2 . . . 27
Prop 2.7.4 . . . 27
Kor. 2.7.6 . . . 27
Grupper og tal (2.8) . . . 27

Produktgrupper . . . 27
Lemma 2.8.1 . . . 28
Symmetriske gruppe (2.9) . . . 28
Def. 2.9.1 . . . 28
Prop 2.9.2 . . . 28
k-cykel . . . 28
Ordnen af en cykel . . . 29
Prop 2.9.5 . . . 29
Prop 2.9.6 . . . 29
Lemma 2.9.8 . . . 29
Transposition . . . 29
Simpel transposition . . . 29
Bubble sort . . . 29
Inversion . . . 30
Prop 2.9.12 . . . 30
Lemma 2.9.13 . . . 30
Lemma 2.9.14 . . . 30
Def. 2.9.15 . . . 30
Prop 2.9.16 . . . 30
Den Alternerende gruppe . . . 31
Prop 2.9.17 . . . 31
Simpel gruppe . . . 31
Lemma 2.9.18 . . . 31
Sætning 2.9.19 . . . 31
Lemma 2.9.20 . . . 31
Gruppevirkninger (2.10) . . . 31
Gruppevirkning . . . 31
Def. 2.10.2 . . . 32
Prop. 2.10.5 . . . 32
Kor. 2.10.7 . . . 32
Lemma 2.10.8 (Burnside) . . . 32
Konjugering . . . 33
p-gruppe . . . 33
Prop. 2.10.13 . . . 33
Kor. 2.10.14 . . . 34
Kor. 2.10.15 . . . 34
Sylow p-undergruppe . . . 34
Sætning 2.10.17 (Første Sylow Sætning) . . . 34

Sætning 2.10.18 (Anden Sylow Sætning) . . . 34
Sætning 2.10.19 (Tredje Sylow Sætning) . . . 34
Supplement til 2.10. Lemma 1 . . . 34
Supplement til 2.10. Korrolar . . . 35
Supplement til 2.10. Observation . . . 35
Supplement til 2.10. Lemma 2 . . . 35

Ringe (3) **36**
Def. Ring (3.1) . . . 36
Ring . . . 36
Delring . . . 36
Nuldivisor . . . 36
Enhed . . . 36
Def. 3.1.1 . . . 37
Legeme . . . 37
Integritetsområde . . . 37
Del - og udvidelseslegeme . . . 37
Prop. 3.1.3 . . . 37
Prop. 3.1.4 . . . 37
Talmængerne $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$ . . . 37
Ideal . . . 37
Ideal frembragt af en mængde . . . 38
Bemærkning 3.1.6 . . . 38
Bemærkning 3.1.7 . . . 38
Bemærkning 3.1.8 . . . 38
Hovedideal . . . 38
Hovedidealområde . . . 38
Prop. 3.1.10 . . . 39
Sætning 3.1.11 . . . 39
Kvotientringe (3.2) . . . 39
Kvotientring . . . 39
Kvotientringe i $\mathbb{Z}$ . . . 39
Prop. 3.2.2 . . . 39
Prop. 3.2.3 . . . 39
$\mathbb{F}_p$ . . . 39
Primideal . . . 40
Maksimalt ideal . . . 40
Maksimale idealer i $\mathbb{Z}$ . . . 40

Ringhomomorfier (3.3) . . . 40
Ringhomomorfi . . . 40
Ringisomorfi . . . 40
Kerne og billede af Ringhomomorfi . . . 40
Prop. 3.3.2 . . . 41
Entydig ringhomomorfi fra $\mathbb{Z}$ . . . 41
Bemærkning 3.3.4 . . . 41
Karakteristik af en ring . . . 41
Lemma 3.3.5 . . . 41
Prop 3.3.7 . . . 41
Lemma 3.3.8 . . . 42
Freshman's Dream . . . 42
Bemærkning 3.3.10 . . . 42
Entydig faktorisering (3.5) . . . 42
Associerede elementer . . . 42
Irreducibelt element . . . 42
Entydig faktorisering til irreducible elementer . . . 43
Faktoriel ring . . . 43
Primelement . . . 43
Prop. 3.5.2 . . . 43
Prop. 3.5.3 . . . 43
Bemærkning 3.5.4 . . . 43
Lemma 3.5.5 . . . 43
Prop. 3.5.6 . . . 43
Sætning 3.5.7 . . . 43
Euklidisk ring . . . 44
Prop. 3.5.9 . . . 44
De Gaussiske heltal $Z[i]$ . . . 44
Prop. 3.5.11 . . . 44
Lemma 3.5.12 (Lagrange) . . . 44
Korollar 3.5.14 . . . 44
Sætning 3.5.15 (Fermat) . . . 44
Lemma 3.5.18 . . . 44
Ringklasser . . . 45

Polynomier (4) **46**

Polynomiumsringe (4.1) . . . 46
Polynomiumsring . . . 46

Bemærkning 4.1.3 . . . 47
Division af Polynomier (4.2) . . . 47
Prop. 4.2.2 . . . 47
Prop. 4.2.3 . . . 47
Prop. 4.2.4 . . . 47
Korollar 4.2.5 . . . 47
Def. 4.2.7 . . . 47
Polynomiumsrødder (4.3) . . . 48
Prop. 4.3.1 . . . 48
Rod . . . 48
Korollar 4.3.2 . . . 48
Multiplicitet af en rod . . . 48
Multipel rod . . . 48
Lemma 4.3.4 . . . 48
Sætning 4.3.5 . . . 49
Differentiering af polynomier . . . 49
Lemma 4.3.7 . . . 49
Lemma 4.3.8 . . . 49
Bemærkning 4.3.9 . . . 49
Cyklotomiske polynomier (4.4) . . . 50
Enhedsrod . . . 50
Lemma 4.4.1 . . . 50
Bemærkning . . . 50
Cyklotomisk polynomium . . . 50
Prop. 4.4.3 . . . 50
Primitive rødder (4.5) . . . 51
Primitiv enhedsrod . . . 51
Lemma 4.5.2 . . . 51
Sætning 4.5.3 (Gauss) . . . 51
Idealer i polynomiumsringe (4.6) . . . 51
Prop. 4.6.1 . . . 51
Prop. 4.6.3 . . . 51
Prop. 4.6.7 . . . 52
Bemærkning 4.6.8 . . . 52
Endelige legemer (4.8) . . . 52
Lemma 4.8.1 . . . 52
Sætning 4.8.2 . . . 52
Lemma 4.8.3 . . . 52

Sætning 4.8.5 . . . 53

Gröbner baser (5) **54**

Polynomier i flere variable (5.1) . . . 54

Termordning . . . 55

Leksikografisk ordning . . . 55

Graderet leksikografisk ordning . . . 55

Lemma 5.1.5 (Dickson) . . . 55

Korollar 5.1.7 . . . 55

Initialterm (5.2) . . . 56

Initialterm . . . 56

Bemærkning 5.2.3 . . . 56

Divisionsalgoritmen (5.3) . . . 56

Prop. 5.3.1 . . . 56

Def. 5.3.2 . . . 56

Gröbnerbaser (5.4) . . . 57

Gröbnerbasis . . . 57

Prop. 5.4.2 . . . 57

Korollar 5.4.5 . . . 57

Prop. 5.4.6 . . . 57

Sætning 5.4.7 . . . 57

Korollar 5.4.8 . . . 58

S-polynomiet . . . 58

Newton Genvisit (5.5) . . . 58

Sætning 5.5.1 . . . 58

Buchbergers S-kriterie (5.6) . . . 58

Korollar 5.6.9 . . . 58

Buchbergers algoritme (5.7) . . . 58

Sætning 5.7.2 . . . 58

Den reducerede Gröbnerbasis (5.8) . . . 59

Minimal Gröbnerbasis . . . 59

Reduceret Gröbnerbasis . . . 59

Sætning 5.8.3 . . . 59

Løsning af ligningssystemer vha Gröbnerbaser (5.9) . . . 59

Sætning 5.9.1 . . . 59

Appendix (6) **60**

Talteori (1) . . . 60

Induktionsprincippet . . . 60

Reference (1.1) . . . 60
Grupper (2) . . . 60
Veldefineret . . . 60
Injektiv . . . 60
Surjektiv . . . 60
Bijektiv . . . 60
Ker(f) . . . 61
f(G) . . . 61
Gröbnerbaser (5) . . . 61
Relation . . . 61
Ækvivalensrelation . . . 61
Partiel ordning . . . 62
Minimalt element . . . 62
Første element . . . 62
Total ordning . . . 62
Velordning . . . 62
$\langle f_1, \ldots, f_m \rangle$ . . . 62

Eksamen (7) **63**

Den kinesiske restklassesætning . . . 63
$\varphi(n)$ . . . 63
Normafbildning . . . 63
Vis at R ikke er et Hovedidealområde . . . 64
Antallet af frembringere i L^* . . . 64
Simple transpositioner . . . 64

Talteori (1)

Mængderne $\mathbb{N}$ og $\mathbb{Z}$ (1.1)

Se bogen.

Division med rest (1.2)

Entydig rest

Sætning 1.2.1: Lad $d \in \mathbb{Z}$, hvor $d > 0$. For alle $x \in \mathbb{Z}$ er der en entydig rest $r \in \mathbb{N}$ sådan at:

$$x = qd + r,$$

hvor $q \in \mathbb{Z}$ og $0 \leq r < d$.

Dvs. at når vi dividerer et helt tal med d vil der altid være en entydig rest, r hvor der gælder at $0 \leq r < d$.

Def. 1.2.2

Antag $a = bc$, hvor $a, b, c \in \mathbb{Z}$.

Vi siger så at c er en divisor i a. Dette skrives $c \mid a$.

Restklasse

Def. 1.2.3: Hvis $x, d \in \mathbb{Z}$, hvor $d > 0$, lader vi

$[x]_d$ udtrykker den Entydig rest r, efter division med d.

Bemærk at $[x]_d$ *er en mængde. Den består af alle tal der har denne rest efter division med d. x kaldes her repræsentanten for restklassen.*

Kongruenser (1.3)

Kongruens

Def. 1.3.1: Lad $a, b, c \in \mathbb{Z}$. Så er a og b kongruente modulo c hvis $c \mid b - a$.

Dette skrives $a \equiv b \pmod{c}$.

Prop. 1.3.2

Lad $c \in \mathbb{Z}$, hvor $c > 0$. Så gælder:

(i) $a \equiv [a]_c \pmod{c}$

(ii) $a \equiv b \pmod{c} \iff [a]_c = [b]_c$

Altså a er kongruent til sin egen entydige rest divideret med c (mod c) og a er kongruent med b $\iff$ *de entydige rester for a,b divideret med c er lig hinanden*

Prop. 1.3.4

Antag $x_1 \equiv x_2 \pmod{d}$ og $y_1 \equiv y_2 \pmod{d}$. Så gælder:

(i) $x_1 + y_1 \equiv x_2 + y_2 \pmod{d}$

(ii) $x_1 y_1 \equiv x_2 y_2 \pmod{d}$

for $x_1, x_2, y_1, y_2, d \in \mathbb{Z}$

Kongruens bliver bevaret ved addition og multiplikation, hvis de er af samme modulo d.

Reference (1.2)

Kombinationen af Prop. 1.3.2 og Prop. 1.3.4 giver os følgende:

$$[xy] = [[x][y]]$$

Supp. Noter 1.3

Antag $a, b, c \in \mathbb{Z}$ sådan at $a \equiv b \pmod{c}$. Hvis $d \in \mathbb{Z}$ og $d \mid c$, så gælder:

$$a \equiv b \pmod{d}$$

Kongruensen mellem a og b bliver bevaret selvom vi erstatter c med en af dens faktorer.

"Repeated squaring"

Se opgaver fra PerspMat.

Største fælles divisor (1.4)

Lemma 1.4.2

Lad $m, n \in \mathbb{Z}$. Der eksisterer et entydigt tal $d \in \mathbb{N}$ sådan at:

$$div(m) \cap div(n) = div(d)$$

Altså er der et entydigt tal d, hvis divisorer er alle divisorer i både m og n.

Største fælles divisor

Def. 1.4.3: Det entydige tal d fra Lemma 1.4.2 kaldes største fælles divisor for m og n, dette er klart da d er den største divisor i mængden $div(d)$ der dividerer m og n.

Dette entydige d skrives $gcd(m, n)$

Euklids algoritme (1.5)

Prop. 1.5.1

(i) $gcd(m, 0) = m$ hvis $m \in \mathbb{N}$

(ii) $gcd(m, n) = gcd(m - qn, n)$ for alle $q \in \mathbb{Z}$

(ii) kan også læses som $gcd(m, n) = gcd(m \ mod \ n, n)$.

Lemma 1.5.7

Lad $m, n \in \mathbb{Z}$. Så eksisterer der heltal $\lambda, \mu \in \mathbb{Z}$ sådan at:

$$\lambda m + \mu n = gcd(m, n)$$

Indbyrdes primisk

Def. 1.5.8: To heltal $a, b \in \mathbb{Z}$ kaldes indbyrdes primiske hvis

$$gcd(a, b) = 1$$

Bemærk at hvis vi kan finde λ, μ sådan at $\lambda a + \mu b = 1$ så er a og b indbyrdes primiske.

Kor. 1.5.10

Antag $a \mid bc$, hvor $a, b, c \in \mathbb{Z}$ og $gcd(a, b) = 1$.

Så $a \mid c$.

Hvis a dividerer et produkt og a er indbyrdes primisk med en af faktorerne, så dividerer a delproduktet fraregnet denne faktor.

Generalisering af Kor. 1.5.11 (supp. noter)

Lad $a_1, \ldots, a_n, c \in \mathbb{Z}$.

(i) Hvis $gcd(a_i, a_j) = 1$ for alle par $i \neq j$ og hvis $a_i \mid c$ for alle i,
$\Rightarrow a_1, \ldots, a_n \mid c$.

Hvis en mængde faktorer er indbyrdes primiske og alle hver især dividerer c, så dividerer deres produkt c.

(ii) Hvis $gcd(a_i, c) = 1$ for alle i,
$\Rightarrow gcd(a_1 \cdots a_n, c) = 1$.

Hvis en mængde heltal alle er indbyrdes primiske med c vil produktet af disse heltal være indbyrdes primisk med c.

Den kinesiske restklassesætning (1.6)

Def. 1.6.1

Definer $\mathbb{Z}/N = \{X \in \mathbb{N} \mid 0 \leq X < N\}$, for $N \in \mathbb{N}$. Lad $N = n_1, \ldots, n_t \neq 0$, hvor $n_1, \ldots, n_t \in \mathbb{N}$. Så lader vi:

$$r : \mathbb{Z}/N \to \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t$$

være afbildningen givet ved $r(X) = ([X]_{n_1}, \ldots, [X]_{n_t})$. Vi kalder r for rest-afbildningen.

$\mathbb{Z}/N$ er mængden af Entydig rester efter division med N. Dette er r's domæne. Givet N og X, giver r(X) os en tupel af rester, nemlig X's entydige rest efter division med N's faktorer. Se evt. ex 1.6.2

Lemma 1.6.3

Antag $N = n_1 \cdots n_t \in \mathbb{N} \setminus \{0\}$ og $gcd(n_i, n_j) = 1$ hvis $i \neq j$. Så er rest-afbildningen:

$$r : \mathbb{Z}/N \to \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t$$

en Bijektiv afbildning.

Den kinesiske restklassesætning

Sætning 1.6.4: Antag $N = n_1 \cdots n_t \in \mathbb{N} \setminus \{0\}$ og $gcd(n_i, n_j) = 1$ for $i \neq j$. (Dvs. Lemma 1.6.3 er opfyldt, så r er en Bijektiv afbildning).

Betragt nu kongruenssystemet for $a_1, \ldots, a_t \in \mathbb{Z}$, hvor $a_i = [X]_{n_i}$, altså den Entydig rest for X divideret med n_i.

Altså $r(X) = a_1, \ldots, a_t$ mht. til N.

$$\begin{aligned} X &\equiv a_1 \pmod{n_1} \\ X &\equiv a_2 \pmod{n_2} \\ &\vdots \\ X &\equiv a_t \pmod{n_t} \end{aligned}$$

Der gælder nu

(i) Systemet har en løsning $X \in Z$.

(ii) Hvis $X, Y \in \mathbb{Z}$ er løsninger, så er $X \equiv Y \pmod{N}$.

(iii) Hvis X er en løsning og $X \equiv Y \pmod{N}$, så er Y en løsning.

Den kinesiske restklassesætning udregner altså afbildningen r^{-1}, så hvis vi er givet resterne, samt betingelserne er opfyldt, kan vi finde det oprindelige X. Se eks. 1.6.5.

