

# Besvarelser af Algebra 1-eksamenssæt

Rasmus Villemoes

6. januar 2003



## **Indhold**

<b>Forord</b>	<b>5</b>
<b>Værd at huske</b>	<b>6</b>
<b>Januar 1997</b>	<b>7</b>
<b>Juni 1997</b>	<b>11</b>
<b>Januar 1998</b>	<b>12</b>
<b>Juni 1998</b>	<b>15</b>
<b>August 1998</b>	<b>17</b>
<b>Januar 1999</b>	<b>19</b>
<b>Juni 1999</b>	<b>21</b>
<b>Januar 2000</b>	<b>24</b>
<b>Juni 2000</b>	<b>28</b>
<b>Januar 2001</b>	<b>32</b>
<b>Juni 2001</b>	<b>37</b>
<b>Januar 2002</b>	<b>42</b>
<b>Juni 2002</b>	<b>46</b>



## Forord

På de følgende få sider følger besvarelser af eksamenssættene i Algebra 1 fra juni 1997 og frem til juni 2002. Dog er ikke alle opgaver besvaret, da ikke alle opgaver ligger inden for det nuværende pensum. Der garanteres ikke for løsningernes korrekthed, skønhed og/eller mangel på samme. Det er tilstræbt at henvise til sætninger i “Concrete Abstract Algebra” af Niels Lauritzen, men det er ikke gjort konsekvent i samtlige besvarelser. Den grad hvori man til eksamen bør referere til sætninger kan og bør man ikke lægge efter niveauet på disse sider; det må komme an på et individuelt skøn.

Jeg har foruden besvarelserne skrevet nogle få ting, som det kan anbefales at lære udenad; fx metoder til hurtigt at afgøre hvorvidt noget er et legeme eller ej. Betragt det dog ikke som en formelsamling, og betragt det ej heller som en “complete walk-through” til eksamen, da det ikke på disse få sider [og ud på disse små timer hvor dette skrives] er muligt at opremse samtlige potentielt nyttige sætninger fra Algebra 1-lærebogen.

Ikke alle opgaver er løst helt; de fleste steder fordi jeg simpelthen ikke har kunnet regne dem eller fået den idé der skal til. Det er tilstræbt at markere sådanne opgaver med  $\square$ .

Spørgsmål og rettelser er yderst velkomne. Den nemmeste måde at kontakte mig på er via email til [burner@imf.au.dk](mailto:burner@imf.au.dk), men hvis du ved hvem jeg er kan du nok også fange mig på gangen. Den nyeste version af dette dokument vil være tilgængelig på <http://home.imf.au.dk/burner/algebra.xhtml>.

Må du få megen glæde og gavn af læsningen...

D03, 6. januar 2003  
Rasmus Villemoes

### Værd at huske

#### Hvad står der her?

Dette er blot en lille oversigt over ting, som man bør huske ved algebra-eksamen, og som kan være nyttige hints. Jeg har forsøgt at omtale nogle forskellige typer opgaver man kan blive udsat for, og en strategi til løsning af dem. Der gives ingen garanti for at strategien er fornuftig at følge; der kan være en nemmere genvej i en given opgave, eller opgaven kan kræve en anden metode end den her beskrevne.

Jeg skriver nogle steder, at man skal “bemærke” eller “huske” noget; det betyder at sætningen, lemmaet, opgaven eller hvad det måtte være, kan være nyttig ved løsning af “typeopgaver” i algebra (altså opgaver hvor der måske kommer en lignende til eksamen). Jeg påstår dog ikke at det nævnte er det eneste der er værd at huske...

#### Talteori

Kapitlet om talteori danner grundlaget for det meste af bogen. Bogen forudsætter, at man er forholdsvis fortrolig med de hele tal og operationerne  $+$  og  $\cdot$ . Senere i bogen behandler man  $\mathbb{Z}$  i en mere abstrakt kontekst. Det mest nyttige i kapitlet er nok proposition 1.2.1 om division med (entydig) rest, at  $\gcd(a, b) = 1$  hvis og kun hvis der findes  $\lambda, \mu \in \mathbb{Z}$  så  $\lambda a + \mu b = 1$  (samt den Euklidiske algoritme til at finde  $\lambda, \mu$ ), den kinesiske restklassesætning (§1.6), samt §1.8.3 om hvordan man kan beregne  $\varphi(n)$ . Det er selvfølgelig også godt at huske på egenskaber ved de hele tal såsom entydig primfaktoriserings (§1.8.6).

#### Grupper

Ved introduktionen af grupper bliver algebra en del mere abstrakt. Der er dog ikke noget hemmeligt eller specielt avanceret ved definitionen af en gruppe. Man skal blot huske, at en gruppe  $G$  er en mængde, som er udstyret med en (én) komposition (i det følgende betegnet  $\circ$ ), der kan opfattes som en funktion fra  $G \times G \rightarrow G$ , og som indeholder et neutralelement  $e$  som opfylder  $e \circ a = a \circ e = a$  for alle  $a \in G$ , og desuden at alle elementer har et såkaldt “inverst element”. Det der måske kan virke underligt er, at de mængder vi normalt har arbejdet med (fx  $\mathbb{R}$  fra Mat11,  $\text{Mat}_n(\mathbb{R})$  fra Mat10) har været forsynet med et væld af kompositioner som man føler sig nogenlunde fortrolig med, og vi er desuden vant til den multiplikative notation  $xy$  for produktet af  $x$  og  $y$ . I virkeligheden er grupper meget simple, da der kun er den ene komposition  $\circ$ , og man kan derfor normalt uden problemer benytte notationen  $xy$  for  $x \circ y$ , uanset om vi måtte befinde os i en additiv eller multiplikativ gruppe, eller sågar en gruppe af funktioner. Desuden er betegnelsen  $x^{-1}$  en nem måde at skrive det inverse element til  $x$ . Holdes tungen lige i munden og andre legemsdele på deres rette pladser burde notationen dog ikke forårsage større vanskeligheder.

## Januar 1997

### Opgave 1

Lad  $P \subseteq \mathbb{P}$  være en delmængde af primtallene  $\mathbb{P}$ , og lad  $R_P$  betegne mængden af rationale tal  $\frac{a}{b}$ , hvor  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N} \setminus \{0\}$  og enhver primdivisor i  $b$  tilhører  $P$ .

For at det ikke skal være alt for kedeligt vil jeg tillade mig at gøre den ekstra antagelse, at  $P$  ikke er tom. (Hvis  $P = \emptyset$  er  $R_P = \mathbb{Z}$ , som klart er en delring af  $\mathbb{Q}$ ).

- (1) Det skal vises, at  $R_P$  er en delring af  $\mathbb{Q}$  (med de sædvanlige operationer  $+$  og  $\cdot$ ). Lad derfor  $\frac{a}{b}, \frac{c}{d} \in R_P$ . Så har vi at

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

Vi har, at  $ad + bc \in \mathbb{Z}$ . Da der desuden gælder, at  $\Pi(bd) = \Pi(b) \cup \Pi(d)$ , og såvel  $\Pi(b)$  som  $\Pi(d) \subseteq P$ , ser man, at summen af de to tal ligger i  $R_P$ . [Her er  $\Pi(x)$  er en muligvis uortodoks notation for mængden af primdivisorer i  $x$ ].

Vi har trivielt, at  $\frac{0}{1} \in R_P$ , da  $\emptyset \subseteq R_P$ , og lige så trivielt vil  $-\frac{a}{b} = \frac{-a}{b} \in R_P$  hvis  $\frac{a}{b} \in R_P$ .

Vi har også  $1 = \frac{1}{1} \in R_P$ , og med samme argument som ved beviset for lukkethed under addition får man at  $\frac{a}{b}, \frac{c}{d} \in R_P \Rightarrow \frac{ac}{bd} \in R_P$ . Altså opfylder  $R_P$  netop kriterierne for at udgøre en delring af  $\mathbb{Q}$ .

- (2) Det skal vises, at der for enhver uforkortelig brøk  $\frac{a}{b} \in \mathbb{Q}$  findes et helt tal  $x$  så at

$$x\frac{a}{b} - \frac{1}{b} \in \mathbb{Z}$$

Hvis  $\frac{a}{b}$  er uforkortelig, er  $\gcd(a, b) = 1$ . Vi har derfor, at der findes  $x, y \in \mathbb{Z}$  så  $xa + yb = 1$ , og ud fra denne fås let at

$$xa - 1 = -yb \in \mathbb{Z},$$

hvilket igen giver at

$$\frac{xa}{b} - \frac{1}{b} = -y \in \mathbb{Z}$$

som ønsket.

- (3) Lad  $R$  være en vilkårlig delring af  $\mathbb{Q}$  og sæt  $P = \{p \mid p \in \mathbb{P}, \frac{1}{p} \in R\}$ . Det skal vises, at  $R = R_P$ .

Hvis  $\frac{a}{b} \in R_P$ , har vi at

$$\frac{a}{b} = a \frac{1}{p_1^{n_1}} \cdots \frac{1}{p_k^{n_k}}$$

hvor  $p_i \in P$ . Men så må  $\frac{1}{p_i} \in R$ , og da  $R$  er en delring, vil  $\prod_{i=1}^k \frac{1}{p_i} \in R$ ; og da  $a$  er et heltal vil også  $a$  gange produktet tilhøre  $R$  (da jo  $1 \in R$  vil  $a \in \mathbb{Z} \subseteq R$ ). Dette viser  $R_P \subseteq R$ .

Hvis  $\frac{a}{b} \in R$  kan vi WLOG antage, at  $\gcd(a, b) = 1$ . Lad derfor  $x$  og  $y$  opfylde  $xa + yb = 1$  som i 2. Dér så vi, at

$$\frac{xa}{b} - \frac{1}{b} = -y,$$

men da vil

$$\frac{1}{b} = \frac{xa}{b} + y$$

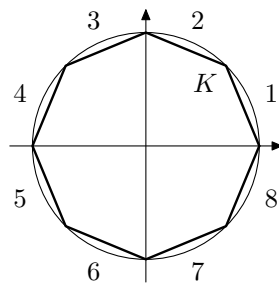
tilhøre  $R$ ; thi enhver delring af  $\mathbb{Q}$  må indeholde  $\mathbb{Z}$ , og er lukket under multiplikation og addition. Men nu er  $\frac{1}{b}$  jo på formen nævnt ovenfor, nemlig

$$\frac{1}{b} = \prod_{i=1}^k \frac{1}{p_i}.$$

Hvis man igen udnytter, at  $R$  er lukket under multiplikation med hele tal, kan man jo gange  $\frac{1}{b}$  med  $b/p_1, b/p_2, \dots, b/p_k$  og således udlede, at  $\frac{1}{p_i} \in R$  for  $i = 1, \dots, k$ . Derfor vil alle disse  $p_i$ 'er netop tilhøre  $P$ , og brøken  $\frac{a}{b}$  er derfor også indeholdt i  $R_P$  (da alle  $b$ 's primdivisorer tilhører  $P$ ). Således er  $R \subseteq R_P$ , og dermed  $R = R_P$ .

## Opgave 2

Betragt den regulære 8-kant  $K$  på figur 1, og lad  $G$  være gruppen af rotations- og spejlingssymmetrier for  $K$ . Lad der desuden være givet  $k$  farver. Det skal udregnes, på hvor mange måder det er muligt at farve de otte kanter når der ses bort fra rotationer og spejlinger. Lad de enkelte kanter være nummereret som vist på figuren.



Figur 1: 8-kanten  $K$  indskrevet i  $S^1$

Til formålet er det oplagt at anvende Burnsid's lemma. Første trin er derfor en præcis beskrivelse af gruppen  $G$ . Man finder, at den består af

- Identiteten.

- Rotation om  $\mathcal{O}$  på  $j \cdot \frac{\pi}{4}$ .
- Spejling i de fire linjer gennem modstående hjørner.
- Spejling i de fire midtnormaler til kanterne.

Næste trin er at finde størrelsen af hver af fixpunktsmængderne for de forskellige elementer i  $G$ . Man finder, at identiteten fastholder samtlige  $k^8$  mulige farvninger. Rotationen på  $\pi$  fastholder  $k^4$  forskellige farvninger (fire kanter kan farvelægges valgfrit; så er de sidste fires farver fastlagt). Tilsvarende fastholder rotationerne på  $\pi/2$  og  $3\pi/2$  netop  $k^2$  farvninger, og de øvrige rotationer ( $k\pi/4$ ,  $k = 1, 3, 5, 7$ ) fastholder  $k$  farvninger, thi når den første kant er farvet skal de øvrige have samme farve. [Man kan bemærke, at for rotationen på  $k\pi/4$  vil antallet af fastholdte farvninger være  $k^{8/\text{ord}(k)}$ , hvor  $\text{ord}(k)$  er ordenen af  $k$  i  $\mathbb{Z}/8\mathbb{Z}$ ].

For spejlingerne i linjerne gennem hjørnerne finder man, at man kan farvelægge 4 kanter valgfrit, mens de sidste fire er bundet af dette valg, så for disse er der  $k^4$  fastholdte farvninger. For spejlingerne i midtnormalerne kan 5 kanter farvelægges efter behag, og disse fastholder derfor  $k^5$  farvninger.

I alt giver Burnsid's lemma altså, at antallet af farvninger modulo spejlinger og rotationer er

$$\frac{k^8 + k^4 + 2k^2 + 4k + 4k^4 + 4k^5}{16} = \frac{k^8 + 4k^5 + 5k^4 + 2k^2 + 4k}{16}$$

### Opgave 3

Lad  $\mathcal{J} = \langle X^8 + X + 1 \rangle$  være hovedidealet i  $\mathbb{F}_2[X]$  frembragt af  $X^8 + X + 1$ , og lad  $L$  være kvotientringen givet ved

$$L = \mathbb{F}_2[X]/\mathcal{J}$$

Lad  $\alpha \in L$  være klassen for  $X$  modulo  $\mathcal{J}$ , altså  $\alpha = X + \mathcal{J}$ . Først bemærkes det, at  $\text{char}(L) = \text{char}(\mathbb{F}_2) = 2$ .

(1) Vi har at  $\alpha^8 + \alpha + 1 = 0$  i  $L$ , og da  $\alpha = -\alpha$  og  $1 = -1$  vil

$$\alpha^8 = \alpha + 1$$

Hvis vi nu bruger, at  $L$  har primtallig karakteristisk  $p = 2$ , kan "freshman's dream" bruges, og man finder ved at kvadrere ovenstående og de følgende udtryk at

$$\begin{aligned} \alpha^{16} &= (\alpha + 1)^2 = \alpha^2 + 1^2 = \alpha^2 + 1 \\ \alpha^{32} &= (\alpha^2 + 1)^2 = \alpha^4 + 1 \\ \alpha^{64} &= (\alpha^4 + 1)^2 = \alpha^8 + 1 = \alpha + 2 = \alpha \end{aligned}$$

(2) Vi har fra det ovenstående, at  $\alpha^{63} = \alpha^{62}\alpha = 1$ , og dermed er  $\alpha$  en enhed.

- (3) Vi har, at da  $\alpha^{63} = 1$ , vil  $\text{ord}(\alpha) \mid 63$ . Altså er  $\text{ord}(\alpha)$  enten lig 1, 3, 7, 9, 21 eller 63. De første tre muligheder kan hurtigt udelukkes, da  $\alpha, \alpha^3, \alpha^7 \neq 1$ . Desuden er  $\alpha^9 = \alpha\alpha^8 = \alpha^2 + \alpha \neq 1$ , og  $\alpha^{21} = \alpha^5\alpha^{16} = \alpha^7 + \alpha^5 \neq 1$ . Altså må  $\text{ord}(\alpha)$  være 63.
- (4) Vi har, at  $|L| = 2^8 = 256$  jf. proposition 4.6.6. Hvis  $L$  er et legeme, er  $|L^*| = 255$ . Men vi har, at for ethvert  $u \in L^*$  vil  $\text{ord}(u) \mid |L^*|$ ; og da  $63 \nmid 255$ , kan  $L$  ikke være et legeme.

## Juni 1997

### Opgave 4

Lad  $\mathbb{F}_{64}$  være et legeme med 64 elementer.

- (1) Teorem 4.7.1 giver, at da  $64 = 2^6$  er  $\mathbb{F}_{64}$  isomorf med  $\mathbb{F}_2[X]/\langle f \rangle$ , hvor  $f$  er et irreducibelt polynomium af grad 6 i  $\mathbb{F}_2[X]$ , og vi kan derfor regne som om  $\mathbb{F}_{64}$  er identisk med dette legeme. Derfor er  $\text{char } F = 2$ , og dermed vil  $\{0, 1\} = \mathbb{F}_2$  udgøre et dellegeme af  $\mathbb{F}_{64}$ .
- (2) Vi har at  $|\mathbb{F}_{64}^*| = 63$ , og teorem 4.5.1 giver, at  $\mathbb{F}_{64}^*$  er en cyklisk gruppe (betragt gruppen af enheder som en undergruppe af sig selv). Proposition 2.6.7 giver så, at da 9 er en divisor i 63 findes der netop en undergruppe af  $\mathbb{F}_{64}^*$  af orden 9, og dermed må der også være elementer af orden 9 (faktisk er der  $\varphi(9) = 6$  sådanne). Vælges  $\alpha$  til at være et af disse, har vi at  $\alpha^9 = 1$ , og da  $1 + 1 = 0$  i  $\mathbb{F}_2$  har vi at  $\alpha$  er rod i  $X^9 + 1 \in \mathbb{F}_2[X]$ .
- (3) Lad  $X^9 + 1 = p_1 p_2 \dots p_k$  være en irreducibel faktorisering af  $X^9 + 1$  i  $\mathbb{F}_2[X]$ . Vi ved, at vi ved at evaluere i  $\alpha$  på begge sider får 0, og da polynomiumsringen over et (del)legeme er et domæne, vil  $p_i(\alpha) = 0$  for passende  $i$  ( $\alpha$  er rod i mindst et af polynomierne på højre side, da nulreglen gælder). Vi kan derfor vælge  $f = p_i$ , og så er det klart at de tre punkter er opfyldt.
- (4) Da  $f$  er irreducibel i  $\mathbb{F}_2[X]$  vil  $\langle f \rangle$  være et maksimalt ideal i  $\mathbb{F}_2[X]$  og dermed er  $\mathbb{F}_2[X]/\langle f \rangle$  et legeme (proposition 4.6.3).

