Emnerapport for MAUMAT644 2014 vår og 2015 vår
av Runar Ile

11/9 2015

Navn på emneansvarlig: Runar Ile (begge årene)

Hvilke styringsorgan har behandlet evalueringen/når: –

Referanse til eventuelle saksforelegg og saksprotokoller, oppsummering av innspill fra behandlingen: –

Vedlegg: FS-rapport emnestatistikk: Se vedlegg 1-4 (bør sammenlinges med MAT220, også vedlagt)

Innledning: Emnet gikk første gang våren 2011 og inngår i videreutdanningsmasteren «Master i undervisning med fordypning i matematikk» som går over 4 år (50%). MAUMAT644 ligger i andre semester av studiet. Emnet skal være en samlingsbasert versjon av det ordinære emnet MAT220.

Oppfølging av eventuelle tidligere evalueringer: Ikke aktuelt

Emnets læringsutbyttebeskrivelser:

Etter fullført emne skal studentene kunne (fra MAT220 – MAUMAT644-beskrivelsen er ikke oppdatert):

- *Forstå og utføre enklere bevisføring*
- *Gjengi definisjoner og begreper knyttet til grupper, ringer, kropper og homomorfier og isomorfier av disse, blant annet permutasjoner, gruppevirkninger, faktorgrupper og faktorringer, integritetsområder, kvotientkropper, polynomringer, idealer, primidealer, maksimalidealer og kroppsutvidelser.*
- *Utføre enkle beregninger knyttet til begrepene over, både i konkrete tilfeller og i mer abstrakte tilfeller.*
- *Beskrive hovedideene i bevis knyttet til begrepene over, slik som for eksempel umuligheten av vinkelens tredeling og kubens dobling.*

Faglærers vurdering av

- *Undervisningsformer*: Fordi studentene kommer fra hele landet er kurset samlingsbasert. Det er **fire samlinger á to dager** (torsdag og fredag), hver på 6 timer, se vedlegg 5. Vi har også gitt tilbud om eksamensforberedelser de to siste dagene før eksamen. I tillegg er det **fire obligatoriske innleveringer** som studenten får individuelle, detaljerte tilbakemeldinger på (se neste punkt). Det er tilsammen 4 x 2d x 6t/d = 48 timer med samling. Til sammenligning hadde det vanlige algebrakurset våren 2015 14,5 uker med 4 timer forelesninger i tillegg til 2 timer med regneøvelser (tilsammen 84 timer). Det er fordeler og ulemper med samlinger. En fordel er konsentrasjonen og at man kan (og bør) gjøre forelesningene mer studentaktiverende ved å gi oppgaver underveis som studentene løser før man går videre. En ufordel er de lange intervallene mellom samlingene og viser seg hvis studentene ikke har arbeidet nok med stoffet i mellomtiden – en utfordring med lærerjobb ved siden av (våren 2015 var flere delvis frikjøpt under den nye KFK-ordningen, i 2014 var det ingen under 100% stilling og flere over). Ellers er det påfallende få eposthenvendelser i periodene mellom samlingene. På direkte spørsmål bekrefter studentene at dette skyldes at de ikke syns de er i posisjon til å stille

spørsmål når de ikke har fått arbeidet med stoffet (og underforstått, når læreboken er lesverdig). De få spørsmålene som kommer er nesten alle knyttet til innleveringene. Dette antyder at innleveringene utgjør en vesentlig del av studentenes innsats i faget noe som også understøttes av studentenes kommentarer.

- *Vurderingsformer*: Det er fem timer skriftlig eksamen ved semsterslutt (felles med MAT220) og fire obligatoriske oppgaver som gis i forbindelse med de fire samlingene. **De obligatoriske innleveringsoppgavene** er omfattende (20-30 siders besvarelser er ikke uvanlig selv om det kan gjøres kortere) og utgjør i praksis en vesentlig del av studentenes arbeid med faget. De må bestås for å få gå opp til eksamen. Beståttgrensen er på 60%. Det er kanskje en student (av 7-8) som ikke får godkjent i første forsøk per innlevering, men det er gjerne noen flere som er i grenseland. At det er frister for dette fordelt utover semesteret opplever studentene som hjelp til å få arbeidet nok, over lengre tid, med dette modningsemnet. Emneansvarlig legger betydelig innsats i å gi ganske omfattende **individuelle tilbakemeldinger** (LaTeX) på oppgavene kort tid (normalt 2-3 dager) etter innleveringsfristen. Se vedlegg 6 for et eks. Det er uklart om utbyttet står i forhold til innsatsen, men dette er ment å være en kompensasjon for begrenset tid til fellesundervisningen og lang avstand til foreleser. Hovedinntrykket er at studentene gjør en betydelig innsats med innleveringsoppgavene. Emneansvarlig har de to siste årene forsøkt å utvikle **eksamensoppgavene** noe slik at de skal dekke større deler av pensum. Se vedlegg 7-10. Dette betyr bl.a. at de kanskje vil variere noe mer fra år til år og at graderingen av vanskelighetsgraden vil være jevnere (f. eks. færre veldig lette punkter og flere middels vanskelige). Et spørsmål er om vurderingsformen bør endres til også å omfatte et prosjekt el. Men da omfanget av det (nominelle) nåværende pensum er i største laget er ikke dette mulig uten å endre på innholdet i emnet.
- *Litteraturliste*: Se vedlegg 5. **Læreboken** (Fraleigh: A first course in abstract algebra, 7. int. utg.) har flere fordeler for dette emnet. Den er kan leses på egenhånd med mye tekst, eksempler og forklaringer og spesielt har den mange gode og varierte oppgaver. Dessverre har fasiten falt ut av den internasjonale utgaven, men ble kopiert opp og lagt ut. Et problem med læreboken er at den har unødvendig mange resultater og mange av disse kalles for teoremer. Dette gjør det krevende for studentene å avgjøre hva som er de viktig resultatene som de virkelig må kunne og hva som er hjelperesultater, eller bare varianter av resultater. Dette problemet forsterkes av at studentene har få timer med forelesninger. Emneansvarlig har derfor lagt ut **forelesningsnotater** (LaTeX). Se vedlegg 11 for et eks. (samling 4) som også gir et visst inntrykk av hva som blir gjort på en samling.