Eulers phi-funktion (1.7)

Vi definerer først

$$(\mathbb{Z}/N)^* = \{X \in \mathbb{Z}/N \mid gcd(X, N) = 1\}$$

for N og definerer funktionen $\phi(N) = |(\mathbb{Z}/N)^*|$.

Dette er Eulers phi-funktion, den tæller antallet af naturlige tal, der Indbyrdes primiske og skarpt mindre end et givent N. Læg mærke til vi tæller antallet af enheder i Kvotientringen $\mathbb{Z}/N$, hvis N er et primtal er alle elementer enheder og $\mathbb{Z}/N$ bliver derved et Legeme.

Prop. 1.7.1

Lad m og n være Indbyrdes primiske naturlige tal. Så gælder:

$$\phi(mn) = \phi(m)\phi(n)$$

Eulers sætning

Sætning 1.7.2: Lad $a, n \in \mathbb{Z}$ være Indbyrdes primiske, hvor $n \in \mathbb{N}$. Så gælder:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Primtal (1.8)

Primtal

Et primtal er et naturligt tal $p > 1$ der ikke kan skrives som et produkt af naturlige tal skarpt mindre end p. Dvs.

(i) $div(p) = \{1, p\}$

(ii) $\phi(p) = p - 1$,

(ii) gælder da p er Indbyrdes primisk med alle tal der ikke er et multiplum af p, hvilket ingen af de tal skarpt mindre end p er.

Lemma 1.8.1

Ethvert $n \in \mathbb{N} \setminus \{0\}$ er et produkt af Primtal.

Euklids sætning

Sætning 1.8.2: Der er uendeligt mange Primtal.

Def. Tvillingeprimtal

Et tvillingeprimtal er et Primtal p sådan at $p+2$ eller $p-2$ er et primtal. Et eksempel er 3, da 5 også er et primtal.

Lemma 1.8.3

Lad p være et Primtal og antag $p \mid ab$, hvor $a, b \in \mathbb{Z}$. Så gælder:

$$p \mid a \vee p \mid b$$

Dette gælder ikke kun for et produkt bestående af to faktorer, hvis $p \mid a_1 a_2 \cdots a_n \Rightarrow p \mid a_1 \vee p \mid a_2 \vee \ldots \vee p \mid a_n$.

Entydig primtalsfaktorisering

Sætning 1.8.5: Ethvert $n \in \mathbb{N} \setminus \{0\}$ har en *entydig* primtalsfaktorisering:

$$n = p_1 p_2 \cdots p_r$$

Bemærkning 1.8.6

Antag $n > 1 \in \mathbb{N}$ med primtalsfaktorisering:

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

hvor $e_1, \ldots, e_r \geq 0$.

Pga. Entydig primtalsfaktorisering gælder nu

$$div(n) = \{p_1^{k_1} \cdots p_r^{k_r} \mid 0 \leq k_1 \leq e_1, \ldots, 0 \leq k_r \leq e_r\}$$

Antag nu at

$$m = p_1^{f_1} \cdots p_r^{f_r}$$

hvor $f_1, \ldots, f_r \geq 0$.

Så gælder

$$div(m) = \{p_1^{k_1}, \cdots, p_r^{k_r} \mid 0 \leq k_1 \leq f_1, \ldots, 0 \leq k_r \leq f_r\}$$

Så er $div(n) \cap div(m)$:

$$\{p_1^{l_1} \cdots p_r^{l_r} \mid 0 \leq l_1 \leq (e_1, f_1), \ldots, 0 \leq k_r \leq (e_r, f_r)\} =$$
$$\{p_1^{l_1} \cdots p_r^{l_r} \mid 0 \leq l_1 \leq min(e_1, f_1), \ldots, 0 \leq k_r \leq min(e_r, f_r)\}$$

Derfor gælder der nu:

$$gcd(m, n) = p_1^{min(e_1, f_1)} \cdots p_r^{min(e_r, f_r)}$$

På samme vis må det mindste tal der har både m og n som divisorer være

$$lcm(m, n) = p_1^{max(e_1, f_1)} \cdots p_r^{max(e_r, f_r)}$$

For gcd gælder der at dette tal skal gå op i både m og n, derfor bliver vi nødt til at bruge $min(e_1, f_1)$ for at dette bliver opfyldt. Lcm skal være større eller lig både m og n, da der skal gælde at både m og n går op i lcm, derfor $max(e_1, f_1)$.

RSA (1.9)

Det første skridt for RSA er altid at udregne primtalsproduktet:

$$N = pq$$

hvor p og q er Primtal (som regel meget store).

Scenariet er at en person ønsker at sende et tal $X (0 \leq X < N)$, dette krypterer han til $[X^e]_N$, se (Entydig rest). Modtageren kan nu dekryptere dette tal fordi han kender et hemmeligt tal d, således at $[[X^e]^d] = X$. Restklasserne er i forhold til N.

Vi skal nu se på hvordan vi konstruerer e, d. Vi kan konkludere følgende fra Prop. 1.3.2 og Reference (1.2):

$$X^{ed} \equiv X \pmod{N} \iff [[X^e]^d] = [X^{ed}] = X \tag{1}$$

Vi ved også at $\phi(N) = \phi(p)\phi(q) = (p-1)(q-1)$.

Prop. 1.9.1

Lad $X \in \mathbb{Z}$ og $k \in \mathbb{N}$. Så gælder:

$$X^{k(p-1)(q-1)+1} \equiv X \pmod{N}$$

Vi skal som sagt udregne e, d og disse skal have det specielle forhold at $[[X^e]^d] = X$. Vi starter med blot at vælge $e \in \mathbb{N}$ frit. Vi kan nu udregne d på følgende vis:

Vi husker på fra Lemma 1.5.7 at der findes heltal λ og μ sådan at:

$$\lambda(p-1)(q-1) + \mu e = 1$$

hvor vi kan antage $0 < \mu < (p-1)(q-1)$ og derfor at $\lambda < 0$. Det viser sig at $d = \mu$. Dette betyder at der findes $k, d \in \mathbb{N}$, hvor $k = -\lambda$ (hvilket gør k positiv) og $d = \mu$ sådan at

$$ed = k(p-1)(q-1)+1$$

Fra RSA (1.9) får vi

$$[[X^e]^d] = [X^{ed}] = [X^{k(p-1)(q-1)+1}] \equiv X \pmod{N} \Rightarrow [X^{ed}] = X$$

for alle naturlige tal $0 \leq X < N$.

Hvis man finder en hurtig måde at udregne $\phi(N) = \phi(p)\phi(q) = (p-1)(q-1)$ så kan man vha. euklids udvidede algortime bryde RSA let vha. ovenstående metode (alle kender jo den offentlige nøgle (e, N). Dette er dog et lige så svært problem som at faktorisere N. Nu skal vi finde store nok primtal p, q så vi får et stort nok N, så det ikke er muligt at finde p og q vha. brute-force (primtalsfaktorisering af N).

Fermats lille sætning

Kor. 1.9.2: Lad p være et Primtal og $a \in \mathbb{Z}$ med $gcd(a, p) = 1$. Så gælder:

$$a^{p-1} \equiv 1 \pmod{p}$$

Dette kan også direkte udledes af Eulers sætning, da $\phi(p) = p-1$. Bemærk dette korollar kun går den ene vej, det gælder altid hvis p er et primtal, men det kan også gælde i tilfælde hvor p er et sammensat tal.

Pseudoprimtal

Def. 1.9.3: Lad $N \in \mathbb{N}$ være sammensat og $a \in \mathbb{Z}$. Så er

(i) N et pseudoprimtal mht. a hvis $a^{N-1} \equiv 1 \pmod{N}$

(ii) N er et Carmichael tal hvis N er et pseudoprimtal $\forall a : 0 < a < N$, hvor $gcd(a, N) = 1$.

Et pseudoprimtal er et naturligt tal der opfylder Fermats lille sætning (husk vi ikke ved om det er Primtal eller ej). Et Carmichael tal er et tal der er pseudoprimtal for alle baser a, der er skarpt mindre og indbyrdes primiske med N.

Lemma 1.9.4

Lad p være et primtal og $x \in \mathbb{Z}$. Hvis $x^2 \equiv 1 \pmod{p}$ så gælder:

$$x \equiv \pm 1 \pmod{p}$$

Stærkt pseudoprimtal

Def. 1.9.5: Et ulige sammensat tal N kaldes et *stærkt pseudoprimtal* mht. basen a hvis enten

(i) $a^q \equiv 1 \pmod{N}$

(ii) $\forall i : 0 \leq i < k$ at $a^{2^i q} \equiv -1 \pmod{N}$,

hvor $N - 1 = 2^k q$ og $2 \nmid q$.

Bemærk at $q =$ er den Entydig primtalsfaktorisering af $N-1$ hvor alle 2'er potenser er smidt væk og k er antallet 2'er potenser i faktoriseringen.

De stærke pseudoprimtal er netop de sammensatte tal der består både Fermats lille sætning og Lemma 1.9.4. Def. af stærke pseudoprimtal siger blot at Lemma 1.9.4 skal gælde for alle $i = 0, \ldots, k-1$, samt at Fermat testen bliver gjort på q som potensopløfter. Se evt. s. 28 for et eksempel.

Prop. 1.9.6

Lad p være et ulige Primtal og antag at

$$p - 1 = 2^k q$$

hvor $2 \nmid q$.

Hvis $a \in \mathbb{Z}$ og $gcd(a, p) = 1$ så gælder enten

(i) $a^q \equiv 1 \pmod{N}$

(ii) $\forall i : 0 \leq i < k$ at $a^{2^i q} \equiv -1 \pmod{p}$

Der gælder for alle primtal at de opfylder kravet for at være et stærkt pseudoprimtal.

Sætning 1.9.7 (Rabin)

Antag $N > 4$ er et ulige sammensat tal og lad B være antallet af baser a sådan at N er et Stærkt pseudoprimtal mht. a. Så gælder:

$$B < \phi(N)/4 \leq (N - 1/4)$$

Kvadratiske rester (1.11)

Kvadratisk rest

Def. 1.11.1: Lad p være et Primtal. Hvis $p \nmid a$ så er a en kvadratisk rest modulo p hvis:

$$\exists x \in \mathbb{Z} : a \equiv x^2 \pmod{p}$$

Hvis et sådan x ikke eksisterer er a en kvadratisk ikke-rest modulo p. Hvis $p \mid a$ er der ingen rest. Definitionen skrives med Legendre symbolet:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{hvis } p \mid a \\ 1 & \text{hvis } \exists x \in \mathbb{Z} : a \equiv x^2 \pmod{p} \\ -1 & \text{hvis et sådan } x \text{ ikke eksisterer} \end{cases}$$

Bemærkning ang. restklasser

Der gælder desuden at

$$\left(\frac{a}{p}\right) = \left(\frac{a + kp}{p}\right)$$

a og $a + kp$ tilhører samme Restklasse mht. p, derfor bliver legendre symbolet bevaret.

Prop. 1.11.3

Lad p være et ulige Primtal. Halvdelen af tallene $1, 2, \ldots, p-1$ er en Kvadratisk rest. Den anden halvdel er ikke.

Sætning 1.11.1

Lad p være et ulige Primtal og $a \in \mathbb{Z}$, hvor $p \nmid a$. Så gælder:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

a's Kvadratisk rest mht. p er kongruent til $a^{\phi(p)/2}$ mod p.

Kor. 1.11.5

Lad p være et ulige Primtal. Så tilfredsstiller legendresymbolet

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Prop. 1.11.6

Lad p være et ulige Primtal. Så gælder:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{hvis } p \equiv 1 \pmod 4 \\ -1 & \text{hvis } p \equiv 3 \pmod 4 \end{cases}$$

Lemma 1.11.10

Se bogen s. 39-40 for forklaring, mest notation.

Kor. 1.11.11

Lad p være et ulige Primtal. Så gælder:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{hvis } p \equiv 1 \pmod 8 \\ -1 & \text{hvis } p \equiv 3 \pmod 8 \\ -1 & \text{hvis } p \equiv 5 \pmod 8 \\ 1 & \text{hvis } p \equiv 7 \pmod 8 \end{cases}$$

Loven for kvadratiske reciprokker

Der gælder:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} = \begin{cases} -\left(\frac{q}{p}\right) & \text{hvis } p \equiv q \equiv 3 \pmod 4 \\ \left(\frac{q}{p}\right) & \text{ellers} \end{cases}$$

hvor p og q er ulige Primtal.

Metode til at udregne $\left(\frac{a}{p}\right)$

For at undersøge om et tal a har en Kvadratisk rest modulo p skal vi nu gøre brug af ovenstående lov.

Det er lettest illustreret via. et eksempel.

$$\left(\frac{19}{43}\right) =$$

$19 \equiv 43 \equiv 3 \pmod 4$ Derfor flipper og negerer vi pga. Loven for kvadratiske reciprokker

$$-\left(\frac{43}{19}\right) =$$

$$-\left(\frac{43}{19}\right) = -\left(\frac{5+2*19}{19}\right) = -\left(\frac{5}{19}\right) \text{ Pga. Bemærkning ang. restklasser}$$

$$-\left(\frac{5}{19}\right) =$$

Vi flipper, men negerer ikke, pga. Loven for kvadratiske reciprokker

$$-\left(\frac{19}{5}\right) =$$

$$-\left(\frac{19}{5}\right) = -\left(\frac{4+3*5}{5}\right) = -\left(\frac{4}{5}\right) \text{ Pga. Bemærkning ang. restklasser}$$

$$-\left(\frac{4}{5}\right) =$$

$$-\left(\frac{4}{5}\right) = -\left(\frac{2}{5}\right)\left(\frac{2}{5}\right) \text{ Pga. Kor. 1.11.5}$$

$$-\left(\frac{2}{5}\right)\left(\frac{2}{5}\right) =$$

$$-\left(\frac{2}{5}\right) = 1 \wedge \left(\frac{2}{5}\right) = -1 \text{ Pga. Kor. 1.11.11}$$

$$= -1$$

Det vil altså sige at der ikke eksisterer et x der opfylder $x^2 \equiv 19 \pmod{43}$ og 19 er derfor ikke en kvadratisk rest modulo p.

Grupper (2)

Indledende gruppeteori (2.1)

Komposition

En komposition på en mængde G er en afbildning $\circ : G \times G \to G$. Kompositionen $\circ(g, h)$ skrives ofte $g \circ h$ eller blot gh.

Gruppe

Def. 2.1.1: Et par, $(G, \circ)$, bestående af en mængde G og en Komposition $\circ : G \times G \to G$ kaldes en *gruppe* hvis den tilfredsstiller følgende tre egenskaber:

(i) Kompositionen skal være **associativ**:

$$g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$$

for alle $g_1, g_2, g_3 \in G$

(ii) Der skal eksistere et **neutralt** element $e \in G$, sådan at:

$$e \circ g = g \quad \text{og} \quad g \circ e = g$$

for alle $g \in G$

(iii) For alle $s \in G$ eksisterer der et **inverst** element $t \in G$, sådan at:

$$g \circ t = e \quad \text{og} \quad t \circ g = e$$

En gruppe G kaldes abelsk hvis der for alle $x, y \in G$ gælder at $x \circ y = y \circ x$. Antallet af elementer $\mid G \mid$ i G kaldes ordnen af G.

Def. 2.1.7

Lad $g \in G$ være et element i en Gruppe. Så er $g^{-1} \in G$ det entydige inverse element til g.

Finde inversen til et produkt

Inversen til et produkt $ab \in G$ er $b^{-1}a^{-1}$ da:

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a(ea^{-1}) = aa^{-1} = e$$

Kompositionstabel (2.1.2)

Se. side 53.

Gruppen S_3

Afs. 2.1.4: S_3 er Gruppen bestående af de 6 Bijektive afbildninger der findes for elementerne $X = \{1, 2, 3\}$. Gruppens komposition er den normale komposition for afbildninger, dvs. operationen $f(g(x))$, for bijektionerne $f, g \in G$.

(i) Det neutrale element e er identitetsafbildningen $X \to X$.

(ii) Den inverse til en bijektion f er den inverse afbildning $f^{-1} : X \to X$.

(iii) Komposition af afbildninger er desuden assosiativ.

Se s. 55 for eksempel og kompositionstabel.

Multiplikation med $g \in G$ er bijektiv

Antag G er en Gruppe og $g \in G$. Der eksisterer en afbildning $\phi : G \to G$ givet ved $\phi(x) = gx$. Denne afbildning er Bijektiv.

Vi kan vise ϕ er bijektiv, givet dens inverse, nemlig $\psi : G \to G$. Denne afbildning er givet ved $\psi(x) = g^{-1}x$. Ved komposition gælder nu:

(i) $\psi(\phi(x)) = x$

(ii) $\phi(\psi(x)) = x$

Udregningerne er sparet væk (se s. 56). Afbildningen $\varepsilon : G \to G$, givet ved $\varepsilon(x) = xg$ er også bijektiv og dette vises på samme måde.