Definer nu funktionen  $\varphi: \mathbb{F}_2[X] \rightarrow \mathbb{F}_2[\alpha]$  ved at  $\varphi$  evaluerer i  $\alpha$ ; så er det ret åbenlyst at  $\varphi$  er en ringhomomorfi. Vi søger nu  $\ker \varphi$ . Da  $\alpha$  er rod i  $f$ , er det klart at  $\langle f \rangle \subseteq \ker \varphi$ . Men da  $\ker \varphi$  er et ideal (i  $\mathbb{F}_2[X]$ ), og  $\langle f \rangle$  er et maksimalt ideal, må enten  $\ker \varphi = \langle f \rangle$  eller  $\ker \varphi = \mathbb{F}_2[X]$ . Den sidste mulighed kan dog nemt udelukkes, da  $\alpha$  ikke er rod i alle polynomier i  $\mathbb{F}_2[X]$  (fx ikke i  $X$ ), og derfor er  $\ker \varphi = \langle f \rangle$ . Men så giver proposition 3.1.16 at  $\tilde{\varphi}: \mathbb{F}_2[X]/\langle f \rangle \rightarrow \mathbb{F}_2[\alpha]$  givet ved  $\tilde{\varphi}([p]) = \varphi(p) = p(\alpha)$  er en ringisomorfi, og dermed er

$$\mathbb{F}_2[X]/\langle f \rangle \cong \mathbb{F}_2[\alpha]$$

- (5) Vi har at  $\mathbb{F}_2[\alpha] \subseteq \mathbb{F}_{64}$ , og derfor er  $|\mathbb{F}_2[\alpha]| \mid 64$ . Desuden er enhederne en multiplikativ undergruppe af  $\mathbb{F}_{64}^*$ , dvs.  $|\mathbb{F}_2[\alpha]^*| \mid 63$ . Desuden er  $|\mathbb{F}_2[\alpha]| = |\mathbb{F}_2[X]/\langle f \rangle| = 2^{\deg f}$ , og heraf kan vi udlede, at  $\deg f = a$  hvor  $a \leq 6$  samt at  $2^a - 1 \mid 2^6 - 1$ . Opgave IV.22 giver så, at  $a$  skal gå op i 6, og dermed er  $a$  enten 1, 2, 3 eller 6. Desuden har vi jo at  $\langle \alpha \rangle \subseteq \mathbb{F}_2[\alpha]$ , så der er mindst 9 elementer heri; og herved ser man, at  $a = \deg f = 6$ .

## Januar 1998

### Opgave 1

Der er i alt 8 spejlinger og drejninger som fører det store kvadrat over i sig selv. Det er spejling i de to diagonaler ( $S_1, S_2$ ), spejling i de to midterlinjer ( $S_3, S_4$ ) parallelle med kvadratets sider, samt drejninger på henholdsvis  $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$  omkring kvadratets centrum ( $D_\theta$ ).

- De fastholdte farvninger ved spejling i en diagonal kan beskrives som følger: Der skal naturligvis være et lige antal sorte på diagonalen, fordi der i de øvrige 12 felter skal farves sorte symmetrisk. Hvis der er 0 sorte på diagonalen, er der  $\binom{6}{2} = 15$  muligheder for fastholdte farvninger. Hvis der er 2 sorte på diagonalen, er der for det første  $\binom{4}{2} = 6$  muligheder for at placere dem, og 6 muligheder for at placere en sort i de øvrige 6 felter (den sidste skal placeres symmetrisk). Endelig er der netop én farvning hvor alle 4 sorte felter lægges på diagonalen. Altså er der for  $S_1$  og  $S_2$   $15 + 36 + 1 = 52$  fastholdte farvninger af kvadratet.
- Ved spejling i en midterakse skal de to sorte placeres i den ene side, og de to sidste skal så være symmetrisk; altså er der  $\binom{8}{2} = 28$  fastholdte farvninger for hver spejling her.
- Ved identitetsafbildningen (rotationen på 0) er alle  $\binom{16}{4} = 1820$  farvninger fastholdt.
- Ved rotation på  $\pi$  er der det samme antal fastholdte farvninger som ved  $S_3$  og  $S_4$ , dvs. 28.
- Ved en rotation på  $\frac{\pi}{2}$  eller  $\frac{3\pi}{2}$  afbildes hver lille kvadrant (med fire småkvadrater) over i det "næste", og der skal derfor placeres en sort i hvert lille kvadrat; altså er der kun 4 fastholdte farvninger her.

I alt giver Burnsidets lemma, at der under hensyntagen til spejlinger og drejninger er

$$\frac{52 + 52 + 28 + 28 + 1820 + 28 + 4 + 4}{8} = 252$$

forskellige farvelægninger.

### Opgave 2

Lad  $N \geq 2$  være et naturligt tal, og lad  $R$  betegne

$$R = \{(a_1, a_2) \in \mathbb{Z} \times \mathbb{Z} \mid a_1 \equiv a_2 \pmod{N}\}.$$

- (1) Betragt  $\mathbb{Z}^2$  som en ring hvor addition og multiplikation defineres komponentvis. Hvis  $(a_1, a_2), (b_1, b_2) \in R$ , har vi at  $a_1 \equiv a_2 \pmod{N}$  og  $b_1 \equiv b_2 \pmod{N}$ . Men heraf følger, at  $a_1 + b_1 \equiv a_2 + b_2 \pmod{N}$  (proposition 1.3.4), og derfor vil  $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \in R$ . Det er

nemt at indse, at  $(0, 0) \in R$  og at det er additivt neutralt element, og endelig har vi at hvis  $a_1 \equiv a_2 \pmod{N}$ , vil  $-a_1 \equiv -a_2 \pmod{N}$ , så  $-(a_1, a_2) = (-a_1, -a_2) \in R$ . Man ser let, at  $(1, 1) \in R$  er neutralt element ved multiplikation, og endelig har vi at kongruenserne  $a_1 \equiv a_2 \pmod{N}$  og  $b_1 \equiv b_2 \pmod{N}$  giver at  $a_1 b_1 \equiv a_2 b_2 \pmod{N}$ , så  $(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2) \in R$ .

- (2) Lad for  $\nu = 1, 2$  og et primtal  $p$   $\mathfrak{M}_{\nu,p}$  betegne delmængden

$$\mathfrak{M}_{\nu,p} = \{(a_1, a_2) \in R \mid a_\nu \equiv 0 \pmod{p}\}$$

af  $R$ . Af samme grunde som ovenfor indser man let, at  $\mathfrak{M}_{\nu,p}$  er en undergruppe af  $R$  med hensyn til  $R$  (hvis  $a_\nu \equiv b_\nu \equiv 0 \pmod{p}$  vil også  $-a_\nu \equiv a_\nu + b_\nu \equiv 0 \pmod{p}$ ), og klart er også  $(0, 0) \in \mathfrak{M}_{\nu,p}$ . Lad nu  $a = (a_1, a_2) \in \mathfrak{M}_{\nu,p}$  og  $\lambda = (\lambda_1, \lambda_2) \in R$ . Så er  $\lambda a = (\lambda_1 a_1, \lambda_2 a_2)$ , og da  $p \mid a_\nu$  vil også  $p \mid \lambda_\nu a_\nu$ , så  $\lambda a \in \mathfrak{M}_{\nu,p}$ . Således er  $\mathfrak{M}_{\nu,p}$  et ideal i  $R$ .

Definer  $\varphi: R \rightarrow \mathbb{Z}/p\mathbb{Z}$  ved  $\varphi(a_1, a_2) = [a_\nu]$ , hvor  $[a_\nu]$  betegner restklassen i  $\mathbb{Z}/p\mathbb{Z}$  som  $a_\nu$  tilhører. Så er  $\varphi$  oplagt en ringhomomorfi (det er sammensætningen af homomorfi  $\varphi': R \rightarrow \mathbb{Z}$  givet ved  $\varphi'(a_1, a_2) = a_\nu$  og den kanoniske homomorfi  $\pi$  fra  $\mathbb{Z}$  ind i  $\mathbb{Z}/p\mathbb{Z}$ ), og det følger af definitionen at  $\ker \varphi = \mathfrak{M}_{\nu,p}$ . Altså følger af isomorfisætningen (proposition 3.1.16) at

$$R/\mathfrak{M}_{\nu,p} \cong \mathbb{Z}/p\mathbb{Z}$$

Da  $\mathbb{Z}/p\mathbb{Z}$  er et legeme, er også  $R/\mathfrak{M}_{\nu,p}$  et legeme, og derfor er  $\mathfrak{M}_{\nu,p}$  et maksimalt ideal jf. §3.2.3.

- (3) Lad  $\mathfrak{J}$  være et ideal i  $R$ , så  $\mathfrak{J}$  indeholder et element af formen  $(x, 1)$  og et element af formen  $(1, y)$ . Da et ideal er lukket under multiplikation, har vi at  $(x, y) \in \mathfrak{J}$ . Men et ideal er også lukket under addition, så også  $(1 + x, 1 + y)$  vil ligge i  $\mathfrak{J}$ , og endelig vil differencen mellem disse to ligge i  $\mathfrak{J}$ ; altså har vi  $(1, 1) \in \mathfrak{J}$  og dermed er  $\mathfrak{J} = R$ .
- (4) Lad  $I \subseteq R$  være et maksimalt ideal, og lad  $\pi_i: R \rightarrow \mathbb{Z}$  betegne projektionen  $(a_1, a_2) \mapsto a_i$ . Så er ikke både  $\pi_1(I) = \mathbb{Z}$  og  $\pi_2(I) = \mathbb{Z}$ , for så ville  $I$  jf. (3) være hele  $R$ . Antag WLOG at  $\pi_1(I) \neq \mathbb{Z}$ .

### Opgave 3

Antag om  $\alpha \in \mathbb{C} \setminus \mathbb{R}$  at

$$R = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$$

er en delring af  $\mathbb{C}$ .

- (1) Hvis  $R$  er en delring, betyder det at  $\alpha^2$  er på formen  $\alpha^2 = a + b\alpha$  hvor  $a$  og  $b$  er hele tal. Lad  $c = -b$  og  $d = -a$ ; så har vi at  $\alpha^2 + c\alpha + d = 0$ , og dermed er  $\alpha$  rod i  $f(X) = X^2 + cX + d \in \mathbb{Z}[X]$ .

- (2) Det er klart, at  $X - \alpha$  går op i  $f(X)$  betragtet som polynomium i  $R[X]$ . Dermed har vi, at vi kan faktorisere  $f$  som  $f(X) = (X - \alpha)(X - \beta)$ , og det giver at  $-(\alpha + \beta) = c$  og  $\alpha\beta = d$ . Heraf får man, at  $\operatorname{Im} \alpha = -\operatorname{Im} \beta$  (da  $\operatorname{Im} c = 0$ ). Desuden er  $\operatorname{Im} d = \operatorname{Im}(\alpha\beta) = \operatorname{Re} \alpha \operatorname{Im} \beta + \operatorname{Re} \beta \operatorname{Im} \alpha = (\operatorname{Re} \beta - \operatorname{Re} \alpha) \operatorname{Im} \alpha = 0$ , og da  $\alpha$  ikke er reel har vi at  $\operatorname{Re} \alpha = \operatorname{Re} \beta$ . Altså er  $\beta = \bar{\alpha}$ . Desuden er  $\beta = -c - \alpha$ , og da såvel  $c$  som  $\alpha$  tilhører  $R$ , vil også  $\beta \in R$ .
- (3) Definer homomorfi  $\varphi: \mathbb{Z}[X] \rightarrow R$  ved evaluering i  $\alpha$ , dvs.  $\varphi(p) = p(\alpha)$ ; med denne definition er det ret oplagt at det bliver en ringhomomorfi. Lad  $\langle f \rangle$  være idealet frembragt af  $f(X) = X^2 + cX + d$  fra (1). Så har vi at  $\langle f \rangle \subseteq \ker \varphi$ . Da  $f(X) = X^2 + cX + d$  er irreducibel i  $\mathbb{Z}[X]$  (rødderne  $\alpha$  og  $\beta$  er ikke hele tal), og  $\mathbb{Z}[X]$  ikke er et legeme, har vi at  $\langle f \rangle$  er et maksimalt ideal. Da  $\ker \varphi$  ikke er hele  $\mathbb{Z}[X]$ , må der gælde at  $\ker \varphi = \langle f \rangle$ . Så giver isomorfiætningen, at afbildningen  $\tilde{\varphi}: \mathbb{Z}[X]/\langle f \rangle \rightarrow R$  givet ved  $\tilde{\varphi}(p + \langle f \rangle) = \varphi(p) = p(\alpha)$  er en isomorfi.
- (4) En ringhomomorfi  $h: R \rightarrow R$  sender i hvert fald 1 i 1, og dermed er  $h(x) = x$  for alle  $x \in \mathbb{Z}$ . Desuden er  $h(a+b\alpha) = h(a) + h(b\alpha) = a + bh(\alpha)$ , så homomorfi er helt bestemt af værdien af  $h(\alpha)$ . Da vi har, at  $\alpha^2 + c\alpha + d = 0$ , må  $0 = h(0) = h(\alpha^2 + c\alpha + d) = h(\alpha)^2 + ch(\alpha) + d$ , og derfor er  $h(\alpha)$  rod i  $X^2 + cX + d$ . Altså skal  $h(\alpha)$  være enten  $\alpha$  eller  $\beta$ . Det er klart, at hvis  $h(\alpha) = \alpha$  er  $h = \operatorname{Id}$  og dermed er  $h$  en ringhomomorfi. Hvis  $h(\alpha) = \beta = \bar{\alpha}$  bliver  $h$  funktionen der kompleks konjugerer (thi  $h(a + b\alpha) = a + b\bar{\alpha} = \overline{a + b\alpha}$ ), og dette er jo også en ringhomomorfi (konjugering sender 0 i 0, 1 i 1, og bevarer sum og produkt). Altså er de eneste ringhomomorfier  $R \rightarrow R$  identiteten og kompleks konjugering.
- (5) Lad  $L$  betegne brøklegemet for  $R$ , og  $K$  dellegemet

$$K = \{x + y\alpha \mid x, y \in \mathbb{Q}\}$$

af  $\mathbb{C}$ .

Ifølge proposition 3.2.7 findes en entydig injektiv ringisomorfi  $\bar{\varphi}: L \rightarrow K$ . Tilbage er blot at vise, at  $\bar{\varphi}$  er surjektiv. Lad derfor  $x + y\alpha = \frac{a}{b} + \frac{c}{d}\alpha \in K$ . Så ser man ved at sætte på fælles brøkstreg, at  $x + y\alpha = \varphi((ad + bc\alpha)(bd)^{-1})$ , hvor indmaden i  $\varphi$  er et element i brøklegemet for  $R$  da  $bd \neq 0$ , og dermed er  $K \cong L$ .

## Juni 1998

### Opgave 1

- (a) Lad  $f = X^3 - X - 1 \in \mathbb{Z}/3\mathbb{Z}[X]$ . Så er  $f(0) = 1$ ,  $f(1) = -1$  og  $f(2) = -1$ . Altså har  $f$  ingen rødder, og da det har grad 3 er  $f$  irreducibel (proposition 4.6.3).
- (b) Lad  $K = \mathbb{Z}/3\mathbb{Z}[X]/\mathcal{J}$ , hvor  $\mathcal{J}$  betegner  $\langle f \rangle$ , og lad  $\alpha = [X]$ . Da  $f$  er irreducibel, er  $\mathcal{J}$  et maksimalt ideal og dermed er  $K$  et legeme. Proposition 4.6.6 giver, at vi entydigt kan beskrive elementerne i  $K$  som  $a\alpha^2 + b\alpha + c$ , hvor  $a, b, c \in \mathbb{Z}/3\mathbb{Z}$ .
- (c) Vi har at  $\alpha^3 - \alpha - 1 = 0$ , og dermed er  $\alpha^3 = \alpha + 1$ . Ved "kubering" får man så (ved hjælp af "freshman's dream"), at  $\alpha^9 = (\alpha + 1)^3 = \alpha^3 + 1 = \alpha + 2 = \alpha - 1$  og endelig  $\alpha^{12} = \alpha^9 \alpha^3 = (\alpha - 1)(\alpha + 1) = \alpha^2 - 1$ . Vi har, at  $K$  er et legeme med 27 elementer, så der er 26 elementer i  $K^*$ . Altså er ordenen af  $\alpha$  i  $K^*$  divisor i 26; dvs. 1, 2, 13 eller 26. Da  $\alpha \neq 1$  er ordenen ikke 1. En udregning giver  $\alpha^{13} = \alpha \alpha^{12} = \alpha^3 - \alpha = 1$ , og derfor kan  $\alpha^2$  ikke være 1 (så ville  $\alpha^{13} = \alpha$ ). Altså er  $\text{ord}(\alpha) = 13$ .
- (d) Gruppen  $(K^*, \cdot)$  kan ikke indeholde et element af orden 3, da 3 ikke er divisor i 26. Faktisk består  $K^*$  af 1 element af orden 1, 1 element af orden 2, 12 elementer af orden 13 og 12 elementer af orden 26 (proposition 2.6.7 og teorem 4.5.1).

### Opgave 4

- (1) Lad

$$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

Så er

$$\begin{aligned} \omega^2 &= \left(\frac{1}{4} - \frac{3}{4}\right) - 2\frac{1}{2}\frac{\sqrt{3}}{2}i \\ &= -\frac{1}{2} - \frac{\sqrt{3}}{2}i \\ &= \bar{\omega} \\ &= -1 - \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) \\ &= -1 - \omega \end{aligned}$$

Lad

$$R = \{a + b\omega \mid a, b \in \mathbb{Z}\}.$$

Så er  $(R, +)$  oplagt en gruppe med neutralelement  $0 + 0\omega$ , og  $1 + 0\omega$  er neutralelement ved multiplikation, som  $R$  i øvrigt er lukket under:  $(a + b\omega)(c + d\omega) = ac + (ad + bc)\omega + bd\omega^2 = ac - bd + (ad + bc - bd)\omega \in R$ .