- **Studentstatistikk**
  - *Vurderings- og undervisningsmeldte*: 7/8 (2014) og 8/11 (2015) – se under for mer realistiske tall
  - *Strykprosent, frafall og karakterfordeling*:

    Våren 2014 startet 8 studenter på emnet. En av disse hoppet av halveis fordi hun hadde 120% stilling på skolen og skulle ta eksamen i diffensialligninger samme vår. Denne studentene fulgte emnet på nytt våren 2015. Diff.ligninger er en del av opptaksgrunnlaget, men det har vært gitt opptak under forutsetning av at emnet tas i løpet av det første året. Denne praksisen er nå strammet inn. 7 studenter tok eksamen og 5 bestod med karakterer: E, E, C,

B, A. Dette var sammenlingbart med resultatene i MAT220 (med 30 studenter på eksamen, to A-er, 7 stryk). En av dem som strøk tok ny eksamen høst 2014 og fikk D. Den andre som strøk fulgte emnet på nytt våren 2015 og fikk C. Dette eksemplifiserer at den nødvendige modningstiden for studentene varierer ganske mye.

Våren 2015 fulgte 9 studenter emnet (inkludert de to fra våren 2014 nevnt over). 8 tok eksamen (ett trekk pga sykdom) og alle bestod med karakterene: E, D, D, C, C, B, A, A. I MAT220 der det f. eks. 7 stryk, tre B og en A (33 tok eksamen). Se vedlegg for resultatfordeling.

- **Rammevilkår**
  - *Lokale og undervisningsutstyr*: Lokaler på VilVite brukes. Her er det ikke anledning til å gi studentene te/kaffe og forfriskninger og kantinen er dyr. Konferanserom D manger en stor tavle på frontveggen.
  - *Andre forhold*: Det kan være ønskelig å gi noen forlesninger/regninger via Adobe Connect og til dette trengs det teknisk utstyr og tidsressurser.

    Mer tid på samlingene hadde vært svært ønskelig, men er kanskje urealistisk.
- **Studentevalueringer**
  - *Metode – gjennomføring*: Kort spørreskjema utsendt og mottatt av studiekonsulent før sensur
  - *Studentenes vurderinger og tilbakemeldinger*: Se vedlegg 12 og 13. NB: Respons på MAUMAT643 Matematikkens historie II (5sp) er (litt forvirrende) også med i dette skjemaet.
  - *Faglærers kommentar*: Oppsummert virker studentene å være godt fornøyd med de praktiske rammene og med det faglige. Men det er (ikke overraskende) signaler om at dette emnet er krevende og at mer undervisning hadde vært ønskelig.
- **Andre merknader (for eksempel undervegstiltak)**: Ingen (se neste).

Faglærers samlede vurderinger med eventuelle forslag til endringer:

MAUMAT644 oppleves som det klart mest krevende emnet på dette masterstudiet. Det fungerer dermed som en «rundingsbøye»: Klarer man det ikke vil man ikke kunne starte på masteroppgavedelen av studiet (det er i tillegg et krav om snittkarakter C). De mateamtikkfaglige krevene i denne videreutdanningen er allikevel klart lavere enn kravene til et masterstudium i ren matematikk. Antagelig er det naturligere å sammenligne med kravene i lektorutdanningen – som har 80 sp matematikk før 8. semester og 30 sp i 8.-9. sem. rettet mot masterspesialiseringen. Opptak til studiet krever 60 sp matematikk på universitetsnivå (se vedlagte studieplan, vedlegg 14) *som dekker emnene MAT111, MAT112, MAT121 og deler av MAT131*. Dessuten innholder studiet «Diskret matematikk» 10 sp, «Matematikkens historie I+II» 10 sp og «Algebra» 10 sp. I tillegg kommer «Diffensialligninger II og didaktisk modellering» 15 sp – dette er et emne som både har matematikk- og matematikkdidaktisk innhold. Det siste emnet er et metodekurs (15 sp) som ikke innholder hverken matematikk eller matematikkdidaktikk. Denne rundingsbøyen er derfor antagelig et rimelig krav sett fra MIs side, men kan oppleves som krevende for mange av studentene.