Prop. 2.1.2

Lad $a, b, n \in \mathbb{Z}$. Så gælder:

(i) $a + n\mathbb{Z} = b + n\mathbb{Z} \iff a \equiv b \pmod{n}$

(ii) $(a + n\mathbb{Z}) \cap (b + n\mathbb{Z}) = \emptyset \iff a \not\equiv b \pmod{n}$

(i): Hvis $[a]_n = [b]_n$ så er a og b kongruente modulo n og vice versa. (ii): Hvis $[a]_n$ og $[b]_n$ ingen elementer har tilfælles er de ikke kongruente modulo n og vice versa.

Undergrupper (2.2)

Undergruppe

Def. 2.2.1: En undergruppe af en Gruppe G er en delmængde $H \subseteq G \neq \emptyset$ sådan at G's Komposition gør H til en gruppe.

H er altså en undergruppe af $G \iff$

(i) $e \in H$

(ii) $x^{-1} \in H$ for alle $x \in H$

(iii) $xy \in H$ for alle $x, y \in H$

Bemærk at en undergruppe skal være lukket under kompositionen. Per definition er kompositionen lukket indenfor G, den skal også være lukket indenfor H for at H er en undergruppe.

Prop. 2.2.3

Lad H være en Undergruppe af $(\mathbb{Z}, +)$. Så gælder:

$$H = d\mathbb{Z} = \{dn \mid n \in \mathbb{Z}\} = \{\ldots, -2d, -d, 0, d, 2d, \ldots\}$$

for et entydigt naturligt tal $d \in \mathbb{N}$.

En undergruppe af $\mathbb{Z}$ vil være en gruppe bestående af alle multiplums af et tal $d \in \mathbb{N}$, ellers kan den f.eks. ikke opfylde lukkethedsegenskaben.

Sideklasse

Lad H være en Undergruppe af en Gruppe G og $g \in G$. Så siger vi:

(i) $gH = \{gh \mid h \in H\} \subseteq G$ kaldes en venstre sideklasse. Mængden af Hs venstre sideklasse skrives G/H.

(ii) $Hg = \{hg \mid h \in H\} \subseteq G$ kaldes en højre sideklasse. Mængden af Hs højre sideklasser skrives $G\backslash H$.

Bemærk samspillet med Kvotientgruppen $\mathbb{Z}/n\mathbb{Z}$.

Desuden er $\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$. Se på Prop. 2.2.3 og lad $G = \mathbb{Z}$ og lad $H = 3\mathbb{Z}$. Dvs. $3\mathbb{Z}$ er en undergruppe til $\mathbb{Z}$. Vi ser nu at $\mathbb{Z}/3\mathbb{Z}$ er mængden af $3\mathbb{Z}$s venstre sideklasser. Fra Kor. 2.2.7 kan vi konkludere at dette er lig $\mathbb{Z}$. En sideklasse er en generalisering af en Restklasse. Mængden af alle restklasser er også lig gruppen den er en restklasse for. F.eks. er mængden $\{[0]_2, [1]_2\} = \mathbb{Z}$. Den består af alle tal der enten har rest 1 eller 0 ved division med 2, hvilket er alle tal i $\mathbb{Z}$.

Lemma 2.2.6

Lad H være en Undergruppe af en Gruppe G og lad $x, y \in G$. Så gælder:

(i) $x \in xH$

(ii) $xH = yH \iff x^{-1}y \in H$ (se Prop. 2.1.2 og tænk på x^{-1} som -x), dvs. $xH = yH \iff x \equiv y \pmod{H = d\mathbb{Z}}$.

(iii) Hvis $xH \neq yH \Rightarrow xH \cap yH = \emptyset$

(iv) Afbildningen $\phi : H \to H$ givet ved $\phi(h) = xh$ er Bijektiv.

Kor. 2.2.7

Lad H være en Undergruppe af G. Så gælder:

$$G = \bigcup_{g \in G} gH$$

og hvis $g_1H \neq g_2H \Rightarrow g_1H \cap g_2H = \emptyset$.

Mængden af Hs venstre Sideklasser er lig den oprindelige gruppe. Sideklassenerne g_1 og g_2 enten er lig hinanden eller disjunkte.

Lagranges sætning

Sætning 2.2.8: Hvis $H \subseteq G$ er en Undergruppe til en endelig Gruppe G så:

$$| G | = | G/H | \, | H |$$

Ordnen af en undergruppe dividerer ordenen af gruppen.

Index

Def. 2.2.9: Antallet af Sideklasser $| G/H |$ kaldes **indexet** af H i G. Det skrives $[G : H]$.

Normale undergrupper (2.3)

Komposition for delmængder af en gruppe

Lad X, Y være delmængder af en Gruppe G. Så definerer vi komposition for disse:

$$XY = \{xy \mid x \in X, y \in Y\}$$

Dette kan vi imidlertid ikke direkte overføre til komposition for Sideklasser. Se s. 64 for forklaring. Der skal gælde nedenstående før vi kan snakke om sideklasser som Undergrupper.

Prop. 2.3.1

Lad H være en Undergruppe af G. Hvis $gH = Hg$ for alle $g \in G$ så gælder:

$$(xH)(yH) = (xy)H$$

for alle $x, y \in G$.

Normal undergruppe

Def. 2.3.2: En Undergruppe N af en Gruppe G kaldes *normal* hvis

$$gNg^{-1} = \{gng^{-1} \mid n \in N\} = N$$

for alle $g \in G$.

En normal undergruppe N af G tilfredsstiller $gN = Ng$ for alle $g \in G$. (Prop. 2.3.1). En Undergruppe af en abelsk gruppe er altid normal. (gælder ikke begge veje).

Bemærk, hvis H har Index 2 i G er H normal, jf. opg. 2.15.

Kor. 2.3.3

Lad N være en Normal undergruppe af Gruppe G. Så gør kompositionen Komposition for delmængder af en gruppe G/N til en gruppe og pga. Prop. 2.3.1 gælder der:

$$(g_1 g_2)N = (g_1 N)(g_2 N)$$

for $g_1 N, g_2 N \in G/N$

Kvotientgruppe

Def. 2.3.4: Lad N være en Normal undergruppe af en Gruppe G. Så kaldes gruppen bestående af Ns Sideklasser, G/N, en kvotientgruppe.

Husk G/N er mængden af Ns Sideklasser og at sideklasser er en generalisering af restklasser, så passer pengene i forhold til Kvotientgruppen $\mathbb{Z}/n\mathbb{Z}$.

Lemma 2.3.6

Lad H og $K \subseteq G$, hvor G er en Gruppe og H er en Normal undergruppe. Så er HK en Undergruppe af G.

Kvotientgruppen $\mathbb{Z}/n\mathbb{Z}$

I forlængelse af Kvotientgruppe kigger vi på gruppen $(\mathbb{Z}, +)$. Dette er en kvotientgruppe hvis elementer er Sideklasser (Restklasser) for et givet $n \in \mathbb{Z}$:

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

En restklasse er selv en mængde, derfor er en **kvotientgruppe en mængde af mængder**.

En restklasse, $[a]_n$ kan udtrykkes på formen:

$$a + n\mathbb{Z} = \{a + nx \mid x \in \mathbb{Z}\}$$

hvor $a \in \mathbb{Z}$ er repræsentanten for klassen og $n \in Z$ er det tal vi regner modulo.

Et eksempel: $[2]_5 = 2 + 5\mathbb{Z} = \{\ldots, -8, -3, 2, 7, \ldots\}$. *Dvs. mængden af alle tal der er kongruent med 2 modulo 5..*

Fra Prop. 1.3.2 gælder der nu at hvis $n > 0$:

$$a + n\mathbb{Z} = b + n\mathbb{Z} \iff [a]_n = [b]_n$$

Der eksisterer kun $n-1$ Entydig rester mht. n. Derfor er $[12]_5 = [2]_5$, da disse har samme rest mht. n. Vi bruger derfor som regel kun repræsentanter fra $0, \ldots, n-1$ da de andre er inkluderede heri.

Nogle eksempler på specielle kvotientgrupper:

$$\mathbb{Z}/0\mathbb{Z} \Rightarrow \{x\} = x + 0\mathbb{Z} = x \Rightarrow (\mathbb{Z}, +)$$
$$\mathbb{Z}/1\mathbb{Z} \Rightarrow \{[0]_1\} = 0 + 1\mathbb{Z} = (\mathbb{Z}, +)$$

Primiske restklasser $(\mathbb{Z}/n\mathbb{Z})^*$

Vi lader mængden:

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[a]_n \in \mathbb{Z}/n\mathbb{Z} \mid gcd(a, n) = 1\}$$

udgøre alle primiske Restklasser, hvor $n \in \mathbb{N}$.

*Elementer i $(\mathbb{Z}/n\mathbb{Z})^*$ er på formen $a+n\mathbb{Z}$, altså det er en Kvotientgruppe. For at en kvotientgruppe, med **multiplikation** med restklasser som komposition, skal være en Gruppe skal alle elementer $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^*$ være indbyrdes primiske med n. Ordnen af sådan en gruppe er $\phi(n)$.*

Supplement til 2.3. Lemma 1

Lad G være en Gruppe, og lad $H \subseteq G$ være en Undergruppe. Lad $g \in G$ være et vilkårligt element. Så er mængden

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

en undergruppe af G.

Supplement til 2.3. Lemma 2

Lad G være en endelig Gruppe af orden N, og lad d være en divisor i N. Hvis der findes netop en Undergruppe $H \subseteq G$ af orden d, så er H en Normal undergruppe i G.

Gruppehomomorfier (2.4)

Gruppehomomorfi

Def. 2.4.1: Lad G og K være Grupper. En afbildning $f : G \to K$ kaldes en gruppehomomorfi hvis

$$f(xy) = f(x)f(y)$$

for alle $x, y \in G$. Kompositionen på venstre side af lighedstegnet er Gs komposition, mens kompositionen på højre side er Ks.

Et eksempel på en gruppehomomorfi er eksponentialfunktionen $e^x : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$, hvor $(\mathbb{R}_{>0}, \cdot) = \{x \in \mathbb{R} \mid x > 0\}$. Dette er den kendte regel $e^{x+y} = e^x \cdot e^y$ for alle $x, y \in \mathbb{R}$.

Der gælder desuden:

(i) $f(e_G) = e_H$

(ii) $f(g^{-1}) = f(g)^{-1}$

Altså at det neutrale element i G afbildes til det neutrale element i H, samt inverserne bliver bevaret af afbildningen. Vi siger at en gruppehomomorfi er kompatibel med gruppestrukturen.

Prop. 2.4.9

Lad $f : G \to K$ være en Gruppehomomorfi. Så gælder:

(i) Billedet *$f(G)$* $\subseteq K$ er en Undergruppe til K.

(ii) Kernen *$Ker(f)$* $\subseteq G$ er en Normal undergruppe til G.

(iii) f er Injektiv $\iff$ $Ker(f) = \{e\}$.

Gruppeisomorfi

(i) En Bijektiv Gruppehomomorfi kaldes en gruppeisomorfi.

(ii) Vi bruger notationen $f : G \xrightarrow{\sim} K$.

(iii) Vi skriver $G \cong K$ og siger G og K er isomorfe.

Isomorfisætningen

2.5.1: Lad G og K være Grupper og $f : G \to K$ en Gruppehomomorfi med kernen $N =$ *$Ker(f)$*. Så er:

$$\tilde{f} : G/N \to f(G)$$

givet ved $\tilde{f}(gN) = f(g)$ en Veldefineret afbildning og en Gruppeisomorfi.

Da N er en Normal undergruppe til G (Prop. 2.4.9) er G/N en Kvotientgruppe. Denne indeholder alle Sideklasser for N. $\tilde{f}$ afbilder fra disse sideklasser til billedet af f (dvs. alle elementer i K der bliver afbildet af f). Man finder oftest først en Surjektiv Gruppehomomorfi $f : G \to K$ for en passende gruppe K, sådan at $N = ker(f)$, så giver sætningen gruppeisomorfien $\tilde{f}$.

Orden af et element i en gruppe (2.6)

Prop. 2.6.1

Lad G være en Gruppe og $g \in G$. Afbildningen

$$f_g : \mathbb{Z} \to G$$

givet ved $f_g(n) = g^n$ er en Gruppehomomorfi fra $(\mathbb{Z}, +)$ til G.

Denne afbildning er den kendte potensopløftning (med $+$ som komposition), og det er en Gruppehomomorfi.

Ordnen af et element

(i) Billedet $f_g(\mathbb{Z}) = \{g^n \mid n \in \mathbb{Z}\}$ skrives $\langle g \rangle$.

(ii) $\langle g \rangle$ er en abelsk Undergruppe af G.

(iii) Antallet af elementer i $\langle g \rangle$ kaldes ordnen af g og skrives $ord(g)$.

(iv) $ord(g)$ kan man tænke på som den mindste positive potens af g der giver e.

(v) Hvis sådan en potens ikke findes siges g at have uendelig orden.

Prop. 2.6.3

Lad G være en endelig Gruppe og lad $g \in G$. Så gælder:

(i) $ord(g)$ dividerer $\mid G \mid$

(ii) $g^{|G|} = e$

(iii) Hvis $g^n = e$ for et $n > 0$ så $ord(g) \mid n$.

Supplement til 2.6

Lad G være en Gruppe og $g \in G$. Betragt afbildningen $f_g : \mathbb{Z} \to G$ (Prop. 2.6.1). Der findes nu et heltal $n_g > 0$ sådan at $Ker(f_g) = n_g\mathbb{Z}$ (Prop. 2.2.3). Fra dette kan vi konkludere

(i) Hvis $n_g = 0$ er f_g Injektiv.

(ii) Hvis $n_g > 0$, så er $g_n = g_m \iff n \equiv m \pmod{n_g}$. Dette medfører at

$$\langle g \rangle = \{g^0 = e, g^1 = g, g^2, \ldots, g^{n_g - 1}\}$$

Der gælder desuden at

$$f(g_n) = f(g)^n \quad \text{for alle g} \in G \text{ og alle } n \in \mathbb{Z}$$

Hvis $Ker(f_g) = 0$ er det kun $0 \in \mathbb{Z}$ der afbilder til $e \in G$ og derved afbilder de andre elementer i $\mathbb{Z}$ til forskellige elementer i G. Hvis $n_g > 0$ så afbilder kongruente heltal $\in \mathbb{Z}$ til det same element i G. Derved giver det kun mening at potensopløfte elementer i g med tal fra $[0; n_g[$, da billedet af f_g kun består af multiplum as disse.

Cykliske grupper (2.7)

Cyklisk gruppe

Def. 2.7.1: En Gruppe G siges at være cyklisk hvis den indeholder et element g, sådan at $G = \langle g \rangle$. Elementet g kaldes en frembringer for G og vi siger g frembringer G.

Hvis alle elementer i G kan skrives som potenser af g er G cyklisk.

Prop 2.7.2

Lad G være en Gruppe med primtalsorden $\mid G \mid = p$. Der gælder nu at $\mathbb{Z}/p\mathbb{Z} \cong G$, som er en Cyklisk gruppe.

Dvs. hvis G har en primtalsordenen p, så eksisterer der en gruppeisomorfi $f : \mathbb{Z}/p\mathbb{Z} \to G$. Dette kommer af Isomorfisætningen

Prop 2.7.4

Lad G være en Cyklisk gruppe. Så gælder:

(i) Enhver Undergruppe af G er cyklisk.

(ii) Antag G er endelig og at d er en divisor i $\mid G \mid$. Så indeholder G en entydig undergruppe H, hvor $\mid H \mid = d$.

(iii) Der er $\phi(d)$ elementer af orden d i G. Disse er frembringerne for H.

Eksempel: Lad $G = \mathbb{Z}/6\mathbb{Z} = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$. Det ses at $ord(G) = 6$, vi lader derfor $d = 3$. En undergruppe skal indeholde det neutrale element $[0]_6$, så denne skal være indeholdt.

Dernæst skal hvert element i en undergruppe have en invers. Vi ved også at enhver undergruppe af G er cyklisk, de to elementer der tilfredsstiller disse krav er $[2]_6$ og $[4]_6$. Dvs. $H = \{[0]_6, [2]_6, [4]_6\}$.

(iii) siger nu at der skal være 2 elementer i G af ordnen 3. Det første element der tilfredsstiller dette er $[2]_6$, da $[2]_6^3 = [0]_6$. Det andet element er $[4]_6$, da $[4]_6^3 = [0]_6$. Ingen af de andre elementer har denne egenskab. (iii) siger nu at $[2]_6$ og $[4]_6$ genererer netop H.