- (2) Lad  $N: R \rightarrow \mathbb{N}$  være givet ved  $N(z) = z\bar{z}$ . Så er  $N(1) = 1\bar{1} = 1$ , og  $N(z_1 z_2) = z_1 z_2 \overline{z_1 z_2} = z_1 \bar{z}_1 \overline{z_2 z_1} = N(z_1)N(z_2)$ . Endelig er

$$\begin{aligned} N(a + b\omega) &= (a + b\omega)\overline{(a + b\omega)} \\ &= (a + b\omega)(a + b\bar{\omega}) \\ &= a^2 + ab\omega + ab(-1 - \omega) + b^2|\omega|^2 \\ &= a^2 - ab + b^2 \\ &= (a - b)^2 + ab \end{aligned}$$

- (3) Antag  $z$  er en enhed. Så findes  $w \in R$  så  $zw = 1$ . Dermed er  $N(zw) = N(z)N(w) = 1$ , og da  $N(z), N(w) \in \mathbb{N}$  må vi have at  $N(z) = N(w) = 1$ . Omvendt hvis  $N(z) = N(a + b\omega) = 1$ , er  $(a - b)^2 + ab = 1$ . Det er klart at ikke både  $a$  og  $b$  kan være 0. Hvis en af dem er 0, skal den anden være  $\pm 1$ , og man finder let at alle elementerne i  $\{1, -1, \omega, -\omega\}$  er enheder (deres inverse er henholdsvis  $1, -1, -1 - \omega, 1 + \omega$ ). Hvis ingen af  $a$  og  $b$  er 0, må  $a$  og  $b$  have samme fortegn, for ellers ville  $a^2 + b^2 - ab$  være  $\geq 3 > 1$ . Når  $a$  og  $b$  har samme fortegn, er både  $(a - b)^2 \geq 0$  og  $ab \geq 1$ . Vi ser derfor, at man må kræve  $a = b = \pm 1$  for at  $N(a + b\omega)$  kan være 1. Dette svarer til  $-1 - \omega$  og  $1 + \omega$ , og disse er allerede nævnt; det er enheder med inverse henholdsvis  $\omega$  og  $-\omega$ . Der er ikke andre muligheder for  $(a, b)$  hvis  $z = a + b\omega$  skal være en enhed. Således er  $z$  en enhed hvis og kun hvis  $N(z) = 1$ .
- (4) I (3) er det eftervist, at de eneste elementer i  $R$  som har norm 1, og dermed enhederne er  $R^*$ , er elementerne

$$R^* = \{1, -1, \omega, -\omega, -1 - \omega, 1 + \omega\}$$

og derfor er  $|R^*| = 6$ .

## August 1998

### Opgave 1

Lad  $f(X)$  være en irreducibel divisor i

$$X^9 + X + 1 \in \mathbb{Z}/2\mathbb{Z}[X]$$

og lad

$$R = \mathbb{Z}/2\mathbb{Z}[X]/\langle f \rangle$$

Med  $\alpha$  menes  $[X]$  i  $R$ .

- (1) Da  $f$  er irreducibel i  $\mathbb{Z}/2\mathbb{Z}[X]$ , er  $\langle f \rangle$  et maksimalt ideal og dermed er  $R$  et legeme (proposition 4.6.3i). Desuden følger af proposition 4.6.6 at elementerne i  $R$  entydigt kan skrives som  $b_0 + b_1\alpha + \dots + b_{d-1}\alpha^{d-1}$  hvor  $d = \deg f$  og  $b_i \in \mathbb{F}_2$ , og dermed er der  $2^d$  elementer i  $R$ .
- (2) Vi har at  $\alpha^9 + \alpha + 1 = [f] = 0$  i  $R$ . Heraf følger at  $\alpha^9 = -\alpha - 1 = \alpha + 1$ , og så at ("freshman's dream"):

$$\begin{aligned}\alpha^{18} &= (\alpha^9)^2 = (\alpha + 1)^2 = \alpha^2 + 1 \\ \alpha^{36} &= (\alpha^{18})^2 = (\alpha^2 + 1)^2 = \alpha^4 + 1 \\ \alpha^{72} &= (\alpha^{36})^2 = (\alpha^4 + 1)^2 = \alpha^8 + 1\end{aligned}$$

- (3) Fra (3) får man at  $\alpha^{73} = \alpha\alpha^{72} = \alpha^9 + \alpha = 1$ . Det betyder, at  $\text{ord } \alpha \mid 73$ , men da 73 er et primtal, er ordenen enten 1 eller 73. Da  $\alpha \neq 1$  er  $\text{ord } \alpha = 73$ . Desuden er  $\langle \alpha \rangle \subseteq (R^*, \cdot)$  en (multiplikativ) undergruppe af enhederne i  $R$ , og en undergruppes orden er divisor i gruppens orden; da  $R$  er et legeme er der  $|R^*| = |R| - 1 = 2^d - 1$  enheder. Altså er 73 divisor i  $2^d - 1$ .
- (4) Vi har at  $73 \nmid 127$ ,  $73 \nmid 255$ , men at  $73 \mid 511$ . Da  $d$  må være  $\leq 9$ , ser man således at  $d = \deg f = 9$ .

### Opgave 3

I ringen  $R$  antages det at der for ethvert element  $a$  gælder  $a^2 = a$ .

- (1) Lad  $a, b \in R$ . Så er

$$(a + b)^2 = a(a + b) + b(a + b) = a^2 + ab + ba + b^2$$

men pr. antagelse gælder også

$$(a + b)^2 = a + b$$

Kombineres disse to udtryk, og bruges det igen at  $a^2 = a$  og  $b^2 = b$ , får man at

$$0 = ab + ba \Rightarrow ab = -ba$$

- (2) Benyttes resultatet fra (1) med  $a = b$  får man at  $a^2 = -a^2$ , og dermed  $a = -a$ ; så  $2a = 0$ . Desuden har vi at for vilkårlige elementer  $a, b$  er  $ab = -ba$ , men da  $0 = 2ba$ , må det ved addition af disse gælde at  $ab = ba$ , så  $R$  er kommutativ.
- (3) Antag  $R$  er et integritetsområde. Antag at der udover elementerne 0 og 1 i  $R$  findes et tredje element  $a$ . Så er  $a^2 = a$  og dermed  $a^2 - a = 0$ ; altså  $a(a - 1) = 0$ . Da  $a$  var antaget at være forskellig fra både 0 og 1, er ingen af disse faktorer 0, og dermed er  $a$  en nuldivisor, hvilket er en modstrid. Altså består  $R$  kun af elementerne  $\{0, 1\}$ , og  $R$  er derfor oplagt ringisomorf med  $\mathbb{Z}/2\mathbb{Z}$ .
- (4) Af §3.2.3 følger det, at hvis  $I$  er et maksimalt ideal, er  $I$  et primideal. Antag derfor nu, at  $I$  er et primideal. Så er  $R/I$  et integritetsområde (§3.2.2), og som i (3) har vi så, at der kun kan være de to elementer  $[0]$  og  $[1]$  i  $R/I$  (et tredje element  $[a]$  ville igen opfylde at  $[a]^2 = [a^2] = [a]$ , så  $[a]$  ville være nuldivisor), og dermed er  $R/I$  ringisomorf med  $\mathbb{Z}/2\mathbb{Z}$ ; da  $R/I$  således er et legeme, må  $I$  være et maksimalt ideal.

## Januar 1999

### Opgave 2

Antag at  $p$  er et primtal forskelligt fra 2, men dog  $\equiv 2 \pmod{3}$ . Lad som sædvanlig  $\mathbb{F}_p$  betegne legemet  $\mathbb{Z}/p\mathbb{Z}$ , og lad

$$L = \mathbb{F}_p[X]/\langle X^2 + X + 1 \rangle$$

Lad  $\omega = [X] = X + \langle X^2 + X + 1 \rangle$  være klassen for  $X$ .

- (1) Antag at  $a \in \mathbb{F}_p$  er rod i  $X^2 + X + 1$ , altså  $a^2 + a + 1 = 0$ . Så er  $a^3 + a^2 + a = 0$ , og ved at trække disse fra hinanden får man  $a^3 - 1 = 0$ , altså  $a^3 = 1$ . Så er ordenen af  $a$  i  $\mathbb{F}_p^*$  divisor i 3, og da  $a = 1$  er en umulighed ( $1 + 1 + 1 = 3 \neq 0$  i  $\mathbb{F}_p$ , da  $p$  er et primtal og  $p \neq 3$ ), må ord  $a$  være 3. Da der er  $p - 1$  elementer i  $\mathbb{F}_p^*$ , og  $p - 1 \equiv 1 \pmod{3}$ , er det en modstrid med at ordenen af elementet  $a$  skal gå op i gruppens orden. Derfor har  $X^2 + X + 1$  ingen rødder i  $\mathbb{F}_p$ .
- (2) Da polynomiet  $X^2 + X + 1$  ingen rødder har, er det irreducibelt, og derfor er  $\langle X^2 + X + 1 \rangle$  et maksimalt ideal, og derfor er  $L$  et legeme (proposition 4.6.3). Af proposition 4.6.6 følger så, at ethvert element  $y$  i  $L$  entydigt kan skrives som  $y = a\omega + b$  hvor  $a, b \in \mathbb{F}_p$ , og at der til ethvert talpar  $a, b \in \mathbb{F}_p$  svarer et element i  $L$ . Der er  $p^2$  sådanne talpar, så  $|L| = p^2$ .
- (3) En lille regning viser at  $(2\omega + 1)^2 = 4\omega^2 + 4\omega + 1 = 4(\omega^2 + \omega + 1) - 3 = -3$  hvor jeg for nemheds skyld har udeladt []. Betragt nu  $f = X^2 + 3 \in L[X]$ . Vi har at  $\pm(2\omega + 1)$  er rødder i  $f$ , og  $f$  kan derfor faktoriseres som  $f = (X - (2\omega + 1))(X + (2\omega + 1))$ . Da  $L$  er et legeme, følger af proposition 4.6.1 at  $L[X]$  er et UFD, og derfor er denne faktorisering entydig (bortset fra multiplikation med enheder); således er  $\pm(2\omega + 1)$  de eneste rødder og dermed de eneste der opfylder  $(a\omega + b)^2 = [-3]$ .
- (4) Hvis  $p \mid n^2 + 3$  for et  $n \in \mathbb{N}$ , vil  $n^2 + 3 \equiv 0 \pmod{p}$ , og dermed er  $[n]$  rod i polynomiet  $f$  fra (3). Men dette kan ikke lade sig gøre, da de eneste rødder var  $\pm(2\omega + 1)$ , og ingen af disse har " $\omega$ -del" 0.

### Opgave 3

Lad  $F$  være et legeme,  $R \subseteq F$  en delring af  $F$  og  $\mathfrak{p} \subseteq R$  et primideal i  $R$ .

- (1) Lad

$$R_1 = \{ab^{-1} \mid a \in R, b \in R \setminus \mathfrak{p}\}$$

Så er  $R_1$  lukket under addition, fordi  $ab^{-1} + cd^{-1} = (ad + cb)(bd)^{-1}$ , og da  $\mathfrak{p}$  er et primideal, vil  $b, d \notin \mathfrak{p}$  medføre at  $bd \notin \mathfrak{p}$ .  $0 \in R_1$  (vælg blot  $a = 0$ ), og hvis  $ab^{-1} \in R_1$  vil  $(-a)b^{-1} = -ab^{-1}$  ligge i  $R_1$ . At  $1 \in R_1$  følger af, at man blot kan vælge et  $b \in R \setminus \mathfrak{p}$  og derefter sætte  $a = b$ , og at  $R_1$  er lukket under multiplikation følger af at  $(ab^{-1})(cd^{-1}) = (ac)(bd)^{-1}$ , og igen har vi jo at  $bd \notin \mathfrak{p}$ . Altså er  $R_1$  en delring af  $F$ .

(2) Lad

$$\mathfrak{p}_1 = \{ab^{-1} \mid a \in \mathfrak{p}, b \in R \setminus \mathfrak{p}\}$$

Da  $\mathfrak{p} \subseteq R$ , er  $\mathfrak{p}_1 \subseteq R_1$ . Som før kontrolleres let, at  $\mathfrak{p}_1$  er en gruppe mht.  $+$ , thi  $ab^{-1} + cd^{-1} = (ad + cb)(bd)^{-1} \in \mathfrak{p}_1$ , da  $\mathfrak{p}$  er lukket under multiplikation og addition, og det er et primideal,  $0 \in \mathfrak{p}_1$  og  $-ab^{-1} \in \mathfrak{p}_1$ . Lad nu  $\lambda = cd^{-1} \in R_1$  og  $ab^{-1} \in \mathfrak{p}_1$ . Så er  $cd^{-1}ab^{-1} = ca(db)^{-1} \in \mathfrak{p}_1$ ; da  $a \in \mathfrak{p}$  og  $c \in R$ , og  $\mathfrak{p}$  er et ideal i  $R$  vil jo  $ca$  tilhøre  $\mathfrak{p}$ , og som før bruges at  $\mathfrak{p}$  er et primideal så  $db \in R \setminus \mathfrak{p}$ .

Antag  $u = ab^{-1}$  er en enhed i  $R_1$ . Så kan vi ikke have at  $u \in \mathfrak{p}_1$ , da det ville medføre at  $1 \in \mathfrak{p}_1$ , og dermed at  $\mathfrak{p}_1 = R_1$ .

Lad nu  $x = ab^{-1} \in R_1 \setminus \mathfrak{p}_1$ . Så ønsker jeg at vise, at  $ba^{-1} \in R_1$  således at  $x$  er en enhed. Da  $b \in R \setminus \mathfrak{p}$ , har vi i hvert fald at  $b \in R$ . Tilbage er blot at vise, at  $a \in R \setminus \mathfrak{p}$ . Antag at  $a \in \mathfrak{p}$ . Så er  $a$  et element i  $\mathfrak{p}_1$  (idet  $1 \in R \setminus \mathfrak{p}$ ), og så vil  $ab^{-1}$  også være et element i  $\mathfrak{p}_1$  i modstrid med antagelsen.

(3) Hvis  $I$  er et vilkårligt ideal i  $R_1$ , som ikke er hele  $R_1$ , kan  $I$  ikke indeholde nogen enheder. Altså er  $I \subseteq R_1 \setminus \mathfrak{p}_1$ , og dermed er  $\mathfrak{p}_1$  det eneste maksimale ideal i  $R_1$ .

(4) Definer  $\varphi: R/\mathfrak{p} \rightarrow R_1/\mathfrak{p}_1$  ved  $\varphi(x + \mathfrak{p}) = x + \mathfrak{p}_1$ . For det første er  $\varphi$  veldefineret, fordi hvis  $x_1 + \mathfrak{p} = x_2 + \mathfrak{p}$ , vil  $x_1 - x_2 \in \mathfrak{p}$ , og da  $\mathfrak{p} \subseteq \mathfrak{p}_1$  vil også  $x_1 - x_2 \in \mathfrak{p}_1$ , og så er  $x_1 + \mathfrak{p}_1 = x_2 + \mathfrak{p}_1$ . Antag nu at  $x_1 + \mathfrak{p}_1 = x_2 + \mathfrak{p}_1$ , hvor  $x_1, x_2 \in R$ . Så vil  $x_1 - x_2 \in \mathfrak{p}_1 \cap R$ . Da  $x_1 - x_2 \in \mathfrak{p}_1$  er  $x_1 - x_2 = ab^{-1}$  hvor  $a \in \mathfrak{p}$  og  $b \in R \setminus \mathfrak{p}$ . Vi får så at  $b(x_1 - x_2) = a \in \mathfrak{p}$ , og da  $\mathfrak{p}$  er et primideal, vil en af faktorerne på højresiden ligge i  $\mathfrak{p}$ . Da det ikke er  $b$ , må  $x_1 - x_2 \in \mathfrak{p}$ , og derfor er  $x_1 + \mathfrak{p} = x_2 + \mathfrak{p}$ ; således er  $\varphi$  injektiv.

## Juni 1999

### Opgave 1

Lad  $\mathbb{F}_q$  være et endeligt legeme med  $q$  elementer. For  $c \in \mathbb{F}_q$  defineres

$$f_c(x) = X^3 - (c + 1)X^2 + cX + 1 \in \mathbb{F}_q[X]$$

- (1) Hvis vi har et polynomium  $g$  af grad  $\geq 1$  som går op i både  $f_{c_1}$  og  $f_{c_2}$ , har vi altså

$$\begin{aligned} f_{c_1} &= gp_1 \\ f_{c_2} &= gp_2 \end{aligned}$$

Nu er  $\deg g$  jo nødvendigvis enten 1 eller 2. Hvis  $\deg g = 1$  har  $f_{c_1}$  og  $f_{c_2}$  en fælles rod; lad os kalde den  $a$ . Først observeres, at  $f_c(0) = f_c(1) = 1$  for alle  $c \in \mathbb{F}_q$ , og en række udregninger giver så

$$\begin{aligned} 0 &= a^3 - (c_1 + 1)a^2 + c_1a + 1 = a^3 - (c_2 + 1)a^2 + c_2a + 1 \\ &\quad -c_1a^2 + c_1a = -c_2a^2 + c_2a \\ &\quad c_1(1 - a) = c_2(1 - a) \end{aligned}$$

hvor jeg undervejs har benyttet, at man i et legeme kan forkorte med alt hvad der ikke er 0. Da jo  $a \neq 1$  har vi endelig at  $c_1 = c_2$ .

Hvis  $\deg g = 2$ , vil polynomierne  $p_1$  og  $p_2$  begge have grad 1 og således begge have en rod. Kald rødderne  $a_1$  henholdsvis  $a_2$ . Konstantleddet i  $g$  kaldes  $k$ , og vi har så at  $ka_1 = ka_2 = 1$ ; og da multiplikativ invers er entydig må vi have at  $a_1 = a_2$ ; og dermed har  $f_{c_1}$  og  $f_{c_2}$  en fælles rod, så med argumentet ovenfor er  $c_1 = c_2$ .

- (2) For  $c \in \mathbb{F}_q$  defineres mængden  $M_c = \{\alpha \in \mathbb{F}_q \mid f_c(\alpha) = 0\}$ , også kendt som  $V(f_c)$ . Det er klart fra det ovenstående, at  $c_1 \neq c_2 \Rightarrow M_{c_1} \cap M_{c_2} = \emptyset$ , thi hvis snittet ikke var tomt ville  $c_1$  være lig  $c_2$  jf. det ovenstående.