Endringsforslag: Muligens kan noe fjernundervisning med Adobe Connect (videokonferanseutstyr) i periodene mellom samlingene virke kompenserende for

problemet med lange intervaller mellom samlingene, ikke minst for å styrke «lagånden», men dette byr på sine egne (bl. a. logistiske) utfordringer.

Pensum er per i dag litt for omfattende. Dette gjør at emnet fremstår for studentene som en stor samling begreper som de ikke får så dype erfaringer med. Dette er uheldig og gir lett en litt instrumentell innstilling til faget. Eksamensoppgavene kan som nevnt brukes til å motvirke noe av dette, og det er et langsiktig prosjekt. Et annet grep kunne være å gjøre en eller to av innleveringene om til miniprosjekter. Å trekke inn geometri i disse prosjektene, f. eks. gjennom isometrigruppen til planet, kan være en idé. Alternativt kunne man vurdere å endre kursets innhold, med større dybde og færre emner, og gjerne med større vekt på noen anvendelser og (geometriske) eksempler.

– Runar Ile

Vedlegg

1-4 Emnestatistikk for MAUMAT644 og MAT220 vår 2014 og vår 2015

5 Semesterplan

6 Eksempel på individuell tilbakemelding på innleveringsoppgave

7-10 Eksamensoppgave og løsningsforslag 2014v og 2015v

11 Eksempel på forelesningsnotater til en samling

12-13 Studenttilbakemeldinger 2014 og 2015

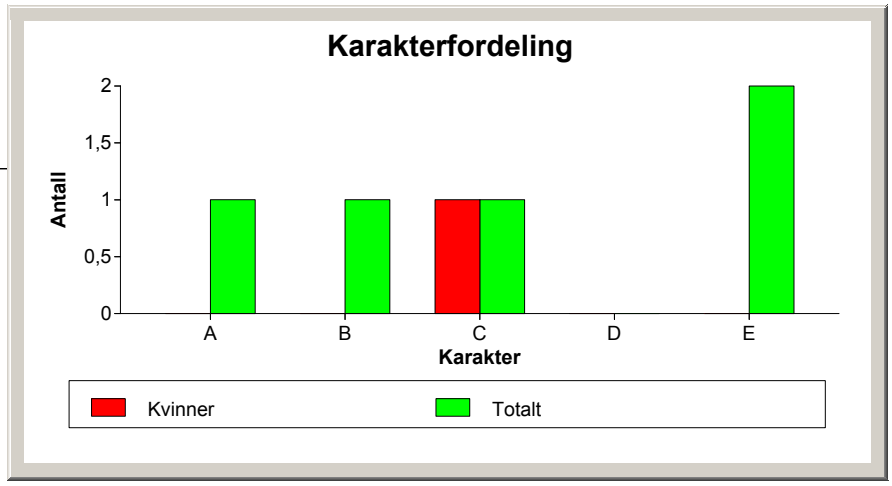
14 Studieplan for VID–MAUMAT

FS580.001 Resultatfordeling

Eksamen: MAUMAT644 0 S 2014 VÅR
Algebra - Skoleeksamen 10,0sp
Karakterregel: Beste: A, Bestått: E, Dårligste: F
-

	Totalt		Kvinner		Menn	
Antall kandidater (oppmeldt):	8		3		5	
Antall møtt til eksamen:	7		2		5	
Antall bestått (B):	5		1		4	
Antall stryk (S):	2	29%	1	50%	1	20%
Antall avbrutt (A):	0		0		0	
Gjennomsnittskarakter:	C		C		C	
Antall med legeattest (L):	0		0		0	
Antall trekk før eksamen (T):	0		0		0	