Kor. 2.7.6

Lad $N > 0 \in \mathbb{Z}$. Så gælder:

$$\sum_{d|N} \phi(d) = N$$

hvor der summeres over $d \in div(N)$.

Eksempel: Lad $N = 6$. $div(N) = div(6) = \{1, 2, 3, 6\}$. Nu siger korollaret at $N = \phi(1) + \phi(2) + \phi(3) + \phi(6) = 1 + 1 + 2 + 2 = 6$.

Grupper og tal (2.8)

Produktgrupper

Hvis $G_1, G_2, \ldots, G_n$ er Grupper, så har produktet:

$$G = G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \ldots, g_n) \mid g_1 \in G_1, g_2 \in G_2, \ldots g_n \in G_n\}$$

den naturlige Komposition

$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1h_1, g_2h_2, \ldots, g_nh_n)$$

En produktgruppe skal ses som en gruppe indeholdende tupler, bestående af et element fra hver faktorgruppe. To produktgrupper G og H komponeres som vist ovenover.

Lemma 2.8.1

Lad M, N være Normal undergrupper af en Gruppe G, hvor $M \cap N = \{e\}$. Så er:

(i) MN en Undergruppe til G.

(ii) $\pi : M \times N \to MN$, givet ved $\pi(x, y) = xy$, en Gruppeisomorfi.

Symmetriske gruppe (2.9)

Den symmetriske gruppe S_n har som elementer alle permutationer af Bijektive afbildninger der afbilder fra tupler bestående af n symboler til sig selv. Altså en gruppe bestående af alle kombinationer af bijektioner over de n symboler. Elementerne i S_n kaldes permutationer. Gruppen S_3 er et eksempel på en symmetrisk gruppe.

Der gælder at $\mid S_n \mid = n!$

Def. 2.9.1

Antag $\sigma \in S_n$. Så definerer vi

$$M_\sigma = \{x \in M_n \mid \sigma(x) \neq x\}$$

hvor $M_n = \{1, 2, \ldots, n\}$. Permutationerne $\sigma, \tau \in S_n$ kaldes disjunkte hvis $M_\sigma \cap M_\tau = \emptyset$.

σ og τ er elementer i S_n, altså Bijektive afbildninger over M_n. M_σ og M_τ er mængderne bestående af de tal som henholdsvist σ og τ permuterer. $M_\sigma \cap M_\tau = \emptyset$ hvis σ og τ permuterer forskellige tal.

Prop 2.9.2

Lad $\sigma, \tau \in S_n$ være disjunkte permutationer. Så gælder:

$$\sigma\tau = \tau\sigma$$

samt at $M_{\sigma\tau} = M_\sigma \cup M_\tau$

k-cykel

Antag vi er givet k forskellige elementer i M_n. En permutation $\sigma \in S_n$, givet ved:

$$\sigma(x_1) = x_2, \quad \sigma(x_2) = x_3, \quad \ldots, \quad \sigma_{k-1} = x_k, \quad \sigma(x_k) = x_1$$

og $\sigma(x) = x$ hvis $x \notin \{x_1, \ldots, x_k\}$ kaldes en k-cykel. Sådan en cykel skrives $\sigma(x_1x_2 \ldots x_k)$.

Bemærk at $M_\sigma = \{x_1, x_2, \ldots, x_k\}$ og at ordnen af en k-cykel i S_n er k. Se Ordnen af et element.

Ordnen af en cykel

Ordnen af en k-cykel er k. Ordnen er altså lig længden af cyklen. *Fra Wikipedia.*

Altså er en k-cykel en permutation der gør at alle k elementer bliver flyttet en frem og hvor det sidste element bliver flyttet til starten. De andre ikke-k elementer i M_n permuterer en k-cykel ikke. Tænk linked list.

Prop 2.9.5

Lad $\sigma \in S_n$ være skrevet som et produkt af disjunkte cykler $\sigma_1 \cdots \sigma_r$. Så er $ord(\sigma) = lcm(ord(\sigma_1), \cdots, ord(\sigma_r))$. Se Ordnen af et element.

Prop 2.9.6

Alle permutationer $\sigma \in S_n$ er et produkt af entydige disjunkte cykler.

Lemma 2.9.8

Antag $(i_1 i_2 \dots i_k)$ er en k-cykel og at $\sigma \in S_n$ er en vilkårlig permutation. Så gælder:

$$\sigma(i_1 i_2 \dots i_k)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\dots\sigma(i_k))$$

Lemmaet fortæller, hvordan man beregner en Konjugering af en k-cykel. Eksempel: Hvis vi vil konjugere 3-cyklen (123) med permutationen $\sigma = (125)(34)$ i S_5, dvs hvis vi vil udregne σ (1 2 3) σ^{-1}, så behøver vi blot at finde $\sigma(1) = 2$, $\sigma(2) = 5$ og $\sigma(3) = 4$. Lemmaet siger nu at $\sigma(123)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)) = (254)$. Vi slipper altså for at beregne σ^{-1}.

Transposition

En 2-cykel kaldes en transposition i S_n. Pga. det er en 2-cykel er en transposition sin egen invers.

Simpel transposition

En simpel transposition er en Transposition på følgende form:

$$s_i = (i \quad i+1)$$

hvor $i = 1, \dots, n-1$

Altså er en simpel transposition en transposition der permuterer et symbol i, en plads frem. i kan ligge i intervallet $1 \leq i < n$.

Bubble sort

Simpel sorteringsalgoritme. Går igennem elementerne en ad gangen og sammenligner naboparrene, hvis et efterfølgende element er skarpt større end det forrige swappes disse og algoritmen starter forfra. Når algoritmen når til sidste element er elementerne sorterede. Disse swaps er eksempler på simple transpositioner.

Inversion

Def. 2.9.10: Lad $\sigma \in S_n$ være en permutation. Et par af indekser (i, j), hvor $1 \leq i < j \leq n$, kaldes en **inversion** af σ, hvis $\sigma(i) > \sigma(j)$.

Et par (i, j), hvor i er mindre end j, men hvor permutationen σ gør at $\sigma(i) > \sigma(j)$ kaldes en inversion af σ.

Lad

$$I_\sigma = \{(i, j) \mid 1 \leq i < j \leq n \wedge \sigma(i) > \sigma(j)\}$$

være mængden af alle inversioner og lad $n(\sigma) =\mid I_\sigma \mid$ være antallet af inversioner af σ.

Prop 2.9.12

Permutationen $\sigma \in S_n$ er identitetsafbildningen $\iff n(\sigma) = 0$. Hvis σ ikke er identitetsafbildningen så eksisterer der et $1 \leq i < n$ sådan at $\sigma(i) > \sigma(i + 1)$.

Identitetsafbildningen er den eneste permutation der ingen Inversioner har. Hvis σ ikke er identitetsafbildningen så eksisterer der en inversion af σ for et nabopar (i, j), altså hvor $j = i + 1$.

Lemma 2.9.13

Lad $s_i \in S_n$ være en Simpel transposition og $\sigma \in S_n$. Så gælder:

$$n(\sigma s_i) = \begin{cases} n(\sigma) + 1 & \text{hvis } \sigma(i) < \sigma(i + 1) \\ n(\sigma) - 1 & \text{hvis } \sigma(i) > \sigma(i + 1) \end{cases}$$

Lemmaet siger at antallet af Inversioner af σ komponeret med den simple transposition s_i, er lig $n(\sigma) \pm 1$ afhængigt af om $(i, i + 1)$ er en inversion af σ eller ej.

Lemma 2.9.14

Lad $\sigma \in S_n$. Så gælder:

(i) σ er et produkt af $n(\sigma)$ Simpel transpositioner.

(ii) $n(\sigma)$ er det mindste antal simple transpositioner der skal bruges for at skrive σ som et produkt af simple transpositioner.

Def. 2.9.15

Fortegnet af en permutation $\sigma \in S_n$ er

$$sgn(\sigma) = (-1)^{n(\sigma)}$$

En permutation med positivt fortegn kaldes lige, en permutation med negativt fortegn kaldes ulige.

Antallet af Inversioner af en permutation afgør om den er lige eller ulige.

Prop 2.9.16

Afbildningen

$$sgn : S_n \to \{\pm 1\}$$

er en Gruppehomomorfi, hvor Kompositionen i $\{\pm 1\}$ er multiplikation.

Den Alternerende gruppe

Mængden af lige permutationer i S_n skrives A_n og kaldes den alternerende Gruppe. Fra Prop 2.9.16 og Prop. 2.4.9 (ii) kan vi konkludere at A_n er en Normal undergruppe til S_n, da A_n netop er kernen til afbildningen sgn. Der gælder at $\mid A_n \mid = n!/2$.

Prop 2.9.17

Lad $n \geq 2$.

(i) En Transposition $\tau = (i \quad j) \in S_n$ er en ulige permutation.

(ii) Fortegnet af en r-cykel $\sigma = (x_1 x_2 \dots x_r)$ er $(-1)^{r-1}$.

Simpel gruppe

En Gruppe N kaldes simpel hvis $\{e\}$ og N er de eneste Normal undergrupper af N.

Lemma 2.9.18

Enhver permutation i A_n er et produkt af en 3-cykel hvis $n \geq 3$.

Sætning 2.9.19

Den Alternerende gruppe A_n er Simpel gruppe for $n \geq 5$.

Lemma 2.9.20

Enhver 3-cykel er et produkt af en simpel 3-cykler i A_n hvis $n \geq 3$.

En 3-cykel kaldes simpel hvis den er på formen $(k \quad k+1 \quad k+2)$.

Gruppevirkninger (2.10)

Gruppevirkning

Def 2.10.1: Lad G være en Gruppe og S en mængde. Vi siger at G virker på en gruppe hvis der eksisterer en afblidning

$$\alpha : G \times S \to S$$

som skrives $\alpha(g, s) = g \cdot s$ sådan at:

(i) $e \cdot s = s$ for alle $s \in S$

(ii) $(g \cdot h)s = g(h \cdot s)$ for alle $g, h \in G$ og for alle $s \in S$.

En virkning er en afbildning der afbilder fra et element $s \in S$ og et gruppeelement $g \in G$, til S. Denne afbildning skal respektere det neutrale element og være associativ.

Def. 2.10.2

Lad $\alpha : G \times S \to S$ være en Gruppevirkning af G på S og $s \in S$ et element i S. Så er:

$$G \cdot s = Gs = \{gs \mid g \in G\}$$

banen af s under virkningen af G. Mængden af baner $\{Gs \mid s \in S\}$ skriver vi S/G.

Banen af s under $G \subseteq S$ er den delmængde af S som α afbilder dette s og hele G til.

Lad $X \subseteq S$ være en delmængde af S og $g \cdot X = gX = \{gx \mid x \in X\}$, hvor $g \in G$. Så er:

$$G_X = \{g \in G \mid gX = X\}$$

stabilisatoren for X. Hvis $X = \{x\}$ skrives G_X som G_x.

Stabilisatoren $G_X \subseteq G$ er den delmængde hvis virkning ikke ændrer elementerne i X.

Et **fikspunkt** for en virkning er et element $s \in S$ sådan at $gs = s$ for alle $g \in G$. Mængden af fikspunkter skriver vi S^G.

Et fikspunkt er et element $s \in S$ der er neutral mht. Gs virkning.

Prop. 2.10.5

Lad $\alpha : G \times S \to S$ være en Gruppevirkning. Så gælder:

(i) Lad $X \subseteq S$ være en delmængde af S. Så er G_X en Undergruppe af G.

(ii) Mængden S er foreningen af G-baner:

$$S = \bigcup_{s \in S} Gs$$

hvor $Gs \neq Gt \Rightarrow Gs \cap Gt = \emptyset$ hvis $s, t \in S$.

(iii) Lad $x \in S$. Så er

$$\tilde{f} : G/G_x \to Gx$$

givet ved $\tilde{f}(gG_x) = gx$ en Veldefineret Bijektiv afbildning fra G_xs venstre Sideklasser til banen Gx.

Kor. 2.10.7

Lad $G \times S \to S$ være en Gruppevirkning hvor S er endelig. Så gælder:

$$\mid S \mid = \mid S^G \mid + \sum_x \mid G/G_x \mid$$

hvor der summes ved at vælge et element x fra hver bane med mere end et element.

Ordnen af S er lig antallet af fikspunkter + summen af antallet af venstre Sideklasser for hvert element i G_x, altså de elementer der er stabile under Konjugering med x.

Lemma 2.10.8 (Burnside)

Lad $G \times S \to S$ være en Gruppevirkning, hvor G er en endelig Gruppe og S en endelig mængde. Så gælder:

$$\mid S/G \mid = \frac{\sum_{g \in G} \mid S^g \mid}{\mid G \mid}$$

hvor $S^g = \{x \in S \mid gx = x\}$.

S^g er de elementer i S der er fikspunkter under g. Antallet af baner for en virkning er altså lig summen af antallet af fikspunker under g divideret med ordnen af G. Sagt med andre ord, antallet af baner (et naturligt tal eller $+\infty$) er lig det gennemsnitlige antal fikspunkt under et element af g.

Konjugering

Afbildningen $\alpha : G \times G \to G$ givet ved $\alpha(g,h) = ghg^{-1}$ er en Gruppevirkning af G på G. Den kaldes konjugering.

$C(h)$ kaldes konjugeringsklassen indeholdende h og udgør banen (Def. 2.10.2)

$$C(h) = G \cdot h = \{ghg^{-1} \mid g \in G\}$$

Altså er konjugeringsklassen indeholdende h en delmængde af G indeholdende de elementer som ghg^{-1} afbilder til. I en abelsk gruppe er enhver konjugeringsklasse en singleton.

$Z(h)$ kaldes centralisatoren af h og udgør stabilisatoren (Def. 2.10.2) G_h:

$$Z(h) = \{g \in G \mid gh = hg\}$$

Altså er centralisatoren af h mængden af elementer i G hvor $ghg^{-1} = hgh^{-1}$.

$Z(G)$ kaldes centeret af G og udgør mængden af fikspunkter for G:

$$Z(G) = G^G = \{g \in G \mid gx = xg \text{ for alle } x \in G\}$$

$Z(G)$ er altså mængden af elementer der er stabile med alle elementer i G under konjugering. $Z(G)$ er en normal abelsk undergruppe af G og indeholder mindst elementet e for konjugeringsvirkningen.

Hvis G er en endelig Gruppe kan vi skrive Kor. 2.10.7 som:

$$\mid G \mid = \mid Z(G) \mid + \sum_{h \in G} \mid G/Z(h) \mid$$

Ordnen af G er lig antallet af fikspunkter for G + summen af antallet af venstre Sideklasser for elementerne i G_h, altså de elementer der er stabile under konjugering med h.

$N_G(H)$ kaldes normalisatoren af H i G og udgør stabilisatoren af Undergruppen $H \subseteq G$:

$$N_G(H) = G_H = \{g \in G \mid gHg^{-1} = H\}$$

H er en Normal undergruppe $\iff N_G(H) = G$.

p-gruppe

En endelig Gruppe med orden p^r, hvor p er et Primtal og $r \in \mathbb{N}$ kaldes en p-gruppe.

Prop. 2.10.13

Lad G være en ikke-triviel p-gruppe med en Gruppevirkning på en mængde S. Så er

$$\mid S \mid \equiv \mid S^G \mid \pmod{p}$$

Ordnen af S er kongruent (mod p) til antallet af fikspunkter i S under G, hvis G er en ikke-triviel p-gruppe.

Kor. 2.10.14

Lad G være en ikke-triviel p-gruppe med orden p^r, så er

$$\mid G \mid \equiv \mid Z(G) \mid \pmod{p}$$

og $\mid Z(G) \mid > 1$.

Ordnen af G er kongruent (mod p) til størrelsen af centeret af G (Konjugering), altså antallet af fikspunkter for G, samt centeret af G består af mere end 1 element.

Kor. 2.10.15

Lad p være et Primtal. En gruppe G med orden $\mid G \mid = p^2$ er abelsk.

Sylow p-undergruppe

Def. 2.10.16: Lad G være en endelig Gruppe og p et Primtal. Antag nu at $\mid G \mid = p^r m$, hvor $p \nmid m$. En Undergruppe $H \subseteq G$ med orden $\mid H \mid = p^r$ kaldes en Sylow p-undergruppe.

Hvis en p-gruppe $H \subseteq G$ og $\mid G \mid = p^r m$, hvor $p \nmid m$, kaldes H en Sylow p-undergruppe.

Sætning 2.10.17 (Første Sylow Sætning)

Lad G være en endelig Gruppe og p et Primtal. Antag at $\mid G \mid = p^r m$, hvor $p \nmid m$. Så indeholder G en Sylow p-undergruppe.