Hvis ingen af mængderne  $M_c$  er tomme, må de alle indeholde mindst et element. Da der er netop  $q$  af disse mængder, og de snitter indbyrdes tomt, må de alle bestå af netop ét element (der er jo kun  $q$  elementer "at tage af"). Men så må der specielt være et  $c \in \mathbb{F}_q$  så at  $M_c = \{0\}$ , men 0 er jo ikke rod i noget polynomium. Altså kan ikke alle mængderne være ikke-tomme.

- (3) Lad  $c$  betegne et element i  $\mathbb{F}_q$  for hvilket  $M_c = \emptyset$ . Så er  $f_c$  altså et tredjegradspolynomium uden rødder i  $\mathbb{F}_q$ , og er derfor irreducibelt jf. proposition 4.6.3v. Ifølge bemærkning 4.6.7 er så  $\mathbb{F}_q[X]/\langle f_c \rangle$  et legeme.
- (4) Vi ved, at for ethvert primtal  $p$  er  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  et legeme. Ovenfor er det vist, at vi kan finde et irreducibelt tredjegradspolynomium  $f \in \mathbb{F}_p[X]$ . Kvotientringen  $\mathbb{F}_p[X]/\langle f \rangle$  er så også et legeme, og antallet af elementer er netop  $p^3$ .

### Opgave 3

Lad  $R$  være en endelig kommutativ ring. For  $a \in R$  defineres  $m_a: R \rightarrow R$  ved

$$m_a(x) = ax$$

- (1) Vi har, at  $m_a(x_1 + x_2) = a(x_1 + x_2) = ax_1 + ax_2 = m_a(x_1) + m_a(x_2)$ , så  $m_a$  er en gruppehomomorfi fra  $(R, +)$  til  $(R, +)$ . Hvis det også skal være en ringhomomorfi, skal vi jo kræve, at  $m_a(1) = 1$ , og dette er opfyldt hvis og kun hvis  $a = 1$  (dvs.  $m_a = \text{Id}_R$ ). Hvis  $a = 1$  er det klart at  $m_a(x_1x_2) = m_a(x_1)m_a(x_2)$ .
- (2) Det skal vises, at  $\ker(m_a)$  er et ideal i  $R$ . Hvis  $x, y \in \ker(m_a)$  har vi at  $m_a(x) = m_a(y) = 0$ , og da  $m_a$  er en gruppehomomorfi er også  $m_a(x+y) = 0$ , og således vil  $x+y \in \ker(m_a)$ . Trivielt har vi at  $0 \in \ker(m_a)$ , og ligeså har vi at hvis  $m_a(x) = 0$  vil  $m_a(-x)$  også være 0. Tilbage er at vise, at  $\ker(m_a)$  er lukket under multiplikation med elementer fra  $R$ . Hvis  $\lambda$  er et vilkårligt element i  $R$  og  $x \in \ker(m_a)$  har vi  $m_a(\lambda x) = a\lambda x = \lambda ax = \lambda 0 = 0$ , så  $\lambda x \in \ker(m_a)$ .

Tilsvarende skal det vises, at  $\text{Im}(m_a)$  er et ideal i  $R$ . De tre første betingelser er trivielt opfyldt, thi to elementer  $\chi, \psi \in \text{Im}(m_a)$  må være på formen  $\chi = ax$  og  $\psi = ay$ , hvor  $x, y \in R$ . Så vil også  $\chi + \psi = ax + ay = a(x+y) \in \text{Im}(m_a)$ , da  $x+y \in R$ ;  $0 \in \text{Im}(m_a)$  da  $m_a(0) = a \cdot 0 = 0$ , og  $-\chi \in \text{Im}(m_a)$  fordi  $-x \in R$ . Lad nu  $\lambda$  være et vilkårligt element i  $R$  og  $\chi = ax$  et element i  $\text{Im}(m_a)$ . Så er  $\lambda\chi = \lambda ax = a\lambda x = m_a(\lambda x)$ , og da  $\lambda x \in R$  vil  $\lambda\chi \in \text{Im}(m_a)$ .

- (3) Lad  $a \in R \setminus \{0\}$  være givet. Det skal vises, at følgende er ensbetydende:

- (i)  $a \in R^*$ .
- (ii)  $m_a: R \rightarrow R$  er bijektiv.
- (iii)  $a$  er ikke nuldivisor.

Antag først, at  $a$  er en enhed. Så vil  $m_a$  være surjektiv, thi elementet  $y \in R$  rammes af elementet  $a^{-1}y \in R$ . Da  $R$  har endeligt mange elementer, vil  $m_a$  således være en bijektion.

Hvis  $m_a$  er bijektiv, har vi at  $m_a(0) = 0$ , og derfor er  $m_a(x) = ax \neq 0$  for alle  $x \in R \setminus \{0\}$ ; således er  $a$  ikke nuldivisor.

Den sidste implikation (iii) $\Rightarrow$ (i) vises ved kontraposition. Antag derfor, at  $a$  ikke er en enhed; så skal det vises at  $a$  er nuldivisor. I følgen  $a, a^2, a^3, \dots$  optræder elementet 1 aldrig, men så kan  $a$  heller ikke findes efter det første gang har optrådt. Hvis  $a^2 \neq 0$  kan det ligeledes heller ikke optræde mere end den ene gang; og da der er et endeligt antal elementer i  $R$  ser man, at fra et vist trin er  $a^n = 0$ ; hvis  $k$  betegner det mindste  $n \in \mathbb{N}_{>0}$  således at  $a^n = 0$  har vi at  $aa^{k-1} = 0$  så  $a$  er en nuldivisor.

Således er det vist at (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i) som ønsket.

- (4) Hvis  $R$  er et integritetsområde (“domain”), har  $R$  ingen nuldivisorer. Altså gælder for alle  $a \in R \setminus \{0\}$  at  $a$  er en enhed (jf. den sidste implikation i 3.); og dermed har vi at  $R^* = R \setminus \{0\}$  så  $R$  er et legeme.
- (5) Lad  $I$  være et primideal i  $R$ . Så har vi jf. §3.2.2 og opgave III.17 at  $R/I$  er et integritetsområde (“domain”). Denne ring har selvfølgelig også et endeligt antal elementer (faktisk  $|R|/|I|$ ), og anvendes 4. på ringen  $R/I$  får vi, at  $R/I$  er et legeme. Men så er  $I$  et maksimalt ideal jf. §3.2.3.

## Januar 2000

### Opgave 1

Lad  $\mathbb{F}_2$  betegne  $\mathbb{Z}/2\mathbb{Z}$ .

- (a)  $X^5 + X + 1$  er ikke irreducibel i  $\mathbb{F}_2[X]$ , for man finder med lidt snilde at  $X^5 + X + 1 = (X^2 + X + 1)(X^3 + X^2 + 1)$ .
- (b) Hvis  $X^4 + X + 1$  ikke er irreducibel i  $\mathbb{F}_2[X]$ , skulle vi kunne finde en faktorisering i to polynomier som enten har grad henholdsvis 1 og 3 eller begge har grad 2. Da  $X^4 + X + 1$  ikke har nogen rødder i  $\mathbb{F}_2$ , er der ingen førstegradspolynomier der går op. Den eneste mulige irreducible faktorisering er derfor 2 + 2-tilfældet. Men da  $X^2 + X + 1$  er det eneste irreducible andengradspolynomium, skulle  $X^4 + X + 1$  være lig  $(X^2 + X + 1)^2$ , hvilket en lille udregning viser ikke er tilfældet:  $(X^2 + X + 1)^2 = X^4 + 2X^3 + 3X^2 + 2X + 1 = X^4 + X^2 + 1$ . Altså må  $X^4 + X + 1$  være irreducibel.
- (c) Da  $X^4 + X + 1$  er irreducibel, er  $\langle X^4 + X + 1 \rangle$  et maksimalt ideal, og derfor er  $L = \mathbb{F}_2[X]/\langle X^4 + X + 1 \rangle$  et legeme med  $2^4 = 16$  elementer (proposition 4.6.3 og 4.6.6).
- (d)  $L^*$  er en multiplikativ cyklisk gruppe pr. teorem 4.5.1 (hvor  $L^*$  betragtes som en undergruppe af sig selv; og  $|L^*| = 15 < \infty$ ). Lad  $\alpha = [X]$ . Så kan man udregne

$$\begin{aligned}\alpha^2 &= [X^2] \\ \alpha^3 &= [X^3] \\ \alpha^4 &= [X^4] = [X + 1] \\ \alpha^5 &= [X^2 + X]\end{aligned}$$

Vi har således, at  $\text{ord}(\alpha) > 5$ , men da et elements orden skal gå op i gruppens orden (som er 15), må  $\text{ord}(\alpha)$  være lige 15; således er  $\alpha$  en frembringer for  $L^*$ .

### Opgave 2

Lad  $I \subseteq k[X, Y, Z]$  betegne idealet  $\langle X^2 - Y, Z^3 + Y^2 \rangle$ , hvor  $k$  er et legeme. Lad  $\leq$  betegne den leksikografiske ordning med  $X \geq Y \geq Z$ .

- (a) Det skal vises, at  $F = (\underline{X}^2 - Y, Z^3 + \underline{Y}^2)$  er en Gröbnerbasis for  $I$ . Hertil benyttes Buchbergers  $\mathcal{S}$ -kriterium, og ved udregning får man

$$\mathcal{S}(\underline{X}^2 - Y, \underline{Y}^2 + Z^3) = Y^2(X^2 - Y) - X^2(Y^2 + Z^3) = \underline{-X^2Z^3} - Y^3$$

Divideres dette med  $F$  får man

$$\begin{array}{r} \underline{-X^2Z^3 - Y^3} \quad : \quad (\underline{X^2 - Y}, \underline{Y^2 + Z^3}) \\ \underline{-X^2Z^3 + YZ^3} \\ -Y^3 - YZ^3 \\ \underline{-Y^3 - YZ^3} \\ 0 \end{array}$$

Derfor er  $F$  jf. Buchbergers  $\mathcal{S}$ -kriterium en Gröbnerbasis for  $\langle F \rangle = I$ .

Man ser let, at  $F$  er en minimal Gröbnerbasis, thi  $X^2$  ikke går op i  $Y^2$  og vice versa, og koefficienterne til initialtermerne begge steder er 1. Desuden har vi, at  $X^2$  ikke går op i  $Z^3$ , og  $Y^2$  ikke går op i  $-Y$ , så  $F$  er sågar reduceret.

- (b) Vi har fra proposition 5.4.2 at  $f = X^3 - XY + Y^2 + Z^4 + ZY^2$  ligger i  $I$  hvis og kun hvis polynomiet ved division med en Gröbnerbasis for  $I$  giver 0. Lad os derfor udføre denne division:

$$\begin{array}{r} \underline{X^3 - XY + Y^2 + Z^4 + ZY^2} \quad : \quad (\underline{X^2 - Y}, \underline{Y^2 + Z^3}) \\ \underline{X^3 - XY} \\ \underline{ZY^2 + Y^2 + Z^4} \\ \underline{ZY^2 + Z^4} \\ Y^2 \quad \longrightarrow \quad \text{rest} \end{array}$$

Vi får således en rest der er forskellig fra 0, og derfor ligger polynomiet  $f$  ikke i  $I$ .

### Opgave 3

- (a) Der skal findes hele tal  $\lambda, \mu$  så  $49\lambda + 13\mu = 1$ . Nogle få linjers udregninger giver

$$\begin{aligned} 10 &= 49 - 3 \cdot 13 \\ 3 &= 13 - 10 = 4 \cdot 13 - 49 \\ 1 &= 10 - 3 \cdot 3 = 49 - 3 \cdot 13 - 3(4 \cdot 13 - 49) \\ 1 &= 4 \cdot 49 - 15 \cdot 13 \end{aligned}$$

så de søgte tal er  $\lambda = 4$  og  $\mu = -15$ .

Heraf følger, at  $[13]$  er en enhed i  $\mathbb{Z}/49\mathbb{Z}$ , da  $[-15][13] = [1] - [4][49] = [1]$  (da jo  $[49] = [0]$ ).

Lad  $R$  betegne ringen  $\mathbb{Z}/p^l\mathbb{Z}$  hvor  $p$  er et primtal og  $l > 0$  er et naturligt tal.

- (b) Hvis  $l > 1$  vil såvel  $[p]$  som  $[p^{l-1}]$  være forskellig fra 0, og deres produkt er  $[p][p^{l-1}] = [p^l] = [0]$ ; der er således nuldivisorer i  $R$  og  $R$  er derfor ikke et integritetsområde.
- (c) Vi har, at  $|R| = p^l$ . Enhederne i  $R$  er netop de  $[x]$ , hvor det WLOG kan antages at  $0 \leq x \leq p^l - 1$ , som er indbyrdes primiske med  $p^l$ , og disse er der  $\varphi(p^l) = p^l - p^{l-1}$  af (§1.8.3). Altså må der være  $p^l - (p^l - p^{l-1}) = p^{l-1}$  ikke-enheder i  $R$ .
- (d) Lad  $r \in R$  opfylde at  $r^2 = r$ . Så har vi at  $r^2 - r = r(r - 1) = [0] = [p^l]$ , og (hvis man et øjeblik ikke skelner mellem et helt tal og klassen hørende til dette hele tal) da  $p$  ikke kan gå op i to på hinanden følgende hele tal, må enten  $p^l \mid r$  eller  $p^l \mid r - 1$ ; hvorved man kan konkludere at enten er  $r = [p^l] = 0$  eller  $r - 1 = [p^l] = [0]$ , dvs.  $r = [0]$  eller  $r = [1]$ .

#### Opgave 4

- (a) Hvis  $x$  skal opfylde, at

$$\begin{aligned} x &\equiv 2 \pmod{7} \\ x &\equiv 3 \pmod{15} \end{aligned}$$

har vi jf. teorem 1.6.3 (da  $\gcd(7, 15) = 1$ ) at en løsning er

$$2 \cdot 1 \cdot 15 + 3 \cdot (-2) \cdot 7 = -12$$

hvor tallene 1 og  $-2$  er de  $\mu$ 'er der optræder i sætningen, og herved er  $x = -12 + 105 = 93$  også en løsning.

- (b) Det følger af samme sætning som ovenfor, at hvis man har to løsninger  $\alpha$  og  $\beta$  til ovenstående kongruenser, så vil  $\alpha \equiv \beta \pmod{105}$ .
- (c) Det skal vises, at der findes netop to naturlige tal mellem 1 og 105 som opfylder kongruenssystemet

$$\begin{aligned} x^3 - 2x + 3 &\equiv 0 \pmod{7} \\ 2x^2 &\equiv 3 \pmod{15} \end{aligned}$$

Ved at gange den anden kongruens med 8 (som er  $2^{-1} \pmod{15}$ ), får man at

$$x^2 \equiv 9 \pmod{15}$$

hvilket igen vil sige at

$$\begin{cases} x^2 \equiv 0 \pmod{3} \\ x^2 \equiv 4 \pmod{5} \end{cases}$$

og heraf får vi endelig

$$\begin{cases} x \equiv 0 \pmod{3} \\ x \equiv \pm 2 \pmod{5} \end{cases}$$

Ved at udregne resten af polynomiet  $x^3 - 2x + 3$  ved division med 7 for  $x$ -værdierne  $-3, \dots, 3$  finder man, at polynomiet er kongruent med 0 modulo 7 hvis og kun hvis  $x$  er kongruent med 2 modulo 7. Vi har altså nu oversat det oprindelige ikke-lineære kongruenssystem til følgende:

$$\begin{cases} x \equiv 0 & (\text{mod } 3) \\ x \equiv \pm 2 & (\text{mod } 5) \\ x \equiv 2 & (\text{mod } 7) \end{cases}$$

Da 3, 5, 7 er indbyrdes primiske, har hvert af disse kongruenssystemer en entydig løsning med  $1 \leq x \leq 105$ ; således er der som ønsket netop to løsninger.

## Juni 2000

### Opgave 1

Lad  $R$  betegne ringen  $\mathbb{Z}[i]/\langle 1+3i \rangle$ , hvor  $\mathbb{Z}[i]$  som sædvanligt betegner ringen af Gaussiske heltal.

- (a) Vi har, at  $i-3 = i(1+3i)$ , så  $i-3 \in \langle 1+3i \rangle$ . Så er  $[i-3] = [0] \in R$ , og derfor er  $[i] = [3] \in R$ . Så har vi også at  $[i]^2 = [i^2] = [-1] = [3]^2 = [9]$ , og derfor  $[0] = [10] \in R$ . Endelig er  $[a+bi] = [a] + [b][i] = [a] + [b][3] = [a+3b]$ .
- (b) Den kanoniske ringhomomorfi  $\varphi: \mathbb{Z} \rightarrow R$  givet ved  $\varphi(1) = [1]$  må nødvendigvis sende  $x$  i  $[x]$  for alle  $x \in \mathbb{Z}$ . Vi har jf. (a) at  $[a+bi] = [a+3b] \in R$ , så ethvert element i  $R$  rammes af  $\varphi$  (vælg blot  $x = a+3b$ ), så  $\varphi$  er surjektiv.
- (c) Definer normfunktionen  $N: \mathbb{Z}[i] \rightarrow \mathbb{N}$  ved  $N(a+bi) = a^2+b^2$ ; den opfylder som sædvanligt at  $N(xy) = N(x)N(y)$ . Nu udregnes

$$N((1+3i)(a+bi)) = 10N(a+bi) = 10(a^2+b^2)$$

Hvis  $1+3i$  var en enhed, skulle vi kunne finde  $a, b \in \mathbb{Z}$  så  $10(a^2+b^2) = N(1) = 1$ , hvilket oplagt er umuligt. Tilsvarende er det umuligt at finde  $a, b$  så man får  $N(2) = 4$  eller  $N(5) = 25$ ; ergo går  $1+3i$  ikke op i hverken 2 eller 5 inden for  $\mathbb{Z}[i]$ .

Da  $[10] = [0]$ , har vi at  $\varphi(10\mathbb{Z}) = \{[0]\}$ , og dermed  $10\mathbb{Z} \subseteq \ker \varphi$ . Vi ved desuden, at kernen for en homomorfi er en undergruppe i homomorfiens domæne, så  $\ker \varphi = a\mathbb{Z}$ , hvor  $a$  så må være enten 1, 2, 5 eller 10. Ovenfor er det vist, at  $1, 2, 5 \notin \langle 1+3i \rangle$ , og derfor er  $[1], [2], [5] \neq [0] \in R$ . Altså vil  $\varphi(1), \varphi(2), \varphi(5)$  alle være forskellige fra  $[0]$  i  $R$ , og dermed er  $1, 2, 5 \notin \ker \varphi$ , så den eneste mulighed der lades tilbage er  $\ker \varphi = 10\mathbb{Z}$ .