Karakter	Antall	Antall kvinner
E	2	0
D	0	0
C	1	1
B	1	0
A	1	0



FS580.001 Resultatfordeling

Eksamen: MAUMAT644 0 S 2015 VÅR

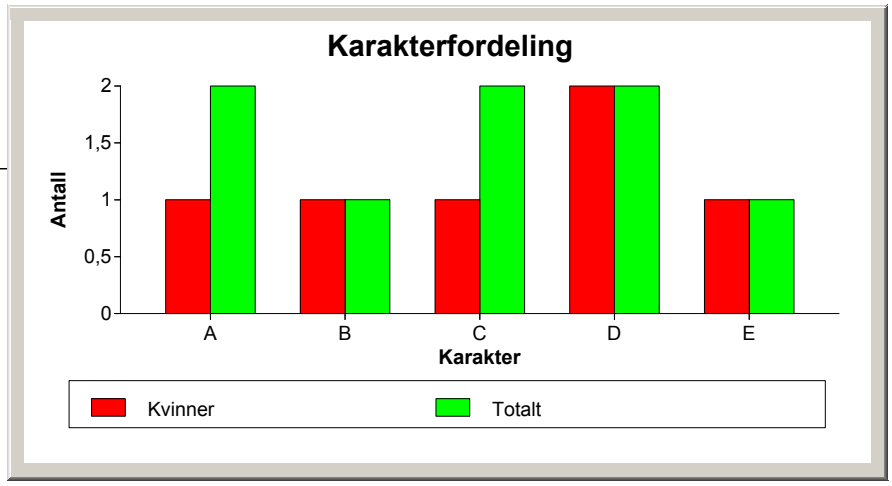
Algebra - Skoleeksamen 10,0sp

Karakterregel: Beste: A, Bestått: E, Dårligste: F

-

	Totalt		Kvinner		Menn	
Antall kandidater (oppmeldt):	11		7		4	
Antall møtt til eksamen:	8		6		2	
Antall bestått (B):	8		6		2	
Antall stryk (S):	0	0%	0	0%	0	0%
Antall avbrutt (A):	0		0		0	
Gjennomsnittskarakter:	C		C		B	
Antall med legeattest (L):	1		1		0	
Antall trekk før eksamen (T):	0		0		0	

Karakter	Antall	Antall kvinner
E	1	1
D	2	2
C	2	1
B	1	1
A	2	1



FS580.001 Resultatfordeling

Eksamen: MAT220 0 S 2014 VÅR

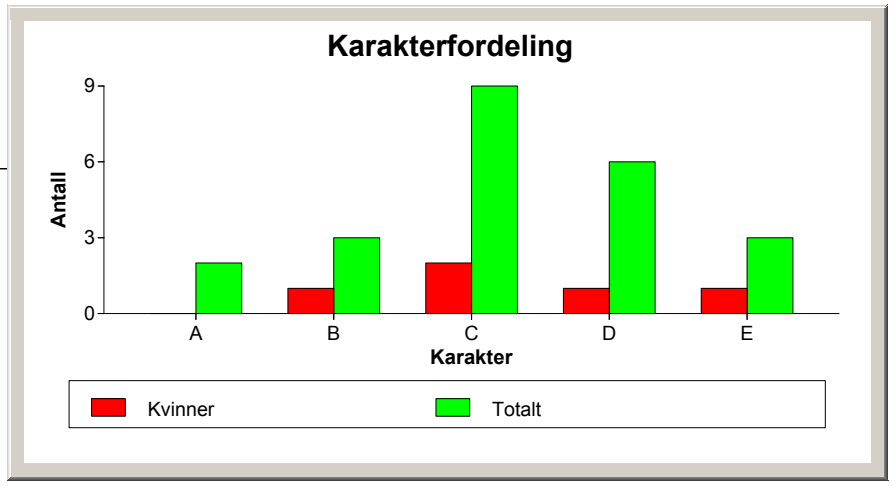
Algebra - Skoleeksamen 10,0sp

Karakterregel: Beste: A, Bestått: E, Dårligste: F

-

	Totalt		Kvinner		Menn	
Antall kandidater (oppmeldt):	44		8		36	
Antall møtt til eksamen:	30		8		22	
Antall bestått (B):	23		5		18	
Antall stryk (S):	7	23%	3	38%	4	18%
Antall avbrutt (A):	0		0		0	
Gjennomsnittskarakter:	C		C		C	
Antall med legeattest (L):	1		0		1	
Antall trekk før eksamen (T):	0		0		0	

Karakter	Antall	Antall kvinner
E	3	1
D	6	1
C	9	2
B	3	1
A	2	0



FS580.001 Resultatfordeling

Eksamen: MAT220 0 S 2015 VÅR

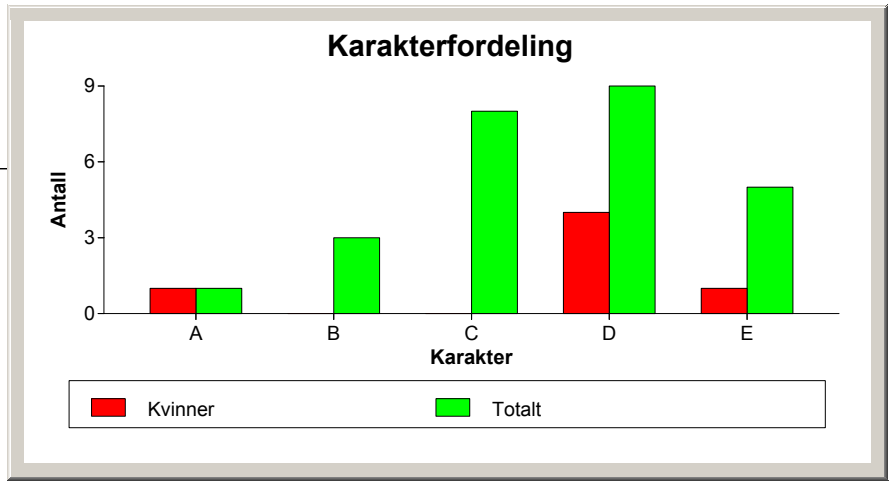
Algebra - Skoleeksamen 10,0sp

Karakterregel: Beste: A, Bestått: E, Dårligste: F

-

	Totalt		Kvinner		Menn	
Antall kandidater (oppmeldt):	45		11		34	
Antall møtt til eksamen:	33		7		26	
Antall bestått (B):	26		6		20	
Antall stryk (S):	7	21%	1	14%	6	23%
Antall avbrutt (A):	0		0		0	
Gjennomsnittskarakter:	D		D		C	
Antall med legeattest (L):	0		0		0	
Antall trekk før eksamen (T):	0		0		0	