Sætning 2.10.18 (Anden Sylow Sætning)

Lad G være en endelig Gruppe og P, Q to Sylow p-undergruppe r. Så eksisterer der et $g \in G$ sådan at:

$$gPg^{-1} = Q$$

Ydermere, enhver p-undergruppe H (p-gruppe) er indeholdt i en Sylow p-undergruppe.

Hvis P, Q er to Sylow p-undergruppe r, har de samme orden. Da der eksisterer et $g \in G$ sådan at $gPg^{-1} = Q$ siger vi at P og Q tilhører samme konjugeringsklasse (Konjugering).

Sætning 2.10.19 (Tredje Sylow Sætning)

Lad G være en endelig Gruppe med orden $p^r m$, hvor $p \nmid m$. Lad $Syl_p(G)$ være mængden af Sylow p-undergruppe r. Så gælder:

(i) $\mid Syl_p(G) \mid$ dividerer m.

(ii) $\mid Syl_p(G) \mid \equiv 1 \pmod{p}$

Eksempler på brugen af Sylow sætningerne kan ses på side 103.

Supplement til 2.10. Lemma 1

Lad G være en Gruppe og $g \in G$. Afbildningen

$$i_g : G \to G$$

givet ved $i_g(x) = gxg^{-1}$ kaldes Konjugering med g.

Afbildningen i_g er en Gruppeisomorfi. Dette medfører:

(i) Hvis H er en Undergruppe af G, så er $i_g(H)$ en undergruppe af G.

(ii) $ord(x) = ord(gxg^{-1})$ for alle $x \in G$.

Supplement til 2.10. Korrolar

Lad p være et Primtal og lad G være en endelig p-gruppe med $\mid G \mid > p$. Så er G ikke en Simpel gruppe.

Supplement til 2.10. Observation

Lad G være en endelig Gruppe og p et Primtal. Hvis G kun har een Sylow p-undergruppe P, så er P en Normal undergruppe af G.

Supplement til 2.10. Lemma 2

Lad G være en endelig Gruppe og lad p og q være to entydige Primtal. Lad P være en Sylow p-undergruppe af G og Q en Sylow q-undergruppe af G. Så gælder:

(i) $P \cap Q = \{e\}$

(ii) Hvis P og Q er Normal undergrupper i G, så er $xy = yx$ for alle $x \in P$ og $y \in Q$

(iii) Hvis p og q er de eneste primdivisorer af $\mid G \mid$, og hvis enten P eller Q er normale i G, så er $G = PQ$.

Ringe (3)

Def. Ring (3.1)

Ring

En ring er en abelsk Gruppe $(R, +)$ med en yderligere Komposition $\cdot : R \times R \to R$ kaldet **multiplikation**. Denne skal tilfredsstille følgende 3 egenskaber:

(i) Multiplikationen skal være **associativ**:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

for alle $x, y, z \in R$

(ii) Der skal eksistere et **neutralt** element $1 \in R$, sådan at:

$$1 \cdot x = x \quad \text{og} \quad x \cdot 1 = x$$

for alle $x \in R$

(iii) Multiplikationen skal være **distributiv**:

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{og} \quad (y + z) \cdot x = y \cdot x + z \cdot x$$

for alle $x, y, z \in R$

Bemærk at 0 er det neutrale element i $(R, +)$.

Delring

En delmængde $S \subseteq R$ af en Ring R, kaldes en **delring** hvis

(i) S er en Undergruppe af $(R, +)$

(ii) $1 \in S$

(iii) $xy \in S$ hvis $x, y \in S$

Nuldivisor

Et element $x \in R \setminus \{0\}$ kaldes en **nuldivisor**, hvis der eksisterer et $y \in R \setminus \{0\}$ sådan at $xy = 0$ eller $yx = 0$.

En nuldivisor er et ikke-nul element der under multiplikation med et andet element afbilder til 0, altså det neutrale element for gruppe-kompositionen, ikke ring-kompositionen. Disse findes ikke for $\mathbb{Z}$, men findes f.eks. for 2×2 matricer.

Enhed

Et element $x \in R$ kaldes en **enhed**, hvis der eksisterer $y \in R$ sådan at $xy = yx = 1$. I dette tilfælde skriver vi y som x^{-1}, altså den inverse til x. Mængden af enheder i R skrives R^*.

En enhed er et element der har en invers i forhold til multiplikation.

Def. 3.1.1

Her følger nogle af de vigtigeste definitioner omkring ringe:

(i) Delring.

(ii) Nuldivisor.

(iii) Enhed.

(iv) Vi siger R er **kommutativ** hvis $xy = yx$ for alle $x, y \in R$.

Multiplikationen i R gør R^* til en Gruppe, $(R^*, \cdot)$. Hvis $R \neq \{0\}$, så $0 \notin R^*$. Gruppen af enheder i en kommutativ Ring R er en abelsk gruppe.

Legeme

En Ring R med $R^* = R \setminus \{0\}$ kaldes et **legeme**.

En ring er et legeme hvis alle elementer, foruden 0, har en invers i forhold til multiplikation (alle elementer skal være Enheder).

Integritetsområde

En Ring, $R \neq \{0\}$, der ikke indeholder Nuldivisorer ($xy = 0, x, y \neq 0$) kaldes et **integritetsområde**.

Del - og udvidelseslegeme

Hvis $K \subseteq L$ er Legemer og K er en Delring af L så er K et **dellegeme** af L, og L er et **udvidelseslegeme** af K.

Prop. 3.1.3

Lad R være et Integritetsområde og $a, x, y \in R$. Hvis $a \neq 0$ og $ax = ay$ så er $x = y$.

Prop. 3.1.4

Lad $\mathbb{F}$ være et Legeme. Så er $\mathbb{F}$ et Integritetsområde.

Et legeme indeholder ingen Nuldivisorer.

Talmængerne $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$

$\mathbb{Z}$ er en Delring af $\mathbb{Q}$ og $\mathbb{Z}^* = \{1, -1\}$. Så $\mathbb{Z}$ er et Integritetsområde, men ikke et Legeme.

Ringen $\mathbb{Q}$ er et legeme, da der for alle brøker gælder $\frac{a}{b} \cdot \frac{b}{a} = 1$, så $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.

$\mathbb{Q}$ er et dellegeme af $\mathbb{R}$ og $\mathbb{R}$ er igen et dellegeme af $\mathbb{C}$ som er et udvidelseslegeme til $\mathbb{R}$.

Ideal

Et ideal i en Ring R er en Undergruppe I af $(R, +)$, sådan at

(i) $\lambda x \in I$ for alle $\lambda \in R$

(ii) $x \in I$

Der gælder at R er et ideal i sig selv. Et ideal I i R udgør hele ringen $R \iff 1 \in I$.

Et ideal er altså en undergruppe af $(R, +)$ der er lukket under multiplikation med elementer i R. Ideal konceptet tillader os at generalisere nogle vigtige egenskaber af heltallene, f.eks. "lige tal" eller "multiplums af 3". Et ideal er en generalisering af en Sideklasse og derved også en Restklasse.

Fra TØ: Hvis $\emptyset \neq I \subseteq R$ så er det nok at vise at I er lukket under addition og skalarmultiplikation.

Ideal frembragt af en mængde

Lad $r_1, \ldots, r_n \in R$. Så er delmængden

$$\langle r_1, \ldots, r_n \rangle = \{\lambda_1 r_1 + \ldots + \lambda_n r_n \mid \lambda_1, \ldots, \lambda_n \in R\}$$

et Ideal i R.

Hvis I er et ideal i R og der eksisterer $r_1, \ldots, r_n \in R$ sådan at $I = \langle r_1, \ldots, r_n \rangle$ siger vi at I er endeligt frembragt af $r_1, \ldots, r_n \in R$.

Så hvis et ideal kan "udspændes" af en mængde elementer $r_1, \ldots, r_n \in R$, siger vi at disse elementer frembringer I. Tænkt basis for et vektorrum og $r_1, \ldots, r_n \in R$ som basisvektorerne for dette.

Bemærkning 3.1.6

Vi kan også snakke om Idealer frembragt af en uendelige mængde. Lad M være en delmængde af R. Så er idealet frembragt af M lig

$$\langle f \mid f \in M \rangle = \{a_1 f_1 + \cdots + a_n f_n \mid n \in \mathbb{N}, a_1, \ldots, a_n \in R, f_1, \ldots, f_n \in M\}$$

Bemærkning 3.1.7

Lad I og J være Idealer i R.

(i) Så er $I \cap J$ og $I + J = \{i + j \mid i \in I, j \in J\}$ også idealer i R.

(ii) Produktet $IJ = \{ij \mid i \in I, j \in J\}$ er et ideal i R.

Bemærk at $IJ \subseteq I \cap J$.

Bemærkning 3.1.8

Et Ideal i et Legeme $\mathbb{F}$ er enten $\langle 0 \rangle$ (Ideal frembragt af en mængde) eller $\mathbb{F}$ selv.

Hovedideal

Et Ideal I i R der kan frembringes af kun et element kaldes et **hovedideal**. Dvs. der eksisterer et $d \in R$ sådan at $I = \langle d \rangle$.

Et hovedideal er et ideal der kan frembringes af kun et element.

Hovedidealområde

Def. 3.1.9: Et Integritetsområde hvor ethvert Ideal er et Hovedideal kaldes et **hovedidealområde**.

Prop. 3.1.10

Ringen $\mathbb{Z}$ er et Hovedidealområde.

Sætning 3.1.11

Ringen bestående af de Gaussiske heltal $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ er et Hovedidealområde.

Bemærk at ringen $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ indeholder idealer der ikke er Hovedidealer.

Kvotientringe (3.2)

Kvotientring

Lad I være et Ideal i en Ring R. Så er I en Undergruppe af den abelske Gruppe $(R, +)$ og mængden

$$R/I = \{[x] \mid x \in R\}$$

bestående af venstre Sideklasser på formen $[x] = x + I$ (da det er i forhold til kompositionen $+$), er en abelsk gruppe.

Dvs. $I \subseteq (R, +)$. $(R/I, +)$ er nu en abelsk gruppe. Vi kan gøre R/I til en ring ved at definere addition og multiplikation på følgende måde:

(i) $[x] + [y] = [x + y]$ for alle $[x], [y] \in R/I$

(ii) $[x][y] = [xy]$ for alle $[x], [y] \in R/I$.

Ringen R/I kaldes kvotientringen af R ved I og har $[0]$ og $[1]$ som neutrale elementer for addition og multiplikation. Der gælder desuden at $[x] = 0$ i $R/I \iff x \in I$.

Kvotientringe i $\mathbb{Z}$

Et Ideal, I i $\mathbb{Z}$ er et Hovedideal $\langle d \rangle$, frembragt af det naturlige tal d. Se sammenhængen med Prop. 2.2.3. To elementer $x, y \in \mathbb{Z}$ repræsenterer det samme element $[x] = [y] \iff x - y \in d\mathbb{Z} \iff d \mid x - y$. Elementerne i $\mathbb{Z}/d\mathbb{Z}$ kan derfor ses som mængden af restklasser ved division med d. Se Kvotientgruppe.

Prop. 3.2.2

Antag $d \in \mathbb{Z}_+$. Så er Gruppen af Enheder $(\mathbb{Z}/d\mathbb{Z})^*$ abelsk med $\phi(d)$ elementer.

Enhederne $x \in (\mathbb{Z}/d\mathbb{Z})^*$ er Indbyrdes primiske med d. Bemærk sammenhængen med Primiske restklasser $(\mathbb{Z}/n\mathbb{Z})^*$.

Prop. 3.2.3

Lad $n \in \mathbb{N}$. Så er $\mathbb{Z}/n\mathbb{Z}$ et Legeme $\iff$ n er et Primtal. Hvis n er et sammensat tal så er $\mathbb{Z}/n\mathbb{Z}$ ikke et Integritetsområde.

$\mathbb{F}_p$

Def. 3.2.5: Legemet $\mathbb{Z}/p\mathbb{Z}$ skrives $\mathbb{F}_p$, hvor p er et Primtal.

Primideal

Prop 3.2.6: Et Ideal, $I \subseteq R$ er et primideal $\iff$ R/I (Kvotientring) er et Integritetsområde.

Ifølge Prop. 3.2.3, hvis n er sammensat tal, så er kvotientringen $\mathbb{Z}/n\mathbb{Z}$ ikke et integritetsområde.

A prime ideal is an ideal I such that whenever $ab \in I \Rightarrow a \in I \vee b \in I$.

Maksimalt ideal

Prop. 3.2.7: Et Ideal $I \subseteq R$ er et maksimalt ideal $\iff$ R/I er et Legeme.

Uddybende: Hvis Kvotientringen R/I er et Legeme så opfylder I følgende:

$$\text{Hvis } I \subsetneq J \Rightarrow J = R$$

Hvor J er et andet ideal i R.

Så er I det vi kalder et maksimalt ideal i R. Hvis R/I er et maksimalt ideal er R/I et legeme.

Bemærk at et maksimalt ideal er et Primideal, da et legeme er et Integritetsområde.

A proper ideal is maximal if it is not contained in any larger proper ideal.

Maksimale idealer i $\mathbb{Z}$

Idealer i $\mathbb{Z}$ er på formen $\langle d \rangle = d\mathbb{Z}$ (Kvotientringe i $\mathbb{Z}$). Et Maksimalt ideal I i $\mathbb{Z}$ er et element $p\mathbb{Z}$ hvor p er et primtal, da kun Kvotientringe på formen $\mathbb{Z}/p\mathbb{Z}$ er Legemer. Se Prop. 3.2.3.

Ringhomomorfier (3.3)

Ringhomomorfi

En afbildning $f : R \to S$ mellem to Ringe R og S kaldes en ringhomomorfi hvis

(i) f er en Gruppehomomorfi fra $(R, +)$ til $(S, +)$

(ii) $f(xy) = f(x)f(y)$ for alle $x, y \in R$

(iii) $f(1) = 1$

Ringisomorfi

En Bijektiv Ringhomomorfi kaldes en ringisomorfi. Hvis R og S er ringe og der eksisterer en ringisomorfi $f : R \to S$ siger vi at R og S er isomorfe, hvilket skrives $R \cong S$.

Kerne og billede af Ringhomomorfi

(i) Kernen *Ker(f)* $= \{r \in R \mid f(r) = 0\} \subseteq R$ af f er et Ideal i R.

(ii) Billedet $f(R)$ er en Delring af S

Prop. 3.3.2

Lad R og S være Ringe og $f : R \to S$ en Ringhomomorfi med kernen $K = Ker(f)$. Så er

$$\tilde{f} : R/K \to f(R)$$

givet ved $\tilde{f}(r + k) = f(r)$ en Veldefineret afbildning og en Ringisomorfi. Se Isomorfisætningen.

Entydig ringhomomorfi fra $\mathbb{Z}$

Lemma 3.3.3: For enhver Ring R, eksisterer der en unik Ringhomomorfi

$$f : \mathbb{Z} \to R$$

Bemærkning 3.3.4

Lad $f : \mathbb{Z} \to R$ være den entydige Ringhomomorfi for en given Ring. For $n \geq 0$, tænker vi $f(n)$ som

$$f(n) = 1 + 1 + \cdots + 1,$$

altså en sum af n kopier af $1 \in R$.

Dvs. givet den entydige ringhomomorfi giver det mening at se alle elementer i en ring som værende heltal. Når $n \in \mathbb{Z}$ og vi derved skriver $n \in R$ menes der altså det f afbilder til, altså $n \in R = f(n) \in R$.

Karakteristik af en ring

Lad R være en Ring. Lad nu skrivemåden $ord(1)$ være ordnen (Ordnen af et element) af $1 \in (R, +)$.

(i) Hvis $ord(1)$ er uendelig siger vi at karakteristikken af R er nul.

(ii) Hvis $ord(1)$ er endelig siger vi at karakteristikken af R er endelig, $ord(1)$.

(iii) $Char(R)$ kan man tænke på som det mindste $n \in \mathbb{N}$ for hvilket der gælder $1_1 + \cdots + 1_n = 0$ i R.

Ringene $\mathbb{Z}, \mathbb{Q}$ og $\mathbb{R}$ har karakteristikken nul. Dog er karakteristikken for $\mathbb{Z}/n\mathbb{Z} = n$ for et $n \in \mathbb{N}$.

Lemma 3.3.5

Lad R være en Ring. Så eksisterer der en Injektiv Ringhomomorfi

$$\mathbb{Z}/n\mathbb{Z} \to R$$

hvor $n = char(R)$.

Vi siger at $\mathbb{Z}/n\mathbb{Z}$ er indeholdt i R, da den er isormorf til en Delring i R.

Prop 3.3.7

Lad R være et Integritetsområde. Så er $char(R)$ enten nul eller et Primtal. Hvis R er endelig er R et Legeme (et endeligt integritetsområde er et legeme), og $char(R)$ er et primtal.