- (d) Proposition 3.1.16 (hvor man gør klogt i at forestille sig at  $f$  er en *surjective* ringhomomorfi) giver, at  $\mathbb{Z}/10\mathbb{Z}$  er isomorf med kodomænet for  $\varphi$ , dvs.  $R$ .

### Opgave 2

- (a) Lad  $\tau \in S_3$  betegne 3-cyklen

$$(123) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Vi har, at  $|S_3| = 3! = 6$ , og  $|\langle \tau \rangle| = 3$ , så  $\langle \tau \rangle$  har index 2 i  $S_3$  og er derfor automatisk normal [opgave II.14(d)].

- (b) Lad  $\sigma \in S_5$  betegne 5-cyklen (12345). Så er  $\text{sgn}(\sigma) = (-1)^{5-1} = 1$  pr. proposition 2.8.17, så  $\sigma$  er en lige permutation. Undergruppen  $\langle \sigma \rangle$  består

af elementerne

$$\begin{aligned}(12345)^1 &= (12345) \\ (12345)^2 &= (13524) \\ (12345)^3 &= (14253) \\ (12345)^4 &= (15432) \\ (12345)^5 &= \text{Id}\end{aligned}$$

hvoraf man ser, at ordenen af  $\langle \sigma \rangle$  er 5.

- (c) Hvis  $\langle \sigma \rangle$  var en normal undergruppe af  $S_5$ , skulle den være stabil under konjugering med elementer fra  $S_5$ . Men fx er

$$(12)(12345)(12) = (13452)$$

og denne er ikke med i undergruppen. Altså kan  $\langle \sigma \rangle$  ikke være en normal undergruppe af  $S_5$ .

### Opgave 3

- (a) Da polynomiet  $f = X^3 + X + 1 \in \mathbb{F}_2[X]$  er irreducibelt (det har grad 3 og ingen rødder, thi  $f(0) = f(1) = 1$ ), følger af proposition 4.6.3i) at  $L$  er et legeme. Desuden står det at læse i beviset for sætning 4.7.1ii) at antallet af elementer i  $L$  er  $2^3 = 8$ .
- (b) Da  $L$  er et legeme, er  $L^* = L \setminus \{0\}$ . De 7 enheder i  $L$  er derfor ( $\alpha = [X]$ ):

$$L^* = \{1, 1 + \alpha, 1 + \alpha^2, 1 + \alpha + \alpha^2, \alpha, \alpha + \alpha^2, \alpha^2\}$$

Ved udregning fås, under gentagen anvendelse af reglerne  $[f] = 2 = 0 \in L$  og, at

$$\begin{aligned}\prod_{x \in L^*} x &= 1(1 + \alpha)(1 + \alpha^2)(1 + \alpha + \alpha^2)(\alpha)(\alpha + \alpha^2)(\alpha^2) \\ &= (1 + \alpha + \alpha^2 + \alpha^3)(1 + \alpha + \alpha^2)(\alpha)(\alpha + \alpha^2)(\alpha^2) \\ &= \alpha^5(1 + \alpha + \alpha^2)(\alpha + \alpha^2) \\ &= \alpha^6(\alpha + 2\alpha^2) \\ &= \alpha^7 \\ &= \alpha^3\alpha^3\alpha \\ &= (-\alpha - 1)(-\alpha - 1)\alpha \\ &= \alpha(\alpha + 1)^2 \\ &= \alpha^3 + 2\alpha^2 + \alpha \\ &= -1\end{aligned}$$

- (c) Lad  $K$  være et endeligt legeme med  $|K| = N$ . Vi har så, at  $N$  må være på formen  $N = p^n$ , hvor  $p$  er et primtal og  $n \in \mathbb{N}_{>0}$  (teorem 4.7.1). Vi kan desuden WLOG antage, at  $K = \mathbb{F}_{p^n}$ . Af afsnit 4.7.2 følger så, at

$$X^N - X = \prod_{x \in K} (X - x)$$

En af faktorerne på højresiden (svarende til  $x = 0$ ) kan forkortes ud, og tilbage står

$$X^{N-1} - 1 = \prod_{x \in K^*} (X - x),$$

og hermed er det vist, at  $X^{N-1} - 1 \in K[X]$  er et produkt af  $|K^*| = N - 1$  førstegradspolynomier med konstantled  $\neq 0$ .

- (d) Vi har fra det ovenstående, at  $-1 = \prod_{x \in K^*} (-x)$ . Ved at benytte, at der er  $N - 1$  elementer i  $K^*$  får man, at

$$(-1)^N = \prod_{x \in K^*} x$$

Der er nu to muligheder. Hvis  $N$  er ulige, vil  $(-1)^N = -1$ , og det ønskede er vist. Hvis  $N$  er lige, betyder det at  $p$  må være 2 (da  $p$  er et primtal). Altså er  $K = \mathbb{F}_2/\langle f \rangle$ , hvor  $\deg f = n$ . Elementer i  $K[X]$  er således på formen  $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}$ , hvor  $\alpha = [X]$  og  $a_i \in \mathbb{F}_2$ . Altså følger det ønskede af, at der inden for  $\mathbb{F}_2$  gælder, at  $1 = -1$ .

#### Opgave 4

Lad  $I \subseteq \mathbb{Q}[X, Y]$  betegne idealet

$$I = \langle X^2 + Y^2, X^3 + Y^3 \rangle,$$

og lad  $\leq$  være den leksikografiske ordning på  $\mathbb{Q}[X, Y]$  med  $X \geq Y$ .

- (a) Man finder let

$$S_1 = \mathcal{S}(\underline{X^2} + Y^2, \underline{X^3} + Y^3) = X(X^2 + Y^2) - (X^3 + Y^3) = \underline{XY^2} - Y^3$$

og

$$S_2 = \mathcal{S}(\underline{X^2} + Y^2, \underline{XY^2} - Y^3) = Y^2(X^2 + Y^2) - X(XY^2 - Y^3) = \underline{XY^3} + Y^4$$

Det gælder jo helt generelt at  $\mathcal{S}$ -polynomiet af  $f_1$  og  $f_2$  fra et ideal selv ligger i selvsamme ideal (da  $\mathcal{S}$ -polynomiet jo er givet som en differens mellem  $f_1$  og  $f_2$  ganget med passende polynomier fra polynomiumsringen, og idealet er jo netop lukket under disse operationer). Vi har derfor også, at  $S_1 - YS_2 = 2Y^4 \in I$ , og da vi arbejder indenfor  $\mathbb{Q}[X, Y]$  vil også  $\frac{1}{2}2Y^4 = Y^4$  tilhøre  $I$ .

- (b) Det påstås at  $F = (\underline{Y^4}, \underline{XY^2 - Y^3}, \underline{X^2 + Y^2})$  er *den* reducerede Gröbnerbasis for  $I$  med hensyn til  $\leq$ . Til at starte med vil jeg vise at det i det hele taget er en Gröbnerbasis:

$$\mathcal{S}(\underline{Y^4}, \underline{XY^2 - Y^3}) = XY^4 - Y^2(XY^2 - Y^3) = Y^5,$$

og da  $Y^5 = YY^4$  har vi oplagt rest 0 ved division med  $F$ .

$$\mathcal{S}(\underline{Y^4}, \underline{X^2 + Y^2}) = X^2Y^4 - Y^4(X^2 + Y^2) = -Y^6,$$

og her har vi igen trivielt at man får rest 0 ved division med  $F$ . Endelig er

$$\mathcal{S}(\underline{XY^2 - Y^3}, \underline{X^2 + Y^2}) = X(XY^2 - Y^3) - Y^2(X^2 + Y^2) = \underline{-XY^3 - Y^4},$$

som giver følgende ved division med  $F$ :

$$\begin{array}{r} \underline{-XY^3 - Y^4} \quad : \quad (\underline{Y^4}, \underline{XY^2 - Y^3}, \underline{X^2 + Y^2}) \\ \underline{-XY^3 + Y^4} \\ \hline -2Y^4 \\ \underline{-2Y^4} \\ \hline 0 \quad \longrightarrow \quad \text{rest} \end{array}$$

Buchbergers  $\mathcal{S}$ -kriterium giver nu, at  $F$  rent faktisk er en Gröbnerbasis mht.  $\leq$ . Den er desuden minimal, da ingen af initialtermene går i andre initialtermer; og endelig er alle ledende koefficienter 1, og initialtermene går ejheller op i nogen andre termer i de andre polynomier, så er  $F$  reduceret. at det er *den* reducerede basis følger af at den er entydig (teorem 5.8.3).

- (c) Det skal vises, at  $(X^2 + Y^2, X^3, Y^3)$  ikke er en Gröbnerbasis for  $I$  for nogen termordning. Lad derfor  $\succeq$  være en given termordning. Vi kan WLOG antage, at der gælder  $X \succeq Y$  på grund af symmetri. Men så vil  $X^2 \succeq XY$  (da  $(1, 0) \succeq (0, 1)$  vil  $(2, 0) \succeq (1, 1)$ ), og heraf får man så igen at  $X^2 \succeq Y^2$ . På samme måde indser man at  $X^3 \succeq Y^3$ . Hvis vi udregner  $\mathcal{S}(X^2 + Y^2, X^3 + Y^3)$  får man  $XY^2 - Y^3$ . Det kan ikke umiddelbart afgøres hvad der er initialtermen her; men ingen af initialtermene  $X^2$  og  $X^3$  går op i nogen af termerne i  $\mathcal{S}$ -polynomiet, så man vil ikke få 0 ved division med  $(X^2 + Y^2, X^3, Y^3)$ ; altså kan det ikke være en Gröbnerbasis jf. Buchbergers  $\mathcal{S}$ -kriterium.

## Januar 2001

### Opgave 1

- (a) Vi har, at førstegradspolynomier altid er irreducible; specielt er  $X + 1 \in \mathbb{F}_2[X]$  irreducibel. Desuden er et andengradspolynomium irreducibelt hvis og kun hvis det ingen rødder har (proposition 4.6.3), og det har  $X^2 + X + 1$  jo ikke i  $\mathbb{F}_2$ . Da desuden  $(X^2 + X + 1)(X + 1) = X^3 + X^2 + X + X^2 + X + 1 = X^3 + 1$  er  $(X^2 + X + 1)(X + 1)$  som ønsket en irreducibel faktorisering af  $X^3 + 1$  i  $\mathbb{F}_2[X]$ .
- (b) Lad  $R$  betegne  $\mathbb{F}_2[X]/\langle X^3 + 1 \rangle$ . Så giver proposition 4.6.6 at

$$|R| = |\mathbb{F}_2|^{\deg(X^3+1)} = 2^3 = 8.$$

Desuden har vi at

$$(\alpha^2 + \alpha + 1)(\alpha + 1) = \alpha^3 + 1 = 0 \in R,$$

da jo  $[X^3 + 1] = [0]$  i  $R$ .

- (c) Vi har jf. (b) at  $\alpha^2 + \alpha + 1$  og  $\alpha + 1$  er nuldivisorer, og kan derfor ikke være enheder (opgave III.1). Desuden er  $\alpha^2 + \alpha = \alpha(\alpha + 1)$ , og da  $\alpha + 1$  er en nuldivisor vil også  $\alpha^2 + \alpha$  være det; tilsvarende er  $\alpha^2 + 1 = (\alpha + 1)(\alpha + 1)$ , så dette er også en nuldivisor og dermed ikke en enhed.
- (d) Vi har, at i hvert fald 5 af de 8 elementer i  $R$  ikke er enheder (de 4 behandlet ovenfor samt  $[0]$ ). Tilbage er elementerne  $[1]$ ,  $\alpha$  og  $\alpha^2$ , og disse er klart enheder (thi et-elementet er  $[1]$ , og  $\alpha\alpha^2 = \alpha^3 = [1]$ , da jo  $\alpha^3 + [1] = [0]$ ). Desuden er  $R^* = \langle \alpha \rangle$  (og den er i øvrigt også frembragt af  $\alpha^2$ ).

### Opgave 2

Betragt grupperne  $(\mathbb{Z}, +)$  og  $(\mathbb{Q}, +)$ . Det er klart, at de er abelske (addition er kommutativ), og at  $\mathbb{Z} \subset \mathbb{Q}$ .

Lad  $[q] = q + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ , hvor  $q \in \mathbb{Q}$ .

- (a) Ordenen af  $g = [\frac{9}{4}] \in \mathbb{Q}/\mathbb{Z}$  findes ved at betragte

$$g, g^2, g^3, \dots,$$

altså sammensætningen af  $g$  med sig selv et antal gange, og så finde det mindste positive  $n$  for hvilket  $g^n = [0]$  (da det er oplagt at  $[0]$  er det neutrale element i  $\mathbb{Q}/\mathbb{Z}$ ). Vi har at

$$\begin{aligned} g^1 &= [\frac{9}{4}] \neq [0] \\ g^2 &= g + g = [\frac{9}{4} + \frac{9}{4}] = [\frac{9}{2}] \neq [0] \\ g^3 &= g^2 + g = [\frac{9}{2} + \frac{9}{4}] = [\frac{27}{4}] \neq [0] \\ g^4 &= g^3 + g = [\frac{27}{4} + \frac{9}{4}] = [\frac{36}{4}] = [0], \end{aligned}$$

da jo  $\frac{36}{4} = 9 \in \mathbb{Z}$  og  $9 + \mathbb{Z} = 0 + \mathbb{Z} = \mathbb{Z}$ . Altså er  $\text{ord}(g) = 4$ .

- (b) Lad  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N} \setminus \{0\}$ , og  $\gcd(a, b) = 1$ . For at finde ordenen af  $[\frac{a}{b}]$  betragtes som før  $[\frac{a}{b}]^n$  for hele positive  $n$ . En tilsvarende udregning giver at

$$\left[\frac{a}{b}\right]^n = \left[\frac{na}{b}\right],$$

og vi har jo at

$$\left[\frac{\alpha}{\beta}\right] = [0] \iff \frac{\alpha}{\beta} \in \mathbb{Z} \iff \beta \mid \alpha.$$

Derfor får vi, at det mindste positive tal  $n$ , så  $b \mid na$ , må være  $b$ . Altså er  $\text{ord}([\frac{a}{b}]) = b$ .

Da alle rationale tal har en entydig repræsentation som en uforkortelig brøk med positiv nævner, ser man, at alle elementer i  $\mathbb{Q}/\mathbb{Z}$  har endelig orden, nemlig denne entydige positive nævner. Samtidig har vi, at  $\gcd(1, n) = 1$  for alle  $n \in \mathbb{N} \setminus \{0\}$ , og derfor at  $\text{ord}([\frac{1}{n}]) = n$ , så der findes elementer af vilkårlig høj orden i  $\mathbb{Q}/\mathbb{Z}$ .

- (c) Fra (b) fås let, at  $\mathbb{Q}/\mathbb{Z}$  må være en uendelig gruppe. Thi da alle elementer har endelig orden, og der findes elementer af arbitrær stor orden, kan man for modstrid antage at der kun findes endeligt mange elementer  $g_1, g_2, \dots, g_k$ , med ordener  $\psi_1, \psi_2, \dots, \psi_k$ ; lad  $K = \max(\psi_1, \psi_2, \dots, \psi_k) \in \mathbb{N}$ . Men vi har at der findes elementer af orden højere end et hvilket som helst naturligt tal, så  $\zeta$ .

For at vise, at  $\mathbb{Q}/\mathbb{Z}$  ikke er cyklisk, antages det at  $\mathbb{Q}/\mathbb{Z}$  er frembragt af fx  $g = [\frac{a}{b}]$ , altså at

$$\mathbb{Q}/\mathbb{Z} = \langle g \rangle.$$

Men vi har jo fra (b) at  $\text{ord}(g) = |\langle g \rangle| < \infty$ , mens vi fra det ovenstående har at  $|\mathbb{Q}/\mathbb{Z}| = \infty$ , så igen har vi  $\zeta$ .

### Opgave 3

Lad  $e = (1)(2)(3)(4)$ ,  $\tau_1 = (12)(34)$ ,  $\tau_2 = (14)(23)$  og  $\tau_3 = (24)(13)$ , og

$$H = \{e, \tau_1, \tau_2, \tau_3\} \subseteq S_4.$$

- (a) Ved udregning finder man at  $\tau_1\tau_2 = (12)(34)(14)(23) = (13)(24) = \tau_3$ , og tilsvarende finder man at  $\tau_i\tau_j = \tau_k$  hvor  $\{i, j, k\} = \{1, 2, 3\}$ . Desuden er  $\tau_i^2 = e$  og  $e\tau_i = \tau_i e = \tau_i$  for  $i = 1, 2, 3$ . Altså er  $H$  en undergruppe af  $S_4$ .
- (b) Det skal vises at  $H$  er en normal undergruppe af  $S_4$ . Lad derfor  $\sigma \in S_4$ , og det skal så vises, at  $\sigma H \sigma^{-1} = H$ . Vi har, at  $\sigma e \sigma^{-1} = e$ , og desuden har vi at  $\sigma \tau_i \sigma^{-1} \in C(\tau_i)$ , altså konjugeringsklassen for  $\tau_i$ . Jf. §2.9.2 er konjugeringsklassen for et af  $\tau_i$ 'erne netop elementerne i  $S_4$  med samme cykeltype, og da  $\tau_i$  har cykeltype  $2+2$ , og samtlige permutationer af denne cykeltype (der er 3) ligger i  $H$ , har vi at  $\sigma \tau_i \sigma^{-1} \in H$ . Det er således vist, at  $\sigma H \sigma^{-1} \subseteq H$  for alle  $\sigma \in S_4$ . Lad nu  $x \in H$ , så skal det vises at  $\exists y \in H$  så  $\sigma y \sigma^{-1} = x$ . Sættes  $y = \sigma^{-1} x \sigma$ , har vi at  $y = (\sigma^{-1}) x (\sigma^{-1})^{-1} \in H$ ,

da vi jo har at  $\sigma H \sigma^{-1} \subseteq H$  for alle  $\sigma$ , og dermed også for  $\sigma^{-1}$ . Da det hermed er vist at  $y \in H$ , vil  $H \subseteq \sigma H \sigma^{-1}$  for alle  $\sigma \in S_4$ , og endelig kan vi konkludere at  $\sigma H \sigma^{-1} = H$  for ethvert  $\sigma$ .