Karakter	Antall	Antall kvinner
E	5	1
D	9	4
C	8	0
B	3	0
A	1	1



MAUMAT644 ALGEBRA vår 2015

Forelesningsplan

Runar Ile

That was the river
This is the sea

Koordinater

– Første samling*: 16. og 17. januar. Grupper
– Andre samling**: 12. og 13. februar. Mer om grupper og gruppevirkninger
– Tredje samling: 19. og 20. mars. Ringer
– Fjerde samling**: 16. og 17. april. Kroppsutvidelser, geometriske konstruksjoner og Sylows teoremer

NB*: Fredag og lørdag første samling (9-15), ellers torsdag (10-16) og fredag (9-15).
NB**: Samlingene er på VilVite (Thormøhlens gate 51) i konferanserom B, unntatt fredag andre samling og siste samling som er i konferanserom D.

Lærebok: J. B. Fraleigh *A first course in abstract algebra*, Pearson Education Limited, 7. utg, ISBN 13: 978-1-292-02496-7

1 Grupper

1.1 Introduksjon: Grupper og ringer

– de to sentrale begrepene i kurset.

1.2 Hva er en gruppe?

Kapittel 1

Avsnitt 4: Definisjon av grupper
Avsnitt 5: Undergrupper
Avsnitt 6: Sykliske grupper

Kapittel 2

Avsnitt 8: Permutasjonsgrupper
Avsnitt 9: Baner, sykler og de alternerende gruppene
Avsnitt 10: Restklasser og Lagrange' teorem
Avsnitt 11: Direkte produkter og endelig genererte abelske grupper

2 Gruppehomomorfier og gruppevirkninger

Kapittel 3

2.1 Når er to grupper strukturlike?

Avsnitt 13: Homomorfier av grupper

2.2 Hvordan lager vi nye grupper fra kjente grupper?

Avsnitt 14: Kvotientgrupper
Avsnitt 15: Kvotientgruppeberegninger og simple grupper

2.3 Hvordan teller vi symmetrisk mønstre?

Avsnitt 16: Gruppevirkninger
Avsnitt 17: Burnsides teorem
Kapittel 2, avsnitt 12: Plane isometrier

3 Ringer

3.1 Hva er en ring?

Kapittel 4

Avsnitt 18: Ringer og kropper
Avsnitt 19: Integritetsområder
Avsnitt 20: Fermats lille teorem og Eulers teorem
Avsnitt 21: Kvotientkroppen til et integritetsområde
Avsnitt 22: Polynomringer
Avsnitt 23: Faktorisering av polynomer over en kropp

3.2 Når er to ringer strukturlike? Hvordan lager vi nye ringer fra kjente ringer?

Kapittel 5

Avsnitt 26: Homomorfismer av ringer og kvotientringer
Avsnitt 27: Primidealer og maksimale idealer

4 Kroppsutvidelser, geometriske konstruksjoner og Sylows teoremer

4.1 Hva har kroppsutvidelser med geometriproblemer å gjøre?

Kapittel 6

Avsnitt 29: Kroppsutvidelser
Avsnitt 30: Vektorrom
Avsnitt 31 til om med 31.11: Algebraiske kroppsutvidelser
Avsnitt 32: Geometriske konstruksjoner. Dobling av kuben, kvadrering av sirkelen og tredeling av vinkelen.

4.2 Når har en gruppe en undergruppe?

Kapittel 7

Avsnitt 36: Sylows teoremer

Det kan komme endringer i denne planen. Gjeldende versjon ligger på MiSide.

MAUMAT644 ALGEBRA vår 2015

Andre obligatoriske oppgave

Runar Ile

«Ok» betyr at besvarelsen er uten plett og lyte. Man må ha minst 60% skår for å bestå.

Kommentarer til innlevering 2, XXX

Avsnitt 8, oppgave 45

Ok

Avsnitt 11, oppgave 18

Det er ikke sant at $\mathbb{Z}_{24}$ er isomorf med $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$, men derimot er $\mathbb{Z}_{24} \cong \mathbb{Z}_8 \times \mathbb{Z}_3$. Etter dette konkluderer du rett. I den lange listen med grupper mot slutten er mange av dem *ikke* isomorfe (du blander antagelig sammen med listen av mulige *ikke-isomorfe* grupper av en gitt orden på standardform). Kanskje du ikke mener det du skriver.

Avsnitt 11, oppgave 26

Ok (her bruker du standardformen helt rett)

Avsnitt 12, oppgave 8

Ok

Avsnitt 12, oppgave 16

Ok (du kunne være helt konkret på to slike rotasjoner hvis sammensetning blir en translasjon. NB: For mange par av rotasjoner blir sammensetningen en ny rotasjon selv om rotasjonssentrene er forskjellige!)