If $\phi : \mathbb{Z} \to R$ is the unique ring homomorphism from $\mathbb{Z}$ to R, then $Ker(\phi) = (p)$, so char(R) is a prime number or zero.

Lemma 3.3.8

Lad R være en Ring og $a, b \in R$. Så gælder

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \cdots + \binom{n}{n-1} ab^{n-1} + b^n$$

for $n \in \mathbb{N}$. Bemærk

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

.

Læg mærke til at i hvert led, $a^y * b^x$, så gælder $y + x = n$. Altså dekrement as potens og inkrement bs ved hvert led op til $n - 1$.

Bemærk at vi ser binomialkoefficienterne ser som elementer i R, vi bruger dem vha. den Entydig ringhomomorfi fra $\mathbb{Z}$.

Freshman's Dream

Sætning 3.3.9: Lad R være en Ring med primkarakteristik p (Karakteristik af en ring). Så gælder

$$(x+y)^{p^r} = x^{p^r} + y^{p^r}$$

for alle $x, y \in R$ og $r \in \mathbb{N}$.

Bemærkning 3.3.10

Bemærk at hvis R er en Ring med primkarakteristik p så viser Freshman's Dream at

$$F : R \to R$$

givet ved $F(x) = x^p$ er en Ringhomomorfi. Det kaldes Frobenius afbildningen.

Entydig faktorisering (3.5)

Associerede elementer

To elementer, $x, y \in R$ hvor R er et Integritetsområde siges at være associerede hvis $x \mid y \wedge y \mid x$.

Irreducibelt element

Et element $r \in R \setminus R^*$ siges at være irreducibelt hvis $r = ab$, hvor $a, b \in R$ medføre at a eller b er en Enhed.

Et element, som ikke er en enhed, siges at være irredicubelt hvis det er et produkt af to elementer, hvor en af disse er en enhed.

Et ikke-nul element $x \in R \setminus R^*$ siges at have en **faktorisering til irreducible elementer** hvis der eksisterer irreducible elementer $p_1, \ldots, p_r \in R$ sådan at

$$x = p_1 \cdots p_r$$

Entydig faktorisering til irreducible elementer

Vi siger ydermere at x har en **entydig faktorisering til irreducible elementer** hvis der for alle andre faktorisering til irreducible elementer,

$$x = q_1 \cdots q_s$$

gælder at $p_i \mid q_i$. Dette medføre at $p_i = uq_i$, hvor u er en enhed.

Faktoriel ring

Et Integritetsområde R, hvor ethvert ikke-nul element i $R \setminus R^*$ har Entydig faktorisering til irreducible elementer kaldes en faktoriel ring.

Primelement

Et ikke-nul element $p \in R \setminus R^*$ siges at være et primelement hvis $p \mid xy \Rightarrow p \mid x \vee p \mid y$, for $x, y \in R$. Se Lemma 1.8.3.

Prop. 3.5.2

Et Primelement er et Irreducibelt element.

Prop. 3.5.3

Lad R være en Ring hvor ethvert ikke-nul element $x \in R \setminus R^*$ har en faktorisering til irreducible elementer.

Ethvert Irreducibelt element er et Primelement i $R \iff R$ er en Faktoriel ring.

Bemærkning 3.5.4

Ringen $\mathbb{Z}[\sqrt{-5}]$ er ikke en Faktoriel ring da elementet $6 \in \mathbb{Z}[\sqrt{-5}]$ har to faktoriseringen til irreducible elementer,

$$6 = 2 * 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Lemma 3.5.5

Lad R være et Hovedidealområde og r et ikke-nul element i R. Så har r en irreducibel faktorisering.

Prop. 3.5.6

Antag R er et Hovedidealområde der ikke er et Legeme. Et ideal $\langle x \rangle \subseteq R$ er et Maksimalt ideal $\iff$ x er et Irreducibelt element i R.

Sætning 3.5.7

Et Hovedidealområde R er en Faktoriel ring.

Euklidisk ring

Et Integritetsområde kaldes en euklidisk ring hvis der eksisterer en euklidisk afbildning

$$N : R \setminus \{0\} \to \mathbb{N}$$

Denne afbildning skal tilfredsstille at for alle $x \in R, d \in R \setminus \{0\}$ eksisterer $q, r \in R$ sådan at

$$x = qd + r$$

hvor enten $r = 0$ eller $N(r) < N(d)$. Se Entydig rest.

For hetalsringen $\mathbb{Z}$ er afbildningen $|\cdot| : \mathbb{Z} \to \mathbb{N}$ en euklidisk afbildning (absolutte værdi).

Prop. 3.5.9

En Euklidisk ring R er et Hovedidealområde.

De Gaussiske heltal $Z[i]$

De gaussiske heltal $Z[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ er en Euklidisk ring.

Prop. 3.5.11

Lad $\pi = a + bi \in \mathbb{Z}[i]$ være et gaussisk heltal med $N(\pi) = a^2 + b^2 = p$, hvor p er et Primtal. Så er π et Primelement i $\mathbb{Z}[i]$.

Lemma 3.5.12 (Lagrange)

Lad p være et Primtal. Hvis $p \equiv 1 \pmod 4$ så kan kongruencen

$$x^2 \equiv -1 \pmod p$$

løses ved $x = (2n)!$, hvor $p = 4n + 1$.

Korollar 3.5.14

Et Primtal $p \equiv 1 \pmod 4$ er ikke et Primelement i $\mathbb{Z}[i]$.

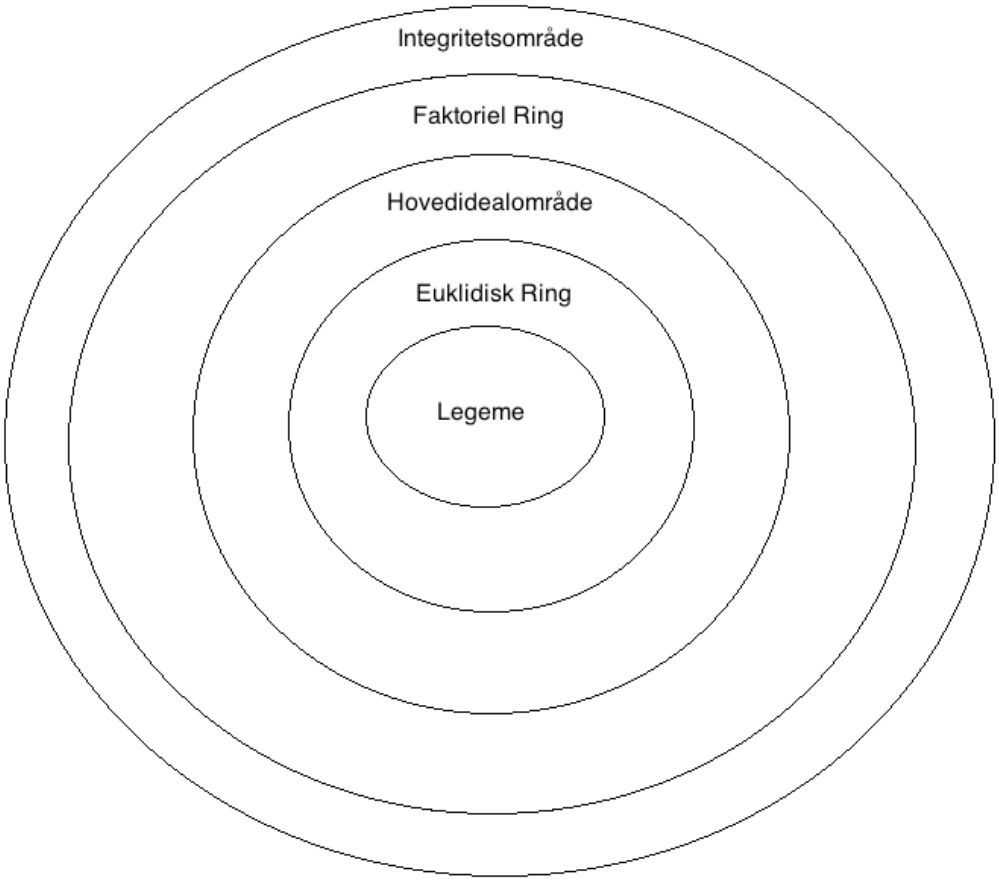
Sætning 3.5.15 (Fermat)

Et Primtal $p \equiv 1 \pmod 4$ er en sum af to entydige kvadrater.

Lemma 3.5.18

Et Primtal $p \equiv 3 \pmod 4$ er et Primelement i $Z[i]$.

Ringklasser



Polynomier (4)

Polynomiumsringe (4.1)

Lad R være en Ring og $R[\mathbb{N}]$ mængden af afbildninger

$$f : \mathbb{N} \to R$$

sådan at $f(n) = 0$ for $n \gg 0$, hvilket vil sige at der findes et tal N, så $f(n) = 0$ for alle $n > N$.

Givet $f, g \in R[\mathbb{N}]$ definerer vi deres sum

$$\begin{aligned}(f+g)(n) &= f(n) + g(n) \\ &= (a_0 + a_1 x + \cdots + a_n x^n) + (b_0 + b_1 x + \cdots + b_n x^n) \\ &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n \\ &= \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i \\ &= \sum_{i=0}^{n} (a_i + b_i) x^i\end{aligned}$$

og deres produkt

$$\begin{aligned}(fg)(n) &= f(n)g(n) \\ &= (a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_n x^n) \\ &= (a_0 b_0) + (a_1 b_0 + a_0 b_1)x + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \cdots \\ &= \sum_{i=0}^{n} a_i x^i \sum_{j=0}^{n} b_i x^i \\ &= \sum_{k=0}^{2n} \sum_{i+j=k} (a_i b_j) x^k\end{aligned}$$

Vi lader $X^i \in R[\mathbb{N}]$ være afbildningen

$$X^i(n) = \begin{cases} 1 & \text{if } n = i \\ 0 & \text{if } n \neq i \end{cases}$$

Vi lader nu elementerne i ringen $a \in R$ være givet ved afbildningen

$$a(n) = \begin{cases} a & \text{if } n = 0 \\ 0 & \text{if } n > 0 \end{cases}$$

Derved kan et element $f \in R[\mathbb{N}]$ skrives som

$$f = a_0 + a_1 X + \cdots + a_n X^n$$

hvor $a_i = f(i)$ og $f_i = 0$ hvis $i > n$.

Polynomiumsring

Vi definerer polynomiumsringen $R[X]$ i en variabel over Ringen R, som $R[\mathbb{N}]$. $X = X^1 \in R[\mathbb{N}]$. Et polynomium $f \in R[X]$ kan skrives

$$a_0 + a_1 X + \cdots + a_n X^n$$

(i) Et *led* er et polynomium på formen aX^m, hvor $a \in R \setminus \{0\}$.

(ii) $a_0, \ldots, a_n \in R$ kaldes f's koefficienter.

(iii) Hvis $a_n \neq 0$ er $deg(f) = n$ og a_n er den ledende koefficient.

(iv) $deg(f)$ kaldes graden af f og $a_{deg(f)}X^{deg(f)}$ er det ledende led.

(v) Et ikke-nul polynomium kaldes normeret hvis dets ledende koefficient er 1.

Bemærkning 4.1.3

To polynomier $f = a_0 + a_1X + \cdots + a_nX^n$ og $g = b_0 + b_1X + \cdots + b_mX^m$ i $R[X]$ er ens $\iff$ $a_0 = b_0, a_1 = b_1, \ldots$. Dette giver også mening når vi ser polynomier som afbildninger $f : \mathbb{N} \to R$, hvor to afbildninger er ens $\iff$ de afbilder til samme værdi for alle $n \in N$.

Division af Polynomier (4.2)

Prop. 4.2.2

Lad $f, g \in R[X] \setminus \{0\}$. Hvis den ledende koefficient af f eller g ikke er en Nuldivisor gælder

$$deg(fg) = deg(f) + deg(g)$$

Prop. 4.2.3

Lad R være et Integritetsområde. Så er $R[X]^* = R^*$.

Prop. 4.2.4

Lad $d \in R[X]$ være et ikke-nul polynomium. Antag at den ledende koefficient af d ikke er en Nuldivisor i R. Givet $f \in R[X]$, eksisterer der polynomier $q, r \in R[X]$ sådan at

$$f = qd + r$$

hvor $r = 0$ eller at d's ledende led ikke dividerer nogle af r's led. Se Entydig rest.

Korollar 4.2.5

Lad $d \in R[X]$ være et ikke-nul polynomium. Antag at den ledende koefficient af d er invertibel (er en Enhed) i R. Givet $f \in R[X]$, eksisterer der polynomier $q, r \in R[X]$ sådan at

$$f = qd + r$$

hvor $r = 0$ eller $deg(r) < deg(d)$.

Def. 4.2.7

Polynomiet r i Korollar 4.2.5 kaldes resten af f divideret med d.

Polynomiumsrødder (4.3)

Afbildningen

$$j : R \to R[X]$$

givet ved $j(r) = r + 0X + 0X^2 + \cdots$ er en Injektiv Ringhomomorfi. Billedet $j(R) = R$ og derved ser vi R som en Delring af $R[X]$.

Prop. 4.3.1

Lad $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$ og $\alpha \in R$. Afbildningen $\phi_\alpha : \mathbb{R}[X] \to R$ givet ved

$$\phi_\alpha(f) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

er en Ringhomomorfi.

Vi holder altså et α fast og givet et vilkårligt polynomium kan vi indsætte dette α i stedet for X og få en Ringhomomorfi.

Rod

Lad $f \in R[X]$ være et polynomium. Elementet $\alpha \in R$ siges at være en rod i f hvis $f(\alpha) = \phi_\alpha(f) = 0$.

Vi lader $V(f) = \{\alpha \in R \mid f(\alpha) = 0\}$ være mængden af rødder for $f \in R[X]$.

Korollar 4.3.2

Lad $f \in R[X]$. Så er $\alpha \in R$ en Rod i $f \iff X - \alpha \mid f$.

Multiplicitet af en rod

Multipliciteten af en Rod α i et ikke-nul polynomium f er den største potens $n \in \mathbb{N}$ sådan at

$$(X - \alpha)^n \mid f$$

Multipliciteten af α i f skrives $\nu_\alpha(f)$. Bemærk at

(i) $\nu_\alpha(f) \leq deg(f)$.

(ii) $f = (X - \alpha)^{\nu_\alpha(f)}h$, hvor $h(\alpha) \neq 0$.

Multipel rod

En multipel rod i f er en Rod $\alpha \in R$ med $\nu_\alpha(f) > 1$.

Lemma 4.3.4

Lad R være et Integritetsområde og $f, g \in R[X]$. Så gælder

$$V(fg) = V(f) \cup V(g)$$

Sætning 4.3.5

Lad R være et Integritetsområde of $f \in R[X] \setminus \{0\}$. Hvis $V(f) = \{\alpha_1, \ldots, \alpha_r\}$ så

$$f = q(X - \alpha_1)^{\nu_{\alpha_1}(f)} \cdots (X - \alpha_r)^{\nu_{\alpha_r}(f)}$$

hvor $q \in R[X]$ og $V(q) = \emptyset$. Antallet af Rodder i f, talt med multiplicitet, er bundet af graden af f, $deg(f)$.

NB. Gælder kun hvis R er et Integritetsområde, så ikke i $\mathbb{Z}/n\mathbb{Z}$, hvor n er sammensat f.eks..

Differentiering af polynomier

Lad R være en Ring og $f = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + a_nX^n \in R[X]$. Så siger vi

$$D(f) = a_1 + \cdots + a_{n-1}(n-1)X^{n-2} + a_n nX^{n-1}$$

er den afledede af f.

Når vi ser polynomier som afbildninger $f : \mathbb{N} \to R$, kan ovenstående omformuleres til

$$D(f)(n-1) = nf(n) \text{ for } n \geq 1$$

Lemma 4.3.7

Lad $f, g \in R[X]$ og $\lambda \in R$. Så gælder

(i) $D(f+g) = D(f) + D(g)$

(ii) $D(\lambda f) = \lambda D(f)$

(iii) $D(fg) = fD(g) + D(f)g$

Lemma 4.3.8

Lad $f, g \in R[X]$.

(i) Hvis $f^2 \mid g \Rightarrow f \mid D(g)$

(ii) Et element $\alpha \in R$ er en Multipel rod i $f \iff \alpha$ er en Rod i f og $D(f)$.

Bemærkning 4.3.9

Hvis Polynomiumsringen $R[X]$ har en primisk karakteristik $p > 0$ (Karakteristik af en ring) findes der mange ikke-konstante polynomier $f \in R[X]$, hvor $D(f) = 0$.