- (c) En 3-cykel i  $S_4$  er bestemt ved hvilket element den ikke flytter, og derefter om  $a$  afbildes i  $b$  eller  $c$ ; man finder derfor at samtlige 3-cykler i  $S_4$  er

$$\begin{array}{cccc} (123) & (124) & (134) & (234) \\ (132) & (142) & (143) & (243) \end{array}$$

- (d) Lad  $K$  være en egentlig normal undergruppe af  $S_4$ , som indeholder en 3-cykel, lad os kalde den  $(abc)$ . Lad  $\sigma$  være permutationen givet ved  $\sigma(a) = i$ ,  $\sigma(b) = j$  og  $\sigma(c) = k$ ; da  $K$  er normal vil  $\sigma(abc)\sigma^{-1} = (\sigma(a)\sigma(b)\sigma(c)) = (ijk)$  tilhøre  $K$  (her har jeg brugt lemma 2.8.7 til at "konjugere ind"). Ved passende valg af  $i, j, k$  ser man at  $K$  derved må indeholde alle 3-cykler. Desuden må  $K$  indeholde identiteten  $e$ , og derfor er  $|K| \geq 9$ . Da  $|K| \mid |S_4| = 4! = 24$ , og  $K \subsetneq S_4$ , må vi så have at  $|K| = 12$ . De sidste 3 elementer i  $K$  må være  $\tau_1, \tau_2$  og  $\tau_3$ , hvilket fx kan indses ved at  $(123)(234) = (12)(34)\tau_1$  og tilsvarende kan man kombinere sig frem til de andre  $\tau$ 'er. Da  $e, \tau_i$  og 3-cyklerne netop er de lige permutationer i  $S_4$  vil en ægte normal undergruppe af  $S_4$  indeholdende en 3-cykel nødvendigvis være  $A_4$ .

#### Opgave 4

Lad  $R$  betegne ringen  $\mathbb{Q}[X, Y, S, T]$ , og lad  $\leq$  være den leksikografiske ordning på  $R$  givet ved

$$X \geq Y \geq S \geq T.$$

Lad desuden  $I$  betegne idealet  $\langle S - X^2, T - XY \rangle$ .

- (a) Overalt i det følgende betegner en understreget term, at det er initialtermen med hensyn til  $\leq$ . For at finde den reducerede Gröbnerbasis for  $I$  benyttes Buchbergers  $\mathcal{S}$ -kriterium først til at afgøre, hvorvidt  $F_1 = (S - X^2, T - XY)$  er en Gröbnerbasis. Man får

$$\mathcal{S}(S - \underline{X^2}, T - \underline{XY}) = Y(S - X^2) - X(T - XY) = YS - \underline{XT}$$

og man indser let, at da ingen af initialtermene i  $F_1$  går op i nogen af termene i  $\mathcal{S}$ -polynomiet, vil man ikke få 0 som rest når man dividerer med  $F_1$ . Lad derfor nu  $F_2 = (S - X^2, T - XY, YS - XT)$ . Nu beregnes

$$\mathcal{S}(S - \underline{X^2}, YS - \underline{XT}) = T(S - X^2) - X(YS - XT) = TS - \underline{XYS} \quad (1)$$

$$\mathcal{S}(T - \underline{XY}, YS - \underline{XT}) = T(T - XY) - Y(YS - XT) = T^2 - \underline{Y^2S} \quad (2)$$

Man ser let, at det første af disse polynomier er det andet polynomium i  $F_2$  ganget med  $S$ , så man får rest 0 ved division af (1) med  $F_2$ . Som i tilfældet ovenfor ser man desuden, at der om  $\mathcal{S}$ -polynomiet i (2) gælder,

at initialtermen ikke er divisibel med nogen initialterm i  $F_2$ , så lad nu  $F_3 = (S - X^2, T - XY, YS - XT, T^2 - Y^2S)$ . Nu beregnes så

$$\begin{aligned} \mathcal{S}(S - \underline{X^2}, T^2 - \underline{Y^2S}) &= Y^2S(S - X^2) - X^2(T^2 - Y^2S) = Y^2S^2 - \underline{X^2T^2} \\ \mathcal{S}(T - \underline{XY}, T^2 - \underline{Y^2S}) &= YS(T - XY) - X(T^2 - Y^2S) = YST - \underline{XT^2} \\ \mathcal{S}(YS - \underline{XT}, T^2 - \underline{Y^2S}) &= Y^2S(YS - XT) - XT(T^2 - Y^2S) = Y^3S^2 - \underline{XT^3} \end{aligned}$$

Nu divideres hver af disse med  $F_3$ :

$$\begin{array}{l} \underline{-X^2T^2} + Y^2S^2 \quad : \quad (S - X^2, T - XY, YS - XT, T^2 - Y^2S) \\ \underline{-X^2T^2 + T^2S} \\ Y^2S^2 - T^2S \\ \underline{Y^2S^2 - ST^2} \\ 0 \end{array}$$

$$\begin{array}{l} \underline{-XT^2} + YST \quad : \quad (S - X^2, T - XY, YS - XT, T^2 - Y^2S) \\ \underline{-XT^2 + TYS} \\ 0 \end{array}$$

$$\begin{array}{l} \underline{-XT^3} + Y^3S^2 \quad : \quad (S - X^2, T - XY, YS - XT, T^2 - Y^2S) \\ \underline{-XT^3 + T^2YS} \\ Y^3S^2 - T^2YS \\ \underline{Y^3S^2 - YST^2} \\ 0 \end{array}$$

Da divisionen således i alle tilfælde giver rest 0 (og de øvrige  $\mathcal{S}$ -polynomier der kan dannes ud fra polynomierne i  $F_3$  oplagt giver rest 0), giver Buchbergers  $\mathcal{S}$ -kriterium nu, at  $F_3$  er en Gröbnerbasis (for  $\langle F_3 \rangle = I$ ). Det ses desuden let, at  $F_3$  er minimal, da ingen af initialtermene  $-X^2$ ,  $-XY$ ,  $-XT$  og  $-Y^2S$  går op i hverandre. Det eneste der adskiller  $F_3$  fra at være reduceret (initialtermene går heller ikke op i nogen af de andre termer i de andre polynomier), er at koefficienterne til initialtermene ikke er 1; da  $\mathbb{Q}$  er et legeme kan det dog naturligvis skaffes ved passende skalering (i dette tilfælde at alle polynomier skal ganges igennem med  $-1$ ), og man ser således at den reducerede Gröbnerbasis for  $I$  er

$$G = (X^2 - S, XY - T, XT - YS, Y^2S - T^2)$$

(b) Ved simpel udregning fås

$$\begin{array}{r}
 \underline{X^4 + 2X^3Y} \quad : \quad (X^2 - S, XY - T, XT - YS, Y^2S - T^2) \\
 \underline{X^4 - X^2S} \\
 2X^3Y + X^2S \\
 \underline{2X^3Y - 2XYS} \\
 X^2S + 2XYS \\
 \underline{X^2S - S^2} \\
 2XYS + S^2 \\
 \underline{2XYS - 2ST} \\
 S^2 + 2ST \quad \longrightarrow \quad \text{rest } Q
 \end{array}$$

Man ser jo let, at  $Q$  er et polynomium i  $S$  og  $T$ , og derfor at  $Q \in \mathbb{Q}[S, T]$ . Desuden ser man ved at indsætte  $S = X^2$  og  $T = XY$  at  $Q(X^2, XY) = X^4 + 2X^3Y$ .

(c) Lad  $f \in \mathbb{Q}[X, Y]$ , og antag at  $Q = f^G \in \mathbb{Q}[S, T]$ . Så giver teorem 5.5.1, at  $f$  er et polynomium i  $X^2$  og  $XY$ , og desuden at  $f = Q(X^2, XY)$ . [Man skal blot oversætte  $X^2$  med  $f_1$ ,  $XY$  med  $f_2$ , og desuden  $X$  med  $X_1$ ,  $Y$  med  $X_2$ ,  $S$  med  $T_1$  og endelig  $T$  med  $T_2$ ].

## Juni 2001

### Opgave 1

Lad  $R$  betegne polynomiumsringen  $\mathbb{F}_2[X]$ .

- (a) Der er i alt fire andegradspolynomier i  $R$ . Men  $X^2$  er reducibel thi  $X^2 = X \cdot X$  (0 er dobbeltrod),  $X^2 + 1$  faktoriseres som  $(X + 1)^2$  og  $X^2 + X = X(X + 1)$ . Tilbage er blot  $X^2 + X + 1$ , og da dette polynomium ingen rødder har (i  $\mathbb{F}_2$ ), og graden i øvrigt er 2 (proposition 4.6.3) er det irreducibelt (således det eneste af grad 2).
- (b) En tilsvarende analyse giver, at tredjegradspolynomier der har konstantled 0 har roden  $X = 0$ , og er derfor reducible. De irreducible må derfor skulle findes blandt polynomierne af formen  $X^3 + aX^2 + bX + 1$ , hvor  $a, b \in \mathbb{F}_2$ . Man ser dog, at hvis der er et lige antal termer i polynomiet, vil  $X = 1$  være en rod; således skal  $a$  være forskellig fra  $b$ . Nu lades således kun polynomierne  $X^3 + X^2 + 1$  og  $X^3 + X + 1$  tilbage som mulige irreducible tredjegradspolynomier, og da de ingen rødder har (og i øvrigt har grad 3; proposition 4.6.3 igen), er de irreducible; således de eneste af grad 3.
- (c) Et irreducibelt polynomium af grad 6 kan ikke have nogen rødder; som ovenfor skal vi derfor søge de irreducible polynomier blandt dem der har konstantled 1 og et ulige antal termer i alt. Nogle stykker kan dog udelukkes på forhånd, nemlig dem der kan dannes ved multiplikation af de ovenstående. Således beregnes

$$\begin{aligned}(X^3 + X^2 + 1)^2 &= X^6 + X^4 + 1 \\(X^3 + X + 1)^2 &= X^6 + X^2 + 1 \\(X^3 + X^2 + 1)(X^3 + X + 1) &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\(X^2 + X + 1)^3 &= X^6 + X^5 + X^3 + X + 1\end{aligned}$$

Således kan man fristes til at gætte på, at fx  $f = X^6 + X^5 + 1$  og  $g = X^6 + X + 1$  er irreducible sjettegradspolynomier. Man ser let, at ingen førstegradspolynomier går op i dem, thi de har ingen rødder. Tilsvarende indser man, at hvis et anden- eller tredjegradspolynomium går op, må det være et irreducibelt ét (thi for anden- og tredjegradspolynomier er det der skiller fårene fra bukkene jo netop om de har rødder eller ej; hvis et reducibelt anden- eller tredjegradspolynomium gik op, ville det behandlede sjettegradspolynomium have en rod). Det lette tilfælde at udelukke er tredjegradspolynomierne, thi de eneste tre sjettegradspolynomier som har irreducible tredjegradspolynomier som faktorer er listet ovenfor, og de påståede irreducible sjettegradspolynomier  $f$  og  $g$  optræder jo netop ikke blandt dem. Ved polynomiers division konstaterer man, at  $f = (X^2 + X + 1)(X^4 + X^2 + X) + X + 1$ , så  $X^2 + X + 1 \nmid f$ , og  $g = (X^2 + X + 1)(X^4 + X^3 + X + 1) + X$ , så  $X^2 + X + 1 \nmid g$ . Således er  $f$  og  $g$  irreducible (ingen polynomier af grad 1, 2 eller 3 går op).

- (d) Ifølge bemærkning 4.6.7 og den foregående proposition er såvel  $R/\langle f \rangle$  som  $R/\langle g \rangle$  legemer med  $2^6 = 64$  elementer. Ifølge teorem 4.7.1 er to (endelige) legemer med det samme antal elementer (ring)isomorfe.

## Opgave 2

I det følgende vil ligningerne

$$\begin{aligned} 25x - 14y &= 37 \\ 12x + 41y &= 829 \end{aligned}$$

blive behandlet i ringene  $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ ,  $\mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$ ,  $\mathbb{Z}/5\mathbb{Z} = \mathbb{F}_5$  samt  $\mathbb{Z}$ .

- (a) I  $\mathbb{F}_2$  er ligningssystemet  $x \equiv 1$  og  $y \equiv 1$ . Det er ikke svært at løse... I  $\mathbb{F}_3$  bliver ligningssystemet  $x + y \equiv 1$ ,  $2y \equiv 1$ ; dvs.  $y \equiv -1$  og  $x \equiv 2$  er løsning. Endelig bliver ligningerne i  $\mathbb{F}_5$  til  $y \equiv 2$  og  $2x + y \equiv -1$ , hvilket har løsningen  $x \equiv 1$ .
- (b) Vi kan stille ovenstående løsninger op som kongruenssystemer i henholdsvis  $x$  og  $y$ :

$$\begin{array}{ll} x \equiv 1 \pmod{2} & y \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} & y \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{5} & y \equiv 2 \pmod{5} \end{array}$$

Da 2, 3 og 5 er indbyrdes primiske, siger den kinesiske restklassesætning at vi kan finde en entydig løsning til hvert af disse systemer af kongruenser modulo 30. Man finder at  $x \equiv 11 \pmod{30}$  og  $y \equiv 17 \pmod{30}$ . Hvis  $(x, y)$  er en løsning til det oprindelige ligningssystem skal  $x$  og  $y$  så i hvert fald opfylde disse kongruenser. Man kan så foranlediges til at prøve, om  $(11, 17)$  mon kunne være en løsning, og en lille udregning viser at det faktisk er tilfældet. Da determinanten for ligningssystemet er  $1193 \neq 0$  er løsningen entydig.

## Opgave 3

Lad  $R$  være en kommutativ ring, og  $I \subseteq J$  idealer i  $R$ .

- (a) Lad  $\varphi: R/I \rightarrow R/J$  være givet ved  $\varphi(x + I) = x + J$ . Det skal så vises, at  $\varphi$  er veldefineret. Lad  $[\cdot]_I$  og  $[\cdot]_J$  betegne sideklasser i henholdsvis  $R/I$  og  $R/J$ . Med denne notation bliver  $\varphi([x]_I) = [x]_J$ .

Hvis  $[x_1]_I = [x_2]_I$ , har vi at  $x_1 - x_2 \in I$ , og dermed også  $x_1 - x_2 \in J$ . Derfor er  $[x_1]_J = [x_2]_J$ , hvilket viser at  $\varphi([x]_I)$  er uafhængig af valget af repræsentant; således veldefineret.

At  $\varphi$  er surjektiv følger af, at hvis  $[x]_J$  er en sideklasse i  $R/J$ , vil

$$R/I \ni [x]_I \xrightarrow{\varphi} [x]_J.$$

Det er oplagt, at  $\varphi$  er en gruppehomomorfi fra  $(R/I, +)$  til  $(R/J, +)$ , thi

$$\varphi([x_1]_I + [x_2]_I) = \varphi([x_1 + x_2]_I) = [x_1 + x_2]_J = [x_1]_J + [x_2]_J = \varphi([x_1]_I) + \varphi([x_2]_I),$$

jf. definitionen af addition i kvotientgrupperne  $R/I$  og  $R/J$ . Helt tilsvarende har vi, at  $\varphi$  bevarer multiplikation; udregningen er helt identisk:

$$\varphi([x_1]_I [x_2]_I) = \varphi([x_1 x_2]_I) = [x_1 x_2]_J = [x_1]_J [x_2]_J = \varphi([x_1]_I) \varphi([x_2]_I)$$

Endelig er  $\varphi([1]_I) = [1]_J$ , og disse er netop de multiplikativt neutrale elementer i henholdsvis  $R/I$  og  $R/J$ . Altså har vi som ønsket at  $\varphi$  er en veldefineret, surjektiv ringhomomorfi fra  $R/I$  ind i  $R/J$ .

- (b) Lad  $R = \mathbb{Z}[i]$ , og  $0 \neq n \in \mathbb{Z}$ . Lad  $I$  være idealet  $\langle n \rangle \subseteq R$ . Det skal vises, at  $a + bi \in I \iff n \mid a \wedge n \mid b$ .

Lad derfor  $a + bi \in I$ . Så findes  $x, y \in \mathbb{Z}$  så at  $a + bi = n(x + yi) = nx + nyi$ . Altså må  $nx = a$  og  $ny = b$ , hvilket viser  $\Rightarrow$ .

Antag nu at  $n \mid a$  og  $n \mid b$ . Så har vi at der findes  $x, y \in \mathbb{Z}$  så  $nx = a$  og  $ny = b$ . Endelig ser man, at tallet  $a + bi = nx + nyi = n(x + yi) \in I$ . Dette viser  $\Leftarrow$ .

Betragt nu kvotientgruppen  $R/I$ ; det skal vises at dette er en endelig ring. Dette vil jeg vise ved at vise at  $R/I \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) = A_n$ . Definer derfor

$$\varphi: R/I \rightarrow A_n$$

ved

$$\varphi([a + bi]_I) = ([a], [b]),$$

hvor  $[\cdot]$  på højresiden betyder den sædvanlige restklasse modulo  $n$ . Nu er  $\varphi$

**veldefineret**, da  $[a + bi]_I = [a' + b'i]_I$  medfører, at  $(a - a') + (b - b')i \in I$ ; altså  $n \mid a - a'$  og  $n \mid b - b'$ ; så  $[a] = [a']$  og  $[b] = [b']$ .

**surjektiv**, da  $([a], [b])$  rammes af  $[a + bi]_I \in R/I$ .

**injektiv**, da  $([a], [b]) = ([a'], [b'])$  medfører at  $n \mid a - a'$  og  $n \mid b - b'$ , så  $(a - a') + (b - b')i \in I$ , og derfor  $[a + bi]_I = [a' + b'i]_I$ .

Nu skulle man jo egentlig også tjekke, at  $\varphi$  er lineær, men bijektiviteten er nok; thi den viser, at  $|R/I| = |A_n| = n^2$  (egentlig er injektivitet nok, fordi det viser at  $|R/I| \leq |A_n|$ ). Altså er  $R/I$  endelig.