Avsnitt 12, oppgave 30

(a) Jo (du skal dessuten rotere rundt et punkt, ikke en akse)
(b) Ok
(c) Ok
(d) Ok
(e) Ok, men glidespeilingen kan ikke lages som sammensetningen av en translasjon og en rotasjon *som ligger i symmetrigruppen*. Derimot kan translasjonene genereres av glidespeilingene og hele gruppen genereres av en glidespeiling og en rotasjon (eller en refleksjon).

Avsnitt 13, oppgave 8

Ok (gruppen må være abelsk for at inversen skal være en gruppehomomorfi)

Avsnitt 13, oppgave 20

Ok

Avsnitt 13, oppgave 29

Ok

Avsnitt 13, oppgave 32

(a) Det er dette som skal vises, men du argumenterer ikke for at aha^{-1} ligger i A_n for alle a i S_n og h i A_n.
(b) Men hvordan vet du at det alltid finnes en gruppehomomorfi mellom to grupper? («of G into G'» oversettes best med «fra G til G'»)
(c) Ok
(d) Ok
(e) Ok
(f) Ok
(g) Ok
(h) $x \mapsto 2x$ gir ikke en gruppehomomorfi fra $\mathbb{Z}_6$ til $\mathbb{Z}_{10}$ fordi $2 \cdot 6 \not\equiv 0 \pmod{10}$, men det finnes en veldig enkel gruppehomomorfi som du kan bruke i stedet.
(i) Ja, det nøytrale elementet er alltid i kjernen fordi $\varphi(e_1) = e_2$ for alle gruppehomomorfier φ.
(j) Rett svar, f. eks. $\mathbb{Z}_2 \to \mathbb{Z} \times \mathbb{Z}_2$ gitt ved $1 \mapsto (0,1)$, men din avbildning gir ikke en gruppehomomorfi ($0 = 1 + 2$ må avbilde på det nøytrale elementet 0 i $\mathbb{Z}$, men avbilder på 3 i stedet.

Avsnitt 14, oppgave 2

Undergruppen $\langle 2 \rangle$ av $\mathbb{Z}_4$ har orden 2, mens undergruppen $\langle 2 \rangle$ av $\mathbb{Z}_{12}$ har orden 6. Produktgruppen $\langle 2 \rangle \times \langle 2 \rangle$ har derfor $2 \cdot 6$ elementer.

Avsnitt 14, oppgave 6

Ok

Avsnitt 14, oppgave 14

Rett svar, men du kunne kanskje ha skrevet ut elementene i $\langle (1,2) \rangle$ slik at vi ser at multipler av $(3,3)$ ikke gir noen av disse elementene før $8 \cdot (3,3)$ – ordenen til $(3,3) + \langle (1,2) \rangle$ (i kvotientgruppen) er akkurat i dette tilfellet lik ordenen til $(3,3)$, men slik er det slettes ikke alltid. Du kan også bare skrive at ingen av elementene $m \cdot (3,3)$ ligger i $\langle (1,2) \rangle$ for $m = 0, 1, 2, \ldots, 7$.

Avsnitt 14, oppgave 30

–

Avsnitt 15, oppgave 4

Ok

Avsnitt 16, oppgave 8

(a) Ok
(b) Ok

(c) e er ikke nødvendigvis det eneste gruppeelementet som fikserer elementer i mengden den virker på. Eks: Du roterer en ensfarvet trekant 120 grader så får du den samme ensfarvede trekanten.
(d) Hmm, konklusjonen skal være at $x_1 = x_2$ hvis $g(x_1) = g(x_2)$. Du roterer en ensfarvet trekant 120 grader eller 240 grader så får du den samme ensfarvede trekanten. Allikevel er ikke disse to gruppeelementene like.
(e) Dette er litt vanskeligere, men det er også nesten per definsion av bane.
(f) ?
(g) ?
(h) ?
(i) ?

Avsnitt 17, oppgave 8

Vi tenker på 50 ohm som rød og 100 ohm som blå. Da skal vi telle antall forskjellige farvelegginger av tetraederkantene når vi har to farver.

Her står det veldig mye. F. eks. står det at det er 6 mulige farvelegginger for hver av rotasjonene (ρ-ene). Men det er bare $2 \cdot 2$ – tre og tre kanter må ha samme farve. Så har du med speilinger, men det skal ikke være med her (vel, det kunne være med). Her må to og to og en og en kant ha samme farve, altså 16 mulige farvelegginger, hvorfor får du 4? – Det er fire valg av farve. Så står det at gruppen innholder 8 elementer. Det gjør den ikke (det er 24 med speilinger og 12 uten, du kan tenke som med kuben – det var noe av vitsen med å ha med den oppgaven). Så har gruppen fått 10 elementer. Osv. Det er ikke så enkelt for meg å forså alt du skriver, dessverre.