F.eks. $X^p \in \mathbb{F}_p[X]$. Her er

$$D(X^p) = pX^{p-1} = 0$$

da $X^{p-1} \equiv 1 \pmod{p}$ ifølge Fermats lille sætning.

Generelt gælder $D(X^n) = 0 \iff p \mid n$ når $X^n \in \mathbb{F}_p[X]$.

Cyklotomiske polynomier (4.4)

Enhedsrod

Et komplekst tal ξ siges at være en enhedsrod af n-te grad for et $n \in \mathbb{N}$ hvis $\xi^n = 1$.

Skriver vi enhedsroden ξ i polære koordinater $re^{i\theta} = r(\cos\theta + i\sin\theta)$ følger det at $r = 1$ og $\theta = k2\pi i/n$ for $k = 0, \ldots, n-1$, hvis ξ er af n-te grad.

Lemma 4.4.1

Et komplekst tal ζ er en Primitiv enhedsrod af n-te grad $\iff$

$$\zeta = e^{k2\pi i/n}$$

hvor $1 \leq k \leq n$ og $gcd(k, n) = 1$. Husk fra Enhedsrod at $\theta = k2\pi i/n$.

Hvis ζ er en primitiv enhedsrod af n-te grad og $\zeta^m \Rightarrow n \mid m$.

Bemærkning

Mængden af enhedsrødder af n-te grad er en Undergruppe af $\mathbb{C}^*$. Denne undergruppe er isomorf til den Cyklisk gruppe $\mathbb{Z}/n\mathbb{Z}$.

Cyklotomisk polynomium

Def. 4.4.2: Lad $n \in \mathbb{N}$ hvor $n \geq 1$. Det n-te cyklotomiske polynomium er defineret som polynomiet

$$\Phi_n(X) = \prod_{1 \leq k \leq n,\ gcd(k,n1)=1} (X - e^{k2\pi i/n})$$

i $\mathbb{C}[X]$.

Et cyklotomisk polynomium er et polynomium hvis rødder er alle Primitiv enhedsroder af n-te grad. Det ses at det opfylder Lemma 4.4.1.

Bemærk at $deg(\Phi_n) = \phi(n)$

Koefficienterne af Φ_n er altid $= \pm 1$ hvis n er et produkt af two forskellige Primtal. Se side 156 for at se de 4 første cykoltomiske polynomier.

Prop. 4.4.3

Lad $n \geq 1$. Så gælder

(i) $X^n - 1 = \prod_{d|n} \Phi_d(X)$

(ii) Et Cyklotomisk polynomium har heltalskoefficienter

$$\Phi_n(X) \in \mathbb{Z}[X]$$

Lad R være en Ring. Den Entydig ringhomomorfi fra $\mathbb{Z}$ $\kappa : \mathbb{Z} \to R$ giver en Ringhomomorfi.

$$\kappa' : \mathbb{Z}[X] \to R[X]$$

På denne måde kan vi se et Cyklotomisk polynomium $\Phi_n(X) \in \mathbb{Z}[X]$ som polynomiet $\kappa'(\Phi_n) \in R[X]$. Dette leder os tilbage til identiteten

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

i $R[X]$ ved at anvende κ' på den tilsvarende identitet i $\mathbb{Z}[X]$.

Primitive rødder (4.5)

Primitiv enhedsrod

Def. 4.5.1: Lad R være en Ring og $n \in \mathbb{N} \setminus \{0\}$. Et element $\alpha \in R$ siges at være en primitiv Enhedsrod af n-te grad i R hvis $\alpha^n = 1$ og

$$a, a^2, .., a^{n-1} \neq 1$$

hvor $n \geq 1$.

Lemma 4.5.2

Lad $\alpha \in R$, hvor R er et Integritetsområde. Hvis $\Phi_n(\alpha) = 0$ og α ikke er en Multipel rod i $X^n - 1 \in R[X] \Rightarrow \alpha$ er en Primitiv enhedsrod af n-te grad i R.

Sætning 4.5.3 (Gauss)

Lad $\mathbb{F}$ være et Legeme og $G \subseteq \mathbb{F}^*$ en endelig Undergruppe af Enhederne i $\mathbb{F}$. Så er G en Cyklisk gruppe.

Denne sætning viser at ${\mathbb{F}_p}^*$ er en cyklisk gruppe, hvor p er et Primtal.

Et heltal a, sådan at $[a]$ frembringer $\mathbb{F}_p^*$, kaldes en primitiv rod modulo p. En primitiv rod a modulo p tilfredsstiller

$$\mathbb{F}_p^* = \{[1], [a], [a^2], \ldots, [a^{p-2}]\}$$

Se side 159 for mere om primitive rødder modulo p.

Idealer i polynomiumsringe (4.6)

Prop. 4.6.1

Polynomiumsringen $\mathbb{F}[X]$, hvor $\mathbb{F}$ er et Legeme er en Euklidisk ring, et Hovedidealområde og et Faktoriel ring.

Prop. 4.6.3

Lad $f \in \mathbb{F}[X]$. Så gælder

(i) Idealet $\langle f \rangle$ er et Maksimalt ideal $\iff$ f er et Irreducibelt element. I dette tilfælde er Kvotientringen

$$\mathbb{F}[X]/\langle f \rangle$$

et Legeme.

(ii) Hvis $f \neq 0$ så er f en Enhed $\iff$ $deg(f) = 0$.

(iii) Hvis $deg(f) = 1$ så er f et Irreducibelt element.

(iv) Hvis f er irreducibelt og $deg(f) > 1$ har f ingen Rodder.

(v) Hvis $deg(f) = 2$ *eller* $deg(f) = 3$ så er f irreducibelt $\iff$ f ingen rødder har.

Se s. 164-165 for yderligere småting omkring idealer.

Prop. 4.6.7

Lad R være en Ring og

$$f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$$

et normeret (ledende koeff $= 1$) polynomium med $deg(f) = n > 0$.

(i) Så er $R \cap \langle f \rangle = \langle 0 \rangle$.

(ii) Elementerne $[g] = g + \langle f \rangle$ i Kvotientringen $R[X]/\langle f \rangle$ kan entydigt udtrykkes som polynomier af grad $< n$

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

hvor $b_0, \ldots, b_{n-1} \in R$ og $\alpha = [X]$.

(iii) I $R[X]/\langle f \rangle$ har vi identiteten

$$\alpha^n = -a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1}$$

Bemærk at R er en naturlig Delring af $R[X]/\langle f \rangle$. Den naturlige Ringhomomorfi

$$\phi : R \to R[X]/\langle f \rangle$$

givet ved $\phi(r) = [r]$ er Injektiv.

Bemærkning 4.6.8

Hvis $\mathbb{F}$ er et Legeme og $f \in \mathbb{F}[X]$ er et Irreducibelt element så er $\langle f \rangle$ et Hovedideal og derved bliver $\mathbb{F}[X]/\langle f \rangle$ et udvidelseslegeme E til $\mathbb{F}$.

Nu viser det sig at $\alpha = [X] \in E$ og er en Rod til $f \in \mathbb{F}[X] \subseteq E[X]$, da $f(\alpha) = 0$ fra Prop. 4.6.7.

Endelige legemer (4.8)

Lemma 4.8.1

Lad $\mathbb{F}$ være et endeligt Legeme. Så er $|\mathbb{F}| = p^n$, hvor p er et Primtal, $n \geq 1$ og der eksisterer et Irreducibelt element $f \in \mathbb{F}_p[X]$ af grad n, sådan at

$$\mathbb{F} \cong \mathbb{F}_p[X]/\langle f \rangle$$

Sætning 4.8.2

Der eksisterer et entydigt endeligt Legeme med p^n elementer, hvor p er et primtal og $n \geq 1$. Der gælder yderligere

(i) Der eksisterer et Irreducibelt element i $\mathbb{F}_p[X]$ af grad n.

(ii) Antag at $\mathbb{F}$ og $\mathbb{F}$' er endelige legemer med p^n elementer. Så eksisterer der er Ringisomorfi (Ringhomomorfi) $\mathbb{F} \xrightarrow{\sim} \mathbb{F}'$.

Lemma 4.8.3

Lad $\tau, d, n \in \mathbb{N}$, hvor $\tau > 1$. Så $t^d - 1 \mid t^n - 1 \iff d \mid n$.

Sætning 4.8.5

Der eksisterer et Irreducibelt element i $\mathbb{F}_p[X]$ af grad $n \geq 1$. Hvis f er irreducibelt og $f \mid \Phi_{p^n-1}$ i $\mathbb{F}_p[X]$ så er $deg(f) = n$.

Gröbner baser (5)

Polynomier i flere variable (5.1)

Vi husker hvordan vi definerede en Polynomiumsring i en variabel. Vi udvider nu dette til en polynomiumsring i flere variable $R[X_1, \ldots, X_n]$ som

$$R[X_1, \ldots, X_n] = R[\mathbb{N}^n] = \{f : \mathbb{N}^n \to R \mid f(v) = 0, |v| \gg 0\}$$

hvor $v = (v_1, \ldots, v_n) \in \mathbb{N}^n$ og $|v| = v_1 + \cdots + v_n$.

Et polynomium $f \in R[X_1, \ldots, X_n]$ er altså det samme som en afbildning

$$f : \mathbb{N}^n \to R$$

der er ikke-nul for kun endeligt mange v.

Vi lader $X^v \in R[\mathbb{N}^n]$ være afbildningen

$$X^v(w) = \begin{cases} 1 & \text{if } v = w \\ 0 & \text{if } v \neq w \end{cases}$$

Med denne notation kan vi nu skrive polynomier i flere variable, $f \in R[\mathbb{N}^n]$, som en endelig sum

$$f = \sum_{v \in N^n} a_v X^v$$

hvor $a_v \in R$.

Vi definerer addition af to polynomier $f, g \in R[\mathbb{N}^n]$ på følgende vis

$$f + g = (f + g)(v) = f(v) + g(v)$$

og multiplikation fg som den endelige sum

$$(fg)(v) = \sum_{v_1 + v_2 = v} f(v_1)g(v_2)$$

hvor $v_1, v_2 \in \mathbb{N}^n$.

Bemærk at

(i) $0 \in R$ er det neutrale element for $+$.

(ii) Afbildningen $X^{(0,0,\ldots,0)}$ der afbilder 0-vektoren i $\mathbb{N}^n$ til $1 \in R$ og alt andet til $0 \in R$ til at være det neutrale element for $\cdot$.

Ved notationen $R[X_1, \ldots, X_n]$ for $R[\mathbb{N}^n]$ menes

(i) $X_1 = X^{(1,0,\ldots,0)}$

(ii) $X_2 = X^{(0,1,\ldots,0)}$

(iii) $X_n = X^{(0,0,\ldots,1)}$

Et *led* er et polynomium $rX^v \in R[\mathbb{N}^n]$, hvor $r \in R \setminus \{0\}$ kaldes *koefficienten*.

Som eksempel kan vi skrive polynomiet f op på to ens måder, en formel og en konkret. De er ækvivalente

$$\begin{aligned} f &= 2X^{(0,0,0)} + 2X^{(1,0,3)} + X^{(2,1,0)} - X^{(0,1,1)} + 3X^{(1,1,1)} \in \mathbb{Z}[\mathbb{N}^3] \\ &= 2 + 2TZ^3 + T^2Y - YZ + 3TYZ \in \mathbb{Z}[T, Y, Z] \end{aligned}$$

hvor $T = X^{(1,0,0)}, Y = X^{(0,1,0)}$ og $Z = X^{(0,0,1)}$. Det formelle polynomium er nu udtrykt ved de 3 variable T, Y, Z.

Termordning

Def. 5.1.2: Mængden $\mathbb{N}^n$, bestående af n-tupler af naturlige tal, har en komponentvis addition $+$ med nul-vektoren $0 = (0, \ldots, 0)$. En Partiel ordning $\leq$ på $\mathbb{N}^n$ kaldes en termordning hvis

(i) $\leq$ er en Total ordning.

(ii) $0 \leq v$

(iii) $v_1 \leq v_2 \Rightarrow v_1 + v \leq v_2 + v$

$\forall v, v_1, v_2 \in N^n$.

Leksikografisk ordning

Vi definerer den leksikografiske ordning $\leq_{lex}$ på $\mathbb{N}^n$ ved

$$(v_1, \ldots, v_n) \leq_{lex} (w_1, \ldots, w_n)$$

hvis en af følgende gælder

$$\begin{aligned}
&(v_1 < w_1) \quad \text{eller} \\
&(v_1 = w_1) \text{ og } (v_2 < w_2) \quad \text{eller} \\
&(v_1 = w_1) \text{ og } (v_2 = w_2) \text{ og } (v_3 < w_3) \quad \text{etc}
\end{aligned}$$

Dette vil sige normal alfabetisk ordning. F.eks. $(1, 1, 3) \leq_{lex} (1, 2, 3)$ da $1 < 2$ og $(4, 5, 1) \leq_{lex} (4, 5, 3)$ da $1 < 3$. Den leksikografiske ordning er en Termordning.

Graderet leksikografisk ordning

Lad $|v| = v_1 + \cdots + v_n$, hvor $v = (v_1, \ldots, v_n) \in \mathbb{N}^n$. Vi definerer nu den graderede leksikografiske ordning ved

$$(v_1, \ldots, v_n) \leq_{grlex} (w_1, \ldots, w_n)$$

hvis

$$\begin{aligned}
&|v| < |w| \quad \text{eller} \\
&|v| = |w| \text{ og } v \leq_{lex} w
\end{aligned}$$

F.eks. $(2, 1, 1) \leq_{grlex} (1, 2, 3)$, da $(2 + 1 + 1 < 1 + 2 + 3)$, selvom
$(2, 1, 1) \geq_{lex} (1, 2, 3)$. Den graderede leksikografiske ordning er en Termordning.

Lemma 5.1.5 (Dickson)

Lad S være en delmængde af $\mathbb{N}^n$. Så er der en endelig mængde af vektorer $v_1, \ldots, v_r \in S$ sådan at

$$S \subseteq (v_1 + \mathbb{N}^n) \cup \cdots \cup (v_r + \mathbb{N}^n)$$

hvor $v_i + \mathbb{N}^n = \{v_i + w \mid w \in \mathbb{N}^n\}$ for en vektor $v_i \in \mathbb{N}^n$.

Korollar 5.1.7

En Termordning $\leq$ på $\mathbb{N}^n$ er en Velordning.

Initialterm (5.2)

Initialterm

Def. 5.2.1: Lad

$$f = \sum_{v \in \mathbb{N}^n} a_v X^v$$

være et ikke-nul polynomium i $R[\mathbb{N}^n]$ og $\leq$ er Termordning på $\mathbb{N}^n$.

Initialtermet af f mht. $\leq$ er defineret som

$$in_{\leq}(f) = a_w X^w$$

hvor $w = max_{\leq}\{v \in \mathbb{N}^n \mid a_v \neq 0\}$.

F.eks. Lad

$$f = X^2 + XY + Y + Y^3 + X^5 \in \mathbb{Z}[X, Y]$$

hvor $X = X^{(1,0)}$ og $Y = X^{(0,1)}$ i $\mathbb{Z}[\mathbb{N}^n]$. Derved er

$$f = X^{(2,0)} + X^{(1,1)} + X^{(0,1)} + X^{(0,3)} + X^{(5,0)} \in \mathbb{Z}[\mathbb{N}^2]$$

Lader vi nu $\leq = \leq_{lex}$ får vi

$$(5,0) \geq (2,0) \geq (1,1) \geq (0,3) \geq (0,1)$$

Efter denne orden skulle man skrive $f = X^5 + X^2 + XY + Y^3 + Y$. Derved er

$$in_{\leq}(f) = X^5$$

Bemærkning 5.2.3

Lad R være et Integritetsområde og $f, g \in R[X_1, \ldots, X_n]$. Så gælder

$$in_{\leq}(fg) = in_{\leq}(f) in_{\leq}(g)$$

Dette er en analogt med Prop. 4.2.2, for polynomier i en variabel.

Divisionsalgoritmen (5.3)

Prop. 5.3.1

Prop. 5.3.1: Hold en Termordning $\leq$ på $\mathbb{N}^n$ fast. Lad $f \in R[X_1, \ldots, X_n] \setminus \{0\}$ og antag at $f_1, \ldots, f_m \in R[X_1, \ldots, X_n]$ er en sekvens af ikke-nul polynomier. Så eksisterer der $a_1, \ldots, a_m, r \in R[X_1, \ldots, X_n]$ sådan at

$$f = a_1 f_1 + \cdots + a_m f_m + r$$

hvor $r = 0$ eller ingen af leddene i r er delelig med $in_{\leq}(f_1), \ldots, in_{\leq}(f_n)$. Desuden er $in_{\leq}(a_i f_i) \leq in_{\leq}(f)$ hvis $f_i \neq 0$. Se Prop. 4.2.4 for algoritmen i en variabel.