- (c) Lad  $J \neq \{0\}$  være et ideal i  $R$ . Det skal vises, at  $A = J \cap \mathbb{Z}$  er et ideal i  $\mathbb{Z}$  og  $A \neq \{0\}$ .

For det første er det klart, at  $A$  ikke er tom, thi  $0 \in A$ . Desuden indeholder  $A$  andre elementer end dette, thi det er givet at  $J$  indeholder et element  $z \neq 0$ . Da  $J$  er et ideal, og  $\bar{z} \in R$  vil  $z\bar{z} = |z|^2 \in J$ ; dette er naturligvis et helt, positivt tal og ligger derfor i  $A$ .

Det er nu trivielt at indse, at  $A$  er en undergruppe af  $(\mathbb{Z}, +)$ . Thi hvis  $x_1, x_2 \in A$  vil  $x_1 + x_2 \in J$  såvel som  $x_1 + x_2 \in \mathbb{Z}$ ; således  $x_1 + x_2 \in A$ . Det er allerede vist at  $0 \in A$ , og det er klart at hvis  $x \in A$  vil også  $-x \in A$ . Enhver undergruppe i  $\mathbb{Z}$  er et ideal i  $\mathbb{Z}$ , thi hvis  $x \in A$  og  $y \in \mathbb{Z}$ , vil  $yx \in A$ .

- (d) Det er i (b) vist, at  $R/I$  er en endelig ring, og i (a) blev det vist, at  $\varphi$  var en surjektiv afbildning fra  $R/I$  ind i  $R/J$ . Derfor må  $R/J$  være endelig (der kan højst være  $|R/I|$  elementer i  $R/J$ ).

### Opgave 4

Lad  $c = (c_1, c_2) \in \mathbb{R}^2$  og lad  $\cdot$  betegne det normale skalarprodukt  $\mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ . Definer relationen  $R_c$  på  $\mathbb{N}^2$  ved

$$v_1 R_c v_2 \iff c \cdot v_1 \geq c \cdot v_2$$

hvor  $\geq$  på højresiden betegner den sædvanlige ordning på  $\mathbb{R}$ .

- (a) Det er klart at  $R_c$  er refleksiv, thi for ethvert  $v = (x, y) \in \mathbb{N}^2$  gælder at  $c \cdot v \geq c \cdot v$ , og dermed  $v R_c v$ .

Tilsvarende har vi, at hvis  $v_1 R_c v_2$  og  $v_2 R_c v_3$ , betyder det at  $c \cdot v_1 \geq c \cdot v_2$  og  $c \cdot v_2 \geq c \cdot v_3$ ; da  $\geq$  på  $\mathbb{R}$  er transitiv betyder det at  $c \cdot v_1 \geq c \cdot v_3$ , og dermed pr. definition at  $v_1 R_c v_3$ .

- (b) Hvis  $c = (1, 0)$  har vi at fx  $(5, 2) R_c (5, 4)$ , idet  $5 \geq 5$ , men samtidig at  $(5, 4) R_c (5, 2)$ , igen fordi  $5 \geq 5$ ; men da  $(5, 2) \neq (5, 4)$  er  $R_c$  ikke antisymmetrisk.

- (c) Antag at  $c_2 \neq 0$ ,  $c_1/c_2 \notin \mathbb{Q}$  og at  $v_1 R_c v_2$  og  $v_2 R_c v_1$ . Så har vi at  $x_1 c_1 + y_1 c_2 = x_2 c_1 + y_2 c_2$  (da der både gælder  $\geq$  og  $\leq$  mellem de to sider). Ved at flytte lidt rundt får man

$$\frac{c_1}{c_2}(x_1 - x_2) = y_2 - y_1$$

Hvis  $x_1 \neq x_2$ , er  $x_1 - x_2 \neq 0$ , og dermed er

$$\frac{c_1}{c_2} = \frac{y_2 - y_1}{x_1 - x_2} \in \mathbb{Q}$$

i modstrid med antagelsen. Altså må  $x_1 = x_2$ , og så må der også gælde  $y_1 = y_2$ . Altså er  $R_c$  antisymmetrisk.

- (d) Lad  $c = (1, \sqrt{2})$ . Så er  $R_c$  en termordning på  $\mathbb{N}^2$  fordi  $R_c$  er en partiel ordning (den er refleksiv, transitiv og da  $1/\sqrt{2} \notin \mathbb{Q}$  også antisymmetrisk), og desuden

- (i)  $R_c$  er en totalordning, da  $\geq$  er en totalordning på  $\mathbb{R}$ , så der vil altid gælde  $c \cdot v_1 \geq c \cdot v_2$  eller  $c \cdot v_2 \geq c \cdot v_1$  (og i tilfælde af at begge gælder vil der gælde lighed mellem  $v_1$  og  $v_2$  jf. (c)).

- (ii)  $v R_c 0$  for alle  $v \in \mathbb{N}^2$ , da  $x + y\sqrt{2} \geq 0$  for alle  $(x, y) \in \mathbb{N}^2$ .
- (iii) Hvis  $x_1 + y_1\sqrt{2} \geq x_2 + y_2\sqrt{2}$ , vil der oplagt også gælde at  $x_1 + x + y_1\sqrt{2} + y\sqrt{2} \geq x_2 + x + y_2\sqrt{2} + y\sqrt{2}$ , og da skalarprodukt er distributiv over vektoraddition, har vi at  $c \cdot (v_1 + v) \geq c \cdot (v_2 + v)$ ; således er  $v_1 + v R_c v_2 + v$ .

Lad nu  $F_1 = (X^2 + Y, X^2Y + 1)$ , og lad  $I = \langle X^2 + Y, X^2Y + 1 \rangle$ . Vi ønsker at finde den reducerede Gröbnerbasis for  $I$  mht. termordningen  $R_c$ , hvor  $c = (1, \sqrt{2})$ . Første trin er at udregne (understregning markerer initialterm mht.  $R_c$ )

$$\mathcal{S}(\underline{X^2} + Y, \underline{X^2Y} + 1) = Y(X^2 + Y) - (X^2Y + 1) = \underline{Y^2} - 1$$

Da denne ikke er divisibel med nogen af initialtermene i  $F_1$  sættes  $F_2 = (X^2 + Y, X^2Y + 1, Y^2 - 1)$ . Nu udregnes så

$$\begin{aligned} \mathcal{S}(\underline{X^2} + Y, \underline{Y^2} - 1) &= Y^2(X^2 + Y) - X^2(Y^2 - 1) = \underline{Y^3} + X^2 \\ \mathcal{S}(\underline{X^2Y} + 1, \underline{Y^2} - 1) &= Y(X^2Y + 1) - X^2(Y^2 - 1) = \underline{X^2} + Y \end{aligned}$$

Division af den først af disse med  $F_2$  giver

$$\begin{array}{r} \underline{Y^3} + X^2 \quad : \quad (X^2 + Y, X^2Y + 1, Y^2 - 1) \\ \underline{Y^3 - Y} \\ \underline{X^2} + Y \\ \underline{X^2 + Y} \\ 0 \end{array}$$

og resten ved division af det andet  $\mathcal{S}$ -polynomim med  $F_2$  giver trivielt 0. Jf. Buchbergers  $\mathcal{S}$ -kriterium er  $F_2$  således en Gröbnerbasis. Den er dog ikke minimal, da initialtermen  $X^2$  går op i initialtermen  $X^2Y$ . Udelades polynomiet med initialterm  $X^2Y$  kan vi sætte  $F_3 = (X^2 + Y, Y^2 - 1)$ , og dette er en minimal basis da initialtermene ikke går op i hverandre, og koefficienterne til initialtermene er 1. Man ser desuden at det er den reducerede basis, da initialtermene heller ikke går op i andre termer.

- (e) Lad  $\leq$  være den leksikografiske termordning på  $\mathbb{N}^2$  med  $(1, 0) \geq (0, 1)$ . Antag at  $\geq = R_c$  for et passende  $c \in \mathbb{R}^2$ . Da  $(1, 0) \geq (0, x)$  for alle  $x \in \mathbb{N}$ , er  $c_1 \geq xc_2$  for alle  $x \in \mathbb{N}$ . Men dette kan kun lade sig gøre, hvis  $c_1 \geq 0$  og  $c_2 \leq 0$ . Som eksemplet fra (b) viser, kan  $R_c$  ikke være antisymmetrisk hvis  $c_1$  eller  $c_2$  er 0; altså er  $c_2 < 0$ . Men da der i den leksikografiske ordning gælder, at  $(0, 0) < (0, 1)$ , mens der for  $R_c$  nu åbenbart gælder, at  $(0, 0)R_c(0, 1)$  (da  $0 > c_2$ ) kan vi ikke have at  $\leq_{\text{lex}} = R_c$ .

## Januar 2002

### Opgave 1

Lad som sædvanlig  $\mathbb{F}_2$  betegne  $\mathbb{Z}/2\mathbb{Z}$ , og lad  $R$  betegne  $\mathbb{F}_2[X]$ .

- (a) Vi har, at der (i en vilkårlig polynomiumsring) gælder, at 1 er rod i  $X^7 - 1$ , hvorfor der altid vil gælde  $X - 1 \mid X^7 - 1$ . Faktoriseringen  $X^7 - 1 = (X - 1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)$  er også altid gyldig. Det søgte  $f$  er derfor  $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ .

Proposition 4.6.6 giver så, at  $R/\langle f \rangle$  er en ring med  $2^6 = 64$  elementer.

- (b) Et irreducibelt polynomium af grad  $\geq 2$  kan ikke have nogen rødder. Derfor må konstantleddet være 1 (hvis det var 0 ville 0 være rod i polynomiet). Irreducible tredjegradspolynomier skal således søges blandt polynomierne på formen  $X^3 + aX^2 + bX + 1$ , hvor  $a, b \in \mathbb{F}_2$ . Der må desuden gælde, at der skal være et ulige antal termer i alt, thi hvis antallet af termer er lige er 1 rod i polynomiet. Således er der kun de to muligheder  $g_1 = X^3 + X^2 + 1$  og  $g_2 = X^3 + X + 1$  som kandidater til irreducible tredjegradspolynomier. Da de ingen rødder har i  $\mathbb{F}_2$  er de pr. proposition 4.6.3 irreducible.

Ved at gange  $g_1$  og  $g_2$  sammen på de tre forskellige måder det nu kan gøres, finder man at

$$f = g_1 g_2 = (X^3 + X^2 + 1)(X^3 + X + 1)$$

- (c) Lad  $\alpha = [X] \in R/\langle f \rangle$ . Et legeme er karakteriseret ved, at alt hvad der ikke er 0 er enheder. Men da  $\alpha^3 + \alpha + 1 \in R/\langle f \rangle$  er en nuldivisor ( $\alpha^6 + \dots + \alpha + 1 = [0]$ ) kan det ikke være en enhed, og dermed er kvotientringen ikke et legeme.

### Opgave 2

Det skal vises, at  $X^2Z + Y$  ikke ligger i idealet  $I = \langle XZ + Y^2, X + Y \rangle \subseteq \mathbb{Q}[X, Y, Z]$ .

Til det formål kan vi jo prøve at finde en Gröbnerbasis for  $I$ . Lad  $\leq$  være den leksikografiske ordning med  $X \geq Y \geq Z$ . Nu er (understregning betegner som sædvanlig initialterm med hensyn til den valgte termordning):

$$\mathcal{S}(\underline{XZ} + Y^2, \underline{X} + Y) = XZ + Y^2 - Z(X + Y) = \underline{Y^2} - ZY$$

og man ser at ingen af initialtermene  $XZ$  og  $X$  går op i  $Y^2$ . Betragt derfor  $F_2 = (XZ + Y^2, X + Y, Y^2 - ZY)$ , og beregn

$$\mathcal{S}(\underline{XZ} + Y^2, \underline{Y^2} - ZY) = Y^2(XZ + Y^2) - XZ(Y^2 - ZY) = \underline{XYZ^2} + Y^4$$

$$\mathcal{S}(\underline{X} + Y, \underline{Y^2} - ZY) = Y^2(X + Y) - X(Y^2 - ZY) = \underline{XYZ} + Y^3$$

Ved at dividere hver af disse med  $F_2$  får man

$$\begin{array}{l} \underline{XYZ^2 + Y^4} \quad : \quad (XZ + Y^2, X + Y, Y^2 - ZY) \\ \underline{XYZ^2 + Y^3Z} \\ Y^4 - Y^3Z \\ \underline{Y^4 - Y^3Z} \\ 0 \end{array}$$

og

$$\begin{array}{l} \underline{XYZ + Y^3} \quad : \quad (XZ + Y^2, X + Y, Y^2 - ZY) \\ \underline{XYZ + Y^3} \\ 0 \end{array}$$

Da man således får 0 som rest ved division af hvert af  $\mathcal{S}$ -polynomierne ved division med  $F_2$ , er  $F_2$  jf. Buchbergers  $\mathcal{S}$ -kriterium en Gröbnerbasis. Vi kan derfor bruge proposition 5.4.3 til at afgøre hvorvidt  $X^2Z + Y$  ligger i  $I$  eller ej. Division giver

$$\begin{array}{l} \underline{X^2Z + Y} \quad : \quad (XZ + Y^2, X + Y, Y^2 - ZY) \\ \underline{X^2Z + XY^2} \\ -XY^2 + Y \\ \underline{-XY^2 - Y^3} \\ Y^3 + Y \\ \underline{Y^3 - ZY^2} \\ ZY^2 + Y \\ \underline{ZY^2 - Z^2Y} \\ Z^2Y + Y \quad \longrightarrow \quad \text{rest} \end{array}$$

Man ser således, at man ikke får 0 som rest, og derfor ligger  $X^2Z + Y$  ikke i  $I$ .

### Opgave 3

(a) Vi har at  $\text{sgn}: S_4 \rightarrow (\{\pm 1\}, \cdot)$  er en gruppehomomorfi, og derfor er

$$\begin{aligned} \text{sgn}(\tau\sigma\tau^{-1}) &= \text{sgn}(\tau) \text{sgn}(\sigma) \text{sgn}(\tau^{-1}) = \text{sgn}(\tau) \text{sgn}(\tau^{-1}) \text{sgn}(\sigma) \\ &= \text{sgn}(\tau\tau^{-1}) \text{sgn}(\sigma) = \text{sgn}(\text{Id}) \text{sgn}(\sigma) \\ &= 1 \text{sgn}(\sigma) = \text{sgn}(\sigma), \end{aligned}$$

da jo en gruppehomomorfi sender neutralelementet i neutralelementet (og  $(\{\pm 1\}, \cdot)$  er abelsk).

- (b) Man ser let at  $(123) = (12)(23)$ . Hvis  $\sigma = (abc)$  er en vilkårlig 3-cykel i  $S_4$ , lad  $\tau$  betegne permutationen i  $S_4$  givet ved at  $\tau(a) = 1$ ,  $\tau(b) = 2$  og  $\tau(c) = 3$ ; så har vi fra lemma 2.8.7 at  $\tau\sigma\tau^{-1} = \tau(abc)\tau^{-1} = (\tau(a)\tau(b)\tau(c)) = (123)$ . Vi har at

$$(123) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

og man ser herved, at  $I_{(123)} = \{(1, 3), (2, 3)\}$  og dermed  $n((123)) = |I_{(123)}| = 2$ . Altså er  $\text{sgn}((123)) = (-1)^2 = 1$ , jf. (a) og det ovenstående er  $\text{sgn}(\sigma) = 1$  for alle 3-cykler  $\sigma \in S_4$ , så alle 3-cykler er lige. 3-cyklen  $(abc)$  har orden 3, hvilket kan ses ved at  $(abc)^2 = (abc)(abc) = (acb)$  og  $(abc)^3 = (abc)(acb)^2 = (a)(b)(c) = \text{Id}$  (uanset om man betragter 3-cyklen som element i  $S_4$  eller  $A_4$ ).

- (c) Der er i alt 8 3-cykler i  $A_4$ , da en 3-cykel er givet ved hvilket af de fire elementer der ikke flyttes, og så hvilken "vej" de tre andre permuteres (der er to muligheder). Hvis en undergruppe af  $A_4$  indeholder alle 3-cyklerne, er der altså strengt flere end 6 elementer i den, og da en undergruppes orden er divisor i gruppens orden, og  $|A_4| = 4!/2 = 12$ , må undergruppens orden være 12, således er undergruppen  $A_4$  selv.
- (d) Lad  $\varphi: A_4 \rightarrow \mathbb{Z}/2\mathbb{Z}$  være en gruppehomomorfi. Lad  $\sigma$  være en 3-cykel. Så har vi at  $\varphi(\sigma^3) = \varphi(\text{Id}) = [0]$ , da en gruppehomomorfi sender neutralelement i neutralelement. Men da en gruppehomomorfi desuden bevarer komposition, er også  $\varphi(\sigma) + \varphi(\sigma) + \varphi(\sigma) = [0]$ , og så kan  $\varphi(\sigma)$  ikke være  $[1]$ . Altså er  $\varphi(\sigma) = [0] = 0 + 2\mathbb{Z}$ . Da vi desuden ved at kernen af en homomorfi er en undergruppe, og samtlige 3-cykler ligger i  $\ker \varphi$ , giver (c) at  $\ker \varphi = A_4$  så  $\varphi(\sigma) = [0]$  for ethvert  $\sigma \in A_4$ .
- (e) Hvis  $K$  er en undergruppe af orden 6, har den index 2 i  $A_4$ , og er dermed normal. Vi kan derfor danne kvotientgruppen  $A_4/K$  (korollar 2.3.3), og antallet af elementer er 2. Lad derfor  $A_4/K = \{[e], [\sigma]\}$ . Det er oplagt, at  $A_4/K$  er gruppeisomorf med  $\mathbb{Z}/2\mathbb{Z}$ , og lad  $\tilde{f}: A_4/K \rightarrow \mathbb{Z}/2\mathbb{Z}$  være en isomorfi ( $\tilde{f}([e]) = [0]$  og  $\tilde{f}([\sigma]) = [1]$ ). Lad desuden  $\pi: A_4 \rightarrow A_4/K$  betegne den kanoniske homomorfi. Definer nu  $\varphi: A_4 \rightarrow \mathbb{Z}/2\mathbb{Z}$  ved  $\varphi = \tilde{f} \circ \pi$ . Så er  $\varphi$  oplagt en homomorfi, og  $\varphi(\sigma) = \tilde{f}([\sigma]) = [1]$  i modstrid med at enhver homomorfi fra  $A_4$  ind i  $\mathbb{Z}/2\mathbb{Z}$  sender alt i  $[0]$ . Altså kan  $A_4$  ikke indeholde en undergruppe af orden 6.