Eksamen vår 2011, oppgave 5

(1) Ok (to isomorfiklasser, ja)
(2) –
(3) Elementet $(3, 5)$ har orden 3, men du skal se på elementet $(5, 3)$. Med ditt element finner du riktige alternativer.
(4) –

Oppsummérende kommentar

Det er ujevnt. På de «resonnerende» oppgavene lager du noen ganger lengre utredninger som ikke er så relevante. Andre ganger har du gode løsninger her (13.8, 13.29 og noen av punktene i 13.32). Gruppehomomorfier er vanskelig stoff. Du må ikke la deg lure i de enklere oppgavene (14.2) eller lese feil (Eksamen (3)). Stå på!

Konklusjon

Ikke bestått.

BOKMÅL

UNIVERSITETET I BERGEN

Det matematisk-naturvitenskapelige fakultet

Eksamen i emnet MAT220/MAUMAT644 - Algebra

Fredag 6. juni 2014, kl. 09-14

Tillatte hjelpemidler: Kalkulator i samsvar med fakultetets regler.

Oppgavesettet er på 3 sider.

Oppgave 1

(a) Anta H og N er to undergrupper av en gruppe G. Forklar hvorfor mengden $H \cap N = \{g \in G \mid g \in H \text{ og } g \in N\}$ med gruppeoperasjonen fra G både er en undergruppe av H og en undergruppe av N.

(b) Forklar hvorfor S_9 har en undergruppe H av orden 81 og en undergruppe N av orden 128. Hvor mange elementer kan det være i undergruppen $H \cap N$?

(c) Anta H og N er to undergrupper av en gruppe G. Forklar hvorfor $H \cap N$ er en normal undergruppe av H hvis N er normal i G.

(d) Mengden av matriser

$$H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \,\middle|\, n \in \mathbb{Z} \right\}$$

under matrisemultiplikasjon er en undergruppe av den generelle lineære gruppen $\mathrm{GL}(2, \mathbb{R})$. Avgjør om H er normal.

Oppgave 2

Du velger fritt bokstaver fra et alfabet med n bokstaver, legger dem i en sirkel og får et «sirkelord». To sirkelord er ekte forskjellige hvis det ene ikke er likt noen av rotasjonene av det andre. Vi lar «lengden» av et sirkelord være antall bokstaver i sirkelen.

(a) Bruk Burnsides teorem til å finne hvor mange ekte forskjellige sirkelord av lengde henholdsvis 3 og 12 som finnes. (For $n = 2$ er svaret 4 og 352.)

(b) La p være et primtall. Forklar hvordan Burnsides teorem kan brukes til å se at det finnes $\frac{1}{p}(n^p + (p-1)n)$ ekte forskjellige sirkelord av lengde p.

(c) Hva sier Fermats lille sats? Bruk resultatet i (b) til å vise Fermats lille sats.

Oppgave 3

Formelen $\alpha(x, y) = (1 - y, x - 1)$ beskriver en isometri av planet.

(a) Beregn $\alpha^2(0, 0)$ og gi en geometrisk beskrivelse av α^4. Er α en translasjon, en rotasjon, en refleksjon eller en glide-refleksjon?

(b) Finn to rotasjoner av planet slik at sammensetningen av dem blir en translasjon ulik identiteten. Forklar hvorfor dette viser at mengden av rotasjoner av planet under sammensetning ikke er en undergruppe av isometrigruppen.

Oppgave 4

Hege og Kåre skal løse andregradsligninger over endelige kropper. Kåre lurer på om han kan bruke abc-formelen.

(a) Kåre løser $3x^2 + 4x + 3 = 0$ der koeffisientene ligger i $\mathbb{Z}_7$. Han får

$$x = \frac{3 \pm \sqrt{2-1}}{6}$$

Dvs at løsningene er $x = 3$ og $x = 5$.

Hege syns dette er mistenkelig og i hvert fall for kort. Sjekk at svaret er korrekt og fyll inn mellomregningene Kåre gjorde da han brukte abc-formelen.

(b) Kåre finner en utledning av abc-formelen i en av lærebøkene sine fra skolen. Der står det: Anta $a \neq 0$.

$$\begin{aligned}
ax^2 + bx + c &= 0 \\
x^2 + \frac{b}{a}x + \frac{c}{a} &= 0 \\
\left(x + \frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a} &= 0 \\
\left(x + \frac{b}{2a}\right)^2 &= \left(\frac{b}{2a}\right)^2 - \frac{c}{a} \\
\left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a^2} \\
x + \frac{b}{2a} &= \pm\sqrt{\frac{b^2 - 4ac}{4a^2}} \\
x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}
\end{aligned}$$

Kåre mener denne utledningen kan brukes mer generelt. Anta $ax^2 + bx + c \in F[x]$ hvor F er en kropp med karakteristikk forskjellig fra 2. Forklar for hvert av de 6 stegene i utledningen over hvilke egenskaper ved kroppen som brukes.

(c) Hege prøver å løse $x^2 + 1 = 0$ i $\mathbb{Z}_2$ og får $x = \pm\sqrt{-1}$. Hun lurer på om dette gir mening. Kan du lese denne formelen på en meningsfull måte? Hvilke løsninger finner du da? Bruk dette til å faktorisere $x^2 + 1$.

(d) Nå prøver Hege å løse $x^2 + 1 = 0$ i $\mathbb{Z}_3$ og får igjen $x = \pm\sqrt{-1}$, men dette gir ingen løsning. Finn en kroppsutvidelse $\mathbb{Z}_3 \subseteq E$ av minimal grad slik at $x^2 + 1$ har en rot i E. Hvor mange elementer har E?

Oppgave 5

Avgjør om utsagnet er sant eller galt. Alle svar skal begrunnes.

(a) Gruppene $\mathbb{Z}_7^* \times \mathbb{Z}_{11}^*$ og $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ er ikke isomorfe.

(b) En nulldivisor i en kommutativ ring med 1 kan ikke ha en multiplikativ invers.

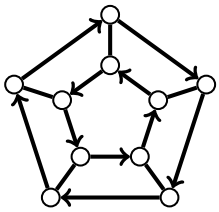
(c) Ligningen $45x \equiv 15 \pmod{24}$ har de samme løsningene som ligningen $15x \equiv 5 \pmod{8}$.

(d) Polynomringen $\mathbb{Z}_8[x]$ har ingen enheter av positiv grad.

(e) Ringen $\mathbb{Q}[x]/\langle 12x^3 + 119x^2 + 98x + 14\rangle$ er en kropp.

(f) Anta $\mathbb{Q} < E$ er en kroppsutvidelse av grad 7. Anta α er et element i E som ikke ligger i $\mathbb{Q}$. Da må $\mathbb{Q}(\alpha) = E$.

(g) En gruppe generert av to elementer er abelsk hvis Cayleygrafen ser slik ut:



Morten Brun og Runar Ile

BOKMÅL

UNIVERSITETET I BERGEN

Det matematisk-naturvitenskapelige fakultet

Eksamen i emnet MAT220/MAUMAT644 - Algebra

Fredag 6. juni 2014, kl. 09-14

Tillatte hjelpemidler: Kalkulator i samsvar med fakultetets regler.

Oppgavesettet er på 3 sider.

Oppgave 1

(a) Anta H og N er to undergrupper av en gruppe G. Forklar hvorfor mengden $H \cap N = \{g \in G \mid g \in H \text{ og } g \in N\}$ med gruppeoperasjonen fra G både er en undergruppe av H og en undergruppe av N.

(b) Forklar hvorfor S_9 har en undergruppe H av orden 81 og en undergruppe N av orden 128. Hvor mange elementer kan det være i undergruppen $H \cap N$?

(c) Anta H og N er to undergrupper av en gruppe G. Forklar hvorfor $H \cap N$ er en normal undergruppe av H hvis N er normal i G.

(d) Mengden av matriser

$$H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \,\middle|\, n \in \mathbb{Z} \right\}$$

under matrisemultiplikasjon er en undergruppe av den generelle lineære gruppen $\mathrm{GL}(2, \mathbb{R})$. Avgjør om H er normal.

Løsningsforslag

(a) Mengden $H \cap N$ er en delmengde av G. Vi vet også at det er en undergruppe av G, for den inneholder neutralelementet, er lukket under gruppeoperasjonen i G og er lukket under å danne inverselement. Alle disse tre egenskapene er konsekvens av at både H og N har de samme egenskapene.

Vi skal vise at $H \cap N$ er en undergruppe av H. Vi vet at både H og $H \cap N$ er undergrupper av G og at $H \cap N$ er inneholdt i H. Derfor er $H \cap N$ en undergruppe av H, for $H \cap N$ er en delmengde av H som er lukket under den binære gruppeoperasjonen i H, og som er en gruppe under den induserte operasjon på $H \cap N$. På samme måte ser vi at $H \cap N$ er en undergruppe av N.

(b) Ved Sylows første teorem har S_9 både en Sylow 3- og en Sylow 2-undergruppe. Da S_9 har $9! = 7 \cdot 5 \cdot 3^4 \cdot 2^7$ elementer består en Sylow 3-undergruppe av $3^4 = 81$ elementer og en Sylow 2-undergruppe består av $2^7 = 128$ elementer.

(c) Fra del (a) vet vi at $H \cap N$ er en undergruppe av H. Vi skal vise at hnh^{-1} ligger i $H \cap N$ for alle h i H og n i $H \cap N$. Siden N er normal i G vet vi at $hnh^{-1} \in N$. Siden både h og n ligger i H og H er en undergruppe av G ligger hnh^{-1} i H. Til sammen har vi sett at $hnh^{-1} \in H \cap N$ for alle h i H og n i $H \cap N$.

(c) Vi har at

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix}$$

Siden $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ er lik sin egen inverse viser dette at H ikke er normal i $\mathrm{GL}(2, \mathbb{R})$.

Oppgave 2

Du velger fritt bokstaver fra et alfabet med n bokstaver, legger dem i en sirkel og får et «sirkelord». To sirkelord er ekte forskjellige hvis det ene ikke er likt noen av rotasjonene av det andre. Vi lar «lengden» av et sirkelord være antall bokstaver i sirkelen.

(a) Bruk Burnsides teorem til å finne hvor mange ekte forskjellige sirkelord av lengde henholdsvis 3 og 12 som finnes. (For $n = 2$ er svaret 4 og 352.)

(b) La p være et primtall. Forklar hvordan