Def. 5.3.2

Antag $f \in R[X_1, \ldots, X_n]$ og lad $F = (f_1, \ldots, f_m)$ være en sekvens af ikke-nul polynomier i $R[X_1, \ldots, X_n]$. Vi lader f^F beskrive resten r af f efter division med F vha. Prop. 5.3.1.

Gröbnerbaser (5.4)

Gröbnerbasis

Lad R være et Legeme.

En mængde af ikke-nul polynomier

$$F = (f_1, \ldots, f_m) \subseteq R[X_1, \ldots, X_n]$$

kaldes en Gröbnerbasis for et Ideal i $R[X_1, \ldots, X_n]$ mht. en Termordning $\leq$ hvis

(i) $F \subseteq I$

(ii) For alle $f \in I \setminus 0$,

$$in_{\leq}(f_i) \mid in_{\leq}(f)$$

for et $i = 1, \ldots, m$.

Mængden F kaldes en Gröbnerbasis mht en termordning $\leq$ hvis den er en Gröbnerbasis for idealet $\langle f_1, \ldots, f_m \rangle$ mht. $\leq$.

Prop. 5.4.2

Lad R være et Legeme. Lad $G = (f_1, \ldots, f_m)$ være en Gröbnerbasis mht en Termordning $\leq$. For et polynomium $f \in R[X_1, \ldots, X_n]$ har vi

$$f \in I \iff f^G = 0$$

hvor $I = \langle f_1, \ldots, f_m \rangle$. Se Def. 5.3.2 for f^G.

Korollar 5.4.5

Lad R være et Legeme. Lad $G = (f_1, \ldots, f_m) \subseteq R[X_1, \ldots, X_n]$ være en Gröbnerbasis for Idealet $I \subseteq R$ mht en Termordning. Så er

$$I = \langle f_1, \ldots, f_m \rangle$$

Prop. 5.4.6

Lad R være et Legeme. Lad $G = (f_1, \ldots, f_m)$ være en Gröbnerbasis i $R[X_1, \ldots, X_n]$ mht en Termordning $\leq$. Så er den entydige rest r i

$$f = a_1 f_1 + \cdots + a_m f_m + r$$

ligesom i Prop. 5.3.1, *entydig* for alle $f \in R$.

Resten fra divisionsalgoritmen er uafhængig af rækkefølgen af elementerne $f_1, \ldots, f_m \in G$.

Sætning 5.4.7

Lad k være et Legeme, $\leq$ en Termordning og $I \subseteq k[X_1, \ldots, X_n]$ et Ideal. Så har I en Gröbnerbasis mht $\leq$.

Korollar 5.4.8

Lad R være et Legeme. Lad I være et arbitrært Ideal i $R[X_1, \ldots, X_n]$. Så er der endeligt mange polynomier $f_1, \ldots, f_m \in I$ sådan at ethvert polynomium $f \in I$ kan skrives

$$f = a_1 f_1 + \cdots + a_m f_m$$

for passende $a_1, \ldots, a_m \in R[X_1, \ldots, X_n]$, hvilket vil sige $I = \langle f_1, \ldots, f_m \rangle$.

S-polynomiet

Def. 5.6.5: S-polynomiet af to ikke-nul polynomier f og g mht en Termordning $\leq$ er defineret som

$$S(f,g) = \frac{X^w}{in_{\leq}(f)} f - \frac{X^w}{in_{\leq}(g)} g$$

hvor X^w er $lcm(in_{\leq}(f), in_{\leq}(g))$.

Newton Genvisit (5.5)

Sætning 5.5.1

Lad $f, f_1, \ldots, f_r \in k[X_1, \ldots, X_n]$. Lad I være idealet

$$I = \langle T_1 - f_1, \ldots, T_r - f_r \rangle$$

i Polynomiumsringen $A = k[X_1, \ldots, X_n, T_1, \ldots, T_r]$ og $\leq$ være den Leksikografisk ordning givet ved

$$T_r \leq \cdots \leq X_n \leq \cdots \leq X_1$$

Lad G være en Gröbnerbasis for I mht $\leq$.

Så kan f skrives som et polynomium i $f_1, \ldots, f_r \iff$

$$f^G \in k[T_1, \ldots, T_r]$$

I dette tilfælde er $f = f^G(f_1, \ldots, f_r)$.

Buchbergers S-kriterie (5.6)

Korollar 5.6.9

En sekvens $F = (f_1, \ldots, f_m)$ af polynomier er en Gröbnerbasis $\iff$ $S(f_i, f_j)^F = 0$ for $1 \leq i \leq j \leq m$.
Se Def. 5.3.2 for $S(f_i, f_j)^F$.

Buchbergers algoritme (5.7)

Sætning 5.7.2

Buchberger's algoritme terminerer og outputtet er en Gröbnerbasis.

Den reducerede Gröbnerbasis (5.8)

Minimal Gröbnerbasis

Def 5.8.1: En minimal gröbnerbasis $(f_1, \ldots, f_m)$ er en Gröbnerbasis sådan at

(i) $in_{\leq}(f_j) \nmid in_{\leq}(f_i)$ for $i \neq j$.

(ii) Koefficienten af $in_{\leq}(f_i)$ er 1.

Reduceret Gröbnerbasis

Def 5.8.2: En reduceret gröbnerbasis $(f_1, \ldots, f_m)$ er en Minimal Gröbnerbasis hvis $in_{\leq}(f_j) \nmid$ noget led i f_i for $i \neq j$.

Sætning 5.8.3

Lad R være et Legeme. Ethvert ideal $I \subseteq R[X_1, \ldots, X_n]$ har en entydig Reduceret Gröbnerbasis.

Løsning af ligningssystemer vha Gröbnerbaser (5.9)

Sætning 5.9.1

Lad R være et Legeme og $G = (f_1, \ldots, f_m)$ være en Gröbnerbasis for et Ideal $I \subseteq R[X_1, \ldots, X_n]$ mht den Leksikografisk ordning $\geq$ givet ved $X_n \geq X_{n-1} \geq \cdots \geq X_1$.

Så er $G \cap R[X_1, \ldots, X_i]$ en gröbnerbasis for idealet $I \cap R[X_1, \ldots, X_i]$ i $R[X_1, \ldots, X_i]$.

Appendix (6)

Talteori (1)

Induktionsprincippet

At mængden $\mathbb{N}$ har en Velordning vil sige at det har et første element, hvilket vil sige $\exists s : s \leq x$ for alle $x \in \mathbb{N}$. Dette er ækvivalent til matematisk induktion der siger:

Lad $P(n)$ være et udsagn hvor der for alle $n \geq 1$ gælder

(i) $P(1)$ er sand.

(ii) $P(n)$ er sand $\Rightarrow$ at $P(n+1)$ er sand.

så kan vi konkludere at $P(n)$ er sand for alle $n \geq 1$.

Reference (1.1)

Der gælder $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$

Grupper (2)

Veldefineret

En afbildning $f : X \to Y$ kaldes veldefineret hvis den afbilder alle elementer i domænet X til et element i codomænet Y.

Uanset valget af repræsentanter for sideklasser så afbilder de til samme element.

Injektiv

En afbildning $f : X \to Y$ kaldes injektiv hvis der gælder

$$\forall a, b \in X \Rightarrow \text{ hvis } f(a) = f(b), \text{ så er } a = b$$

Alle elementer i domænet X afbilder til et unikt element i $Y \Rightarrow |\, X \,| \leq |\, Y \,|$.

Surjektiv

En afbildning $f : X \to Y$ kaldes surjektiv hvis der gælder

$$\forall y \in Y \exists x \in X, \text{ hvor } f(x) = y$$

Alle elementer i codomænet Y bliver ramt af et element i $X \Rightarrow |\, X \,| \geq |\, Y \,|$.

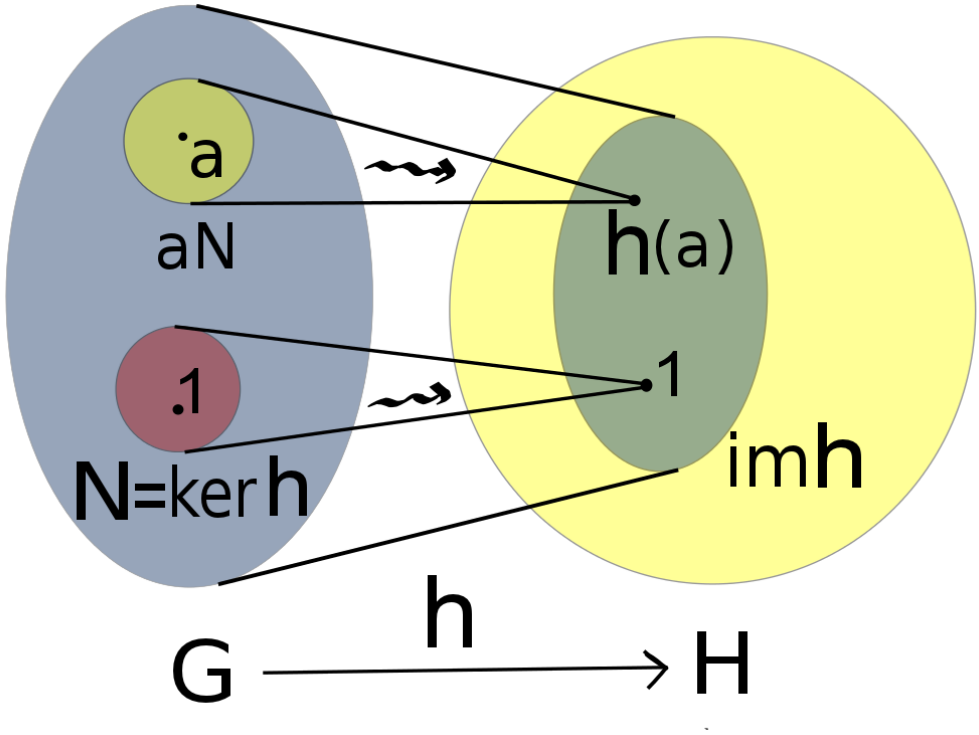
Bijektiv

En afbildning $f : X \to Y$ kaldes bijektiv hvis den er både

(i) Injektiv. *Alle elementer i codomænet Y bliver ramt af et element i $X \Rightarrow |\, X \,| \geq |\, Y \,|$.*

(ii) Surjektiv. *Alle elementer i domænet X afbilder til et unikt element i $Y \Rightarrow |\, X \,| \leq |\, Y \,|$.*

Enhver afbildning der har en invers er bijektiv



Figur 1: Animation af en gruppehomomorfi $h : G \to H$. Den lille oval inde i H er billedet af H. N er kernen af H og aN er en sideklasse til N.

Ker(f)

Lad $f : G \to K$ være en Gruppehomomorfi, så er:

$$Ker(f) = \{g \in G \mid f(g) = e\}$$

Kernen af f er mængden af alle elementer i G, som f afbilder til det neutrale element i K.

f(G)

Lad $f : G \to K$ være en Gruppehomomorfi, så er:

$$f(G) = \{f(g) \mid g \in G\} \subseteq K$$

Billedet af f er alle de elementer i K som f afbilder til fra G.

Gröbnerbaser (5)

Relation

Def. A.1.1: En relation R på en mængde S er en delmængde $R \subseteq S \times S$. Vi skriver xRy hvor vi mener $(x, y) \in R$.

Ækvivalensrelation

Def. A.1.2: En Relation R på en mængde S er kaldes en ækvivalensrelation hvis den er

(i) Refleksiv: $xRx \quad \forall x \in S$.

(ii) Symmetrisk: $xRy \Rightarrow yRx \quad \forall x, y \in S$.

(iii) Transativ: $xRy \wedge yRz \Rightarrow xRz \quad \forall x, y, z \in S$.

som eksempel er kongruens modulo et ideal, I en ækvivalensrelation

$$x \equiv y \pmod{I} \iff x - y \in I$$

Dette er det generelle tilfælde af relationen kongruens modulo et heltal i $\mathbb{Z}$, hvilket også er en ækvivalensrelation.

Partiel ordning

Def. A.1.2: En Relation R på en mængde S er kaldes en partiel ordning hvis den er

(i) Refleksiv: $xRx \quad \forall x \in S$.

(ii) Antisymmetrisk: $xRy \wedge yRx \Rightarrow x = y \quad \forall x, y \in S$.

(iii) Transativ: $xRy \wedge yRz \Rightarrow xRz \quad \forall x, y, z \in S$.

Som eksempel er $\leq$ en partiel ordning på $\mathbb{Z}$.

Minimalt element

Et element $s \in S$ med en Partiel ordning $\leq$ siges at være et minimalt element hvis

$$x \leq s \Rightarrow x = s$$

$\forall x \in S$.

Første element

Et element $t \in S$ med en Partiel ordning $\leq$ siges at være et første element hvis

$$t \leq x$$

$\forall x \in S$. Fordi $\leq$ er antisymmetrisk må dette t være unikt. Er første element er et Minimalt element.

Total ordning

Def. A.3.4: En Partiel ordning $\leq$ på en mængde S kaldes en total ordning hvis

$$x \leq y \vee y \leq x \quad \forall x, y \in S$$

Velordning

Def. A.3.5: En Partiel ordning $\leq$ på en mængde S kaldes en velordning hvis enhver ikke-tomt delmængde $M \subseteq S$ har et Første element.

$\langle f_1, \ldots, f_m \rangle$

$\langle f_1, \ldots, f_m \rangle =$
$\{a_1(X_1, \ldots, X_m)f_1 + \cdots + a_m(X_1, \ldots, X_m)f_m \mid a_1(X_1, \ldots, X_m), b_1(X_1, \ldots, X_m) \in R[X_1, \ldots, X_n]\}$

hvilket vil sige alle "lineære" kombinationer af $f_1, \ldots, f_m$.

Eksamen (7)

Den kinesiske restklassesætning

Vi har et system.

$$\begin{aligned} X &\equiv a_1 \pmod{n_1} \\ X &\equiv a_2 \pmod{n_2} \\ &\vdots \\ X &\equiv a_t \pmod{n_t} \end{aligned}$$

Når vi har fundet vores λ'ere og μ'ere er det blot at indsætte i formlen

$$X = a_1\mu_1(N/n_1) + \cdots + a_t\mu_t(N/n_t)$$

$\varphi(n)$

Der gælder følgende om $\varphi(p^l)$, hvor p er et primtal og $l \geq 1$.

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right)$$

Proof: Since p is a primer number the only possible values of gcd(pk,m) are 1, p, p2,. . . , pk, and the only way for gcd(pk,m) to not equal 1 is for m to be a multiple of p. The multiples of p that are less than or equal to pk are p, 2p, 3p, . . . , pk - 1p = pk, and there are pk - 1 of them. Therefore the other $pk - pk - 1$ *numbers are all relatively primt to pk.*

Yderemere gælder:

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{k_1})\varphi(p_2^{k_2})\cdots\varphi(p_r^{k_r}) \\ &= p_1^{k_1}\left(1 - \frac{1}{p_1}\right)p_2^{k_2}\left(1 - \frac{1}{p_2}\right)\cdots p_r^{k_r}\left(1 - \frac{1}{p_r}\right) \\ &= p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right). \end{aligned}$$

Eller kortere $\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$,

Eksempel:

$$\varphi(36) = \varphi\left(2^2 3^2\right) = 36\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12$$

Normafbildning

Hvis $N(z_1z_2) = N(z_1)N(z_2)$ og $N(1) = 1$ gælder

$$\text{Et element z} \in R \text{ er en Enhed} \iff N(z) = \pm 1$$

Bevis:

(i) Hvis z er en enhed så $\exists y$ sådan at $zy = 1$, derved $N(zy) = N(z)N(y)$ og derfor $N(z) = \pm 1$

(ii) Hvis $N(z) = \pm 1$ så $z\varphi(z) = \pm 1$ og z er en enhed.

Dette er smart at udnytte når vi skal vise om et element er irreducibelt eller ej.

Vis at R ikke er et Hovedidealområde

Nok at vise R ikke er en Faktoriel ring. Generelt gælder at hvis et element har to forskellige faktoriseringer, og der findes en faktor i den ene faktorisering der ikke går op i nogle af faktorerne i den anden faktorisering, så er ringen *ikke* en faktoriel ring.

Antallet af frembringere i L^*

Bevis 4.5.3 siger antallet af frembringere i $L^* = \varphi(|L^*|)$.

Simple transpositioner

Givet en cykel så start med at tæl inversionerne. Skriv den i 2-række form og målet er nu at vi skal ende ud med identiteten. Vi skal bruge lige mange simple transpositioner som der er inversioner.