#### Opgave 4

Lad  $p$  være et primtal  $\equiv 3 \pmod{4}$ .

- (a) Lad  $J$  være idealet  $\langle p \rangle \subseteq \mathbb{Z}[i]$ . Hvis  $c + di \in J$  betyder det, at der er  $a + bi \in \mathbb{Z}[i]$  så  $c + di = p(a + bi) = pa + pbi$ , hvorefter man ser at  $c = pa$  og  $d = pb$ ; altså  $p \mid c$  og  $p \mid d$ . Hvis omvendt  $p \mid c$  og  $p \mid d$  betyder det at der findes  $a, b \in \mathbb{Z}$  så  $c = pa$  og  $d = pb$ , og så ligger  $c + di = pa + pbi = p(a + bi)$  jo i  $J$ .

- (b) Lad  $[x] = x + J \in \mathbb{Z}[i]/J$ . Så har vi at  $[a + bi] = [c + di]$  hvis og kun hvis  $(a + bi) - (c + di) \in J$ , og dermed hvis og kun hvis  $(a - c) + (b - d)i \in J$ . Men jf. (a) gælder dette hvis og kun hvis  $p \mid a - c$  og  $p \mid b - d$ , som er ækvivalent med  $a \equiv c \pmod{p}$  og  $b \equiv d \pmod{p}$ .
- (c) Lad  $x = a + bi \in \mathbb{Z}[i]$  være givet. Lad nu  $a'$  henholdsvis  $b'$  betegne den ifølge proposition 1.2.1 entydigt bestemte rest der fremkommer ved division af  $a$  henholdsvis  $b$  med  $p$ . Så har vi i hvert fald, at  $0 \leq a', b' \leq p - 1$ . Desuden gælder, at  $a \equiv a' \pmod{p}$  og  $b \equiv b' \pmod{p}$ . Altså er  $[x'] = [a' + b'i] = [a + bi] = [x]$ .
- (d) Lad  $\pi$  være et primelement i  $\mathbb{Z}[i]$  så  $p = \pi x$  for et passende  $x \in \mathbb{Z}[i]$ . Defineres normfunktionen  $N: \mathbb{Z}[i] \rightarrow \mathbb{N}$  som sædvanlig ved  $N(a + bi) = a^2 + b^2$ , har vi regnereglen  $N(xy) = N(x)N(y)$ . Så har vi altså at

$$p^2 = N(\pi)N(x)$$

Da  $p$  er et primtal, er der kun få muligheder for hvad  $N(\pi)$  og  $N(x)$  kan være.

- $N(\pi) = N(x) = p$  kan nemt udelukkes, da en sum af to kvadrattal enten er kongruent med 0, 1 eller 2 modulo 4 (og aldrig 3, som  $p$  er).
  - $N(\pi) = 1$ ,  $N(x) = p^2$  kan heller ikke lade sig gøre, da  $N(\pi) = 1$  ville betyde at  $\pi$  var en enhed (og det er jo et primelement).
  - Tilbage er kun muligheden  $N(\pi) = p^2$  og  $N(x) = 1$ , og enhederne i  $\mathbb{Z}[i]$  er jo netop de elementer der har norm 1. Da  $\pi$  er et primelement, er  $\pi$  ganget med en enhed også et primelement; dermed er  $p$  et primelement.
- (e) Da  $\mathbb{Z}[i]$  er et PID, men ikke et legeme, kan vi bruge proposition 3.3.7 til at sige, at  $J = \langle p \rangle$  er et maksimalt ideal hvis og kun hvis  $p$  er irreducibel. Men da  $p$  er et primelement, er det irreducibelt (proposition 3.3.2), og dermed er  $J$  et maksimalt ideal. Så er kvotientringen  $\mathbb{Z}[i]/J$  et legeme jf. §3.2.3. Det er ret let at konstruere en bijektion mellem  $\mathbb{F}_p \times \mathbb{F}_p$  og  $\mathbb{Z}[i]/J$ ; lad nemlig  $f([a], [b]) = [a + bi]$ . Ved brug af (a), (b) og (c) er det ikke svært at kontrollere at det faktisk er en bijektion, og dermed må der være netop  $p^2$  elementer i  $\mathbb{Z}[i]/J$ .
- (f) Lad  $X \in \mathbb{Z}$ . Antag  $p$  går op i  $X^2 + 1$ . Dette kan faktorerises som  $(X + i)(X - i)$ , og da  $p$  er et primelement vil der så gælde, at  $p$  går op i  $X + i$  eller  $p$  går op i  $X - i$ . Men da  $p$  er et helt tal (primtal), kan det ikke gå op i imaginærdelene, og dermed kan  $p$  ikke gå op i  $X \pm i$ ; så  $p \nmid X^2 + 1$ .
- (g) Lad  $F = \mathbb{Z}/p\mathbb{Z}$  og lad  $I = \langle X^2 + 1 \rangle \subseteq F[X]$ . Fra (f) har vi, at  $X^2 + 1$  ikke har nogen rødder i  $F$ , da jo  $[0] = [p]$  og  $p$  ej går op i  $X^2 + 1$ . Polynomiet er således irreducibelt (proposition 4.6.3), og dermed er kvotientringen  $M = F[X]/I$  et legeme med  $|M|^{\deg(X^2+1)} = p^2$  elementer (proposition 4.6.6 og bemærkning 4.6.7). Da  $M$  og  $L$  således begge er legemer med det samme antal elementer, giver teorem 4.7.1 at de er (ring)isomorfe.

## Juni 2002

### Opgave 1

Lad  $R = \{a + b\sqrt{-11} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ .

- (a) Man indser nemt, at  $(R, +)$  er en additiv gruppe (man kan betragte den som  $\mathbb{Z}^2$ ) idet  $(a + b\sqrt{-11}) + (c + d\sqrt{-11}) = (a + c) + (b + d)\sqrt{-11} \in R$ ,  $0 = 0 + 0\sqrt{-11}$  er neutralt element ved addition, og  $-a - b\sqrt{-11}$  er additivt invers til  $a + b\sqrt{-11}$ ; og da addition i  $\mathbb{Z}$  er kommutativ bliver  $(R, +)$  selvfølgelig abelsk.

Multiplikation defineres som multiplikation i  $\mathbb{C}$ , og det er derfor klart at denne bliver associativ og distributiv over addition. 1-element er  $1 = 1 + 0\sqrt{-11}$ . Det eneste der skal kontrolleres er at  $R$  faktisk er lukket under multiplikation:

$$\begin{aligned} (a + b\sqrt{-11})(c + d\sqrt{-11}) &= ac + ad\sqrt{-11} + bc\sqrt{-11} - 11bd \\ &= ac - 11bd + (ad + bc)\sqrt{-11}, \end{aligned}$$

og man ser at dette igen er et element i  $R$ .

- (b) Lad  $N: R \rightarrow \mathbb{N}$  være givet ved  $N(x + y\sqrt{-11}) = x^2 + 11y^2$ . Så er  $N(1) = 1^2 + 0^2 = 1$  og

$$\begin{aligned} N(ab) &= N((x + y\sqrt{-11})(x' + y'\sqrt{-11})) \\ &= N(xx' - 11yy' + (xy' + x'y)\sqrt{-11}) \\ &= (xx' - 11yy')^2 + 11(xy' + x'y)^2 \\ &= x^2x'^2 + 121y^2y'^2 - 22xx'yy' + 11x^2y'^2 + 11x'^2y^2 + 22xy'x'y \\ &= x^2x'^2 + 121y^2y'^2 + 11x^2y'^2 + 11x'^2y^2 \\ &= (x^2 + 11y^2)(x'^2 + 11y'^2) \\ &= N(x + y\sqrt{-11})N(x' + y'\sqrt{-11}) \\ &= N(a)N(b) \end{aligned}$$

Hvis vi antager, at  $u = a + b\sqrt{-11}$  er en enhed i  $R$ , betyder det at der findes  $z = x + y\sqrt{-11} \in R$  så  $(a + b\sqrt{-11})(x + y\sqrt{-11}) = 1$ . Benyttes  $N$  på begge sider fås at så vil  $N(uz) = N(u)N(z) = (a^2 + 11b^2)(x^2 + 11y^2) = N(1) = 1$ . Heraf ser man let  $(a, b) \neq (0, 0)$ , og at  $b = y = 0$  (ellers ville en af faktorerne være  $\geq 11$ ). Så følger igen at  $a^2x^2 = 1$ , og da  $a, x \in \mathbb{Z}$  må vi have at  $ax = \pm 1$ , hvilket igen giver at  $a = \pm 1$ . Hvis  $u$  er en enhed, er den således enten 1 eller  $-1$  (dvs.  $R^* \subseteq \{\pm 1\}$ ). Omvendt ser man let, at både 1 og  $-1$  er enheder (de er begge deres egne multiplikativt inverse), så  $R^* = \{\pm 1\}$ .

- (c) Antag at  $3 = ab$  hvor  $a, b \in R$ . Igen benyttes  $N$  på begge sider af lighedstegnet, og man får at  $9 = N(a)N(b)$ . Da  $N(a), N(b) \in \mathbb{N}$  er der kun

mulighederne  $N(a) = N(b) = 3$  og  $N(a) = 1, N(b) = 9$  (bortset fra det symmetriske tilfælde). Men da  $N(a) = x^2 + 11y^2$  kan  $N(a)$  aldrig blive 3 (det ville kræve  $y = 0$ , og 3 er ikke et kvadrattal). Altså er  $N(a) = 1$ , og det følger af det (b) at det betyder, at  $a$  må være en enhed. Således er 3 irreducibel.

Hvis 3 går op i  $1 \pm \sqrt{-11}$ , vil der findes  $x, y \in \mathbb{Z}$  så  $3x \pm 3y\sqrt{-11} = 1 \pm \sqrt{-11}$ ; men da  $3x = 1$  ikke kan lade sig gøre inden for  $\mathbb{Z}$  kan 3 ikke gå op i  $1 \pm \sqrt{-11}$  inden for  $R$ .

- (d) Vi har at  $12 = 3 \cdot 4 = (1 + \sqrt{-11})(1 - \sqrt{-11})$ , og derfor er  $R$  ikke et UFD (idet vi har to forskellige faktoriseringer af 12, og der findes en faktor i den ene som ikke går op i nogen af faktorerne i den anden). Da ethvert PID er et UFD (teorem 3.3.8), kan  $R$  ikke være et hovedidealområde.

## Opgave 2

Lad  $\sigma$  være permutationen

$$\sigma = (123)(34)(153) \in S_5$$

- (a) Man finder let, at  $\sigma$  kan skrives som produkt af disjunkte cykler ved  $\sigma = (154)(23)$ .
- (b) Da 2-cykler har orden 2 og 3-cykler har orden 3, og desuden at disjunkte cykler kommuterer, ser man at  $\sigma^{2n} = (154)^{2n}$  og  $\sigma^{3n} = (23)^{3n}$ . Heraf finder man nemt, at  $\sigma^6 = \text{Id}$ , og at 6 derfor må være  $\text{ord}(\sigma)$ .
- (c) Da  $\text{sgn}: S_5 \rightarrow \{\pm 1\}$  er en gruppehomomorfi, og fortegnet for en  $r$ -cykel er  $(-1)^{r-1}$ , får man at  $\text{sgn}(\sigma) = \text{sgn}((154)(23)) = \text{sgn}((154)) \text{sgn}((23)) = -1$ .
- (d) I  $S_5$  findes cykeltyperne
- $1 + 1 + 1 + 1 + 1$ , dvs. identiteten, der har orden 1
  - $1 + 1 + 1 + 2$ , som blot er 2-cykler, og derfor har orden 2
  - $1 + 1 + 3$ , dvs. 3-cykler, og de har orden 3
  - $1 + 4$ , 4-cykler, har orden 4
  - 5, 5-cykler har orden 5
  - $1 + 2 + 2$  er et produkt af to 2-cykler, og denne cykeltype har derfor orden 2
  - $2 + 3$  er den ovenfor behandlede cykeltype, og permutationer af denne cykeltype har orden 6.

Man ser således, at der ikke findes elementer i  $S_5$  af orden højere end 6.

### Opgave 3

Lad som sædvanlig  $\mathbb{F}_2$  betegne legemet  $\mathbb{Z}/2\mathbb{Z}$ , lad  $L$  betegne kvotientringen  $\mathbb{F}_2[X]/\langle X^2 + X + 1 \rangle$ , og lad  $\xi = [X] \in L$ .

- (a) Vi har at 1-elementet i  $\mathbb{F}_2[X]$  er det konstante polynomium 1; derfor bliver 1-elementet i  $L$  klassen hørende til 1, dvs.  $[1]$ . Da vi har, at  $[1] + [1] = [1 + 1] = [2] = [0]$  ser man, at  $\text{char } L = 2$  (da jo  $2 = 0$  i  $\mathbb{F}_2$ ). Men heraf følger  $[1] = [-1]$ , og dermed at  $a = [1]a = [-1]a = -a$ . Desuden har vi, at  $(a + b)^2 = (a + b)(a + b) = (a + b)a + (a + b)b = a^2 + ba + ab + b^2 = a^2 + 2ab + b^2 = a^2 + b^2$ , hvor jeg har udnyttet at  $L$  er en kommutativ ring ( $ab = ba$ ) samt den distributive lov.
- (b) Da  $X^2 + X + 1$  er irreducibel i  $\mathbb{F}_2[X]$  (det har ingen rødder, proposition 4.6.3), er  $L = \mathbb{F}_2[X]/\langle X^2 + X + 1 \rangle$  et legeme med  $2^2 = 4$  elementer. Da  $[X^2 + X + 1] = [0]$  i  $L$ , er de fire elementer i  $L$  netop  $[0], [1], \xi$  og  $[1] + \xi$  (hvor jeg for kortheds skyld vil skrive 1 for  $[1]$  og 0 for  $[0]$ ). Desuden er  $\xi^2 = -\xi - 1 = \xi + 1$ .
- (c) Lad  $P_a = X^2 + a \in L[X]$ , hvor  $a \in L$ . Vi har, at  $P_0$  er reducibel, da 0 er (dobbel)rod. Tilsvarende er 1 (dobbel)rod i  $P_1$ . En udregning viser, at  $P_\xi(1 + \xi) = (1 + \xi)^2 + \xi = 1 + \xi^2 + \xi = 0$ , og  $P_\xi$  er derfor reducibel. Endelig er  $P_{1+\xi}(\xi) = \xi^2 + 1 + \xi = 0$ , så denne er også reducibel.
- (d) Lad  $f = X^2 + \xi X + \xi \in L[X]$ . Ved udregning får man, at  $f(0) = \xi$ ,  $f(1) = 1 + \xi + \xi = 1$ ,  $f(\xi) = \xi^2 + \xi^2 + \xi = \xi$  og  $f(1 + \xi) = 1 + \xi^2 + \xi + \xi^2 + \xi = 1$ . Således har  $f$  ingen rødder i  $L$ , og da  $f$  desuden har grad 2 er  $f$  irreducibel. Derfor får man igen, at  $K = L[X]/\langle f \rangle$  er et legeme, og at det har  $4^2 = 16$  elementer.
- (e) Lad  $\eta = [X] \in K$ . Vi har at elementer i  $K$  entydigt kan skrives på formen  $a + b\eta$ , hvor  $a, b \in L$ , og da elementer i  $L$  kan skrives som  $c + d\xi$ , hvor  $c, d \in \mathbb{F}_2$  finder man, at  $K$  alt i alt kan opfattes som  $\{a + b\xi + c\eta + d\xi\eta \mid a, b, c, d \in \mathbb{F}_2\}$ . Vi har at  $\eta^2 = \eta\xi + \xi$ , og givet at  $\eta^4 = \eta + \xi$  får man at  $\eta^5 = \eta\eta^4 = \eta^2 + \eta\xi = \xi$ . Vi kan derfor hurtigt udelukke, at  $\eta^3$  skulle være 1, fordi så ville  $\eta^5 = \eta^2$ . Da således både  $\eta, \eta^3$  og  $\eta^5$  ikke er 1, og der er  $16 - 1 = 15$  elementer i  $(K^*, \cdot)$ , vil  $\text{ord}(\eta) = 15$  og dermed er  $\eta$  en frembringer for  $K^*$  (elementets orden går op i gruppens orden).

### Opgave 4

Lad  $f = XY + 1$  og  $g = X^2 + 1$  være polynomier i  $\mathbb{Q}[X, Y]$ , og lad  $\leq$  være en termordning på  $\mathbb{N}^2$ .

- (a) Da  $\leq$  er en termordning, er det en totalordning, og der gælder at  $(0, 0) \leq (a, b)$  for alle  $(a, b) \in \mathbb{N}^2$ . Da termen  $XY$  identificeres med  $(1, 1)$ ,  $X^2$  med  $(2, 0)$  og 1 med  $(0, 0)$ , har vi at der gælder  $XY \geq 1$  og  $X^2 \geq 1$ . Altså er  $\text{in}_{\leq}(f) = XY$  og  $\text{in}_{\leq}(g) = X^2$ .

- (b) Vi har at  $\mathcal{S}(\underline{XY} + 1, \underline{X^2} + 1) = X(XY + 1) - Y(X^2 + 1) = X - Y$ . Det er ikke umiddelbart til at sige, hvilken af disse termer der er initialtermen.
- (c) Vi har, at ingen af initialtermenerne i  $f$  og  $g$  går op i nogen af termene i  $\mathcal{S}(f, g)$ , og derfor får man  $X - Y$  selv som rest ved division af  $X - Y$  med  $(f, g)$ .
- (d) Buchbergers  $\mathcal{S}$ -kriterium giver, at  $(f, g)$  er en Gröbnerbasis for  $I = \langle f, g \rangle$  hvis og kun hvis  $(\mathcal{S}(f, g))^{(f, g)} = 0$ , og da denne rest er udregnet i (c) og ikke var 0, kan  $(f, g)$  ikke være en Gröbnerbasis for  $I$  med hensyn til  $\leq$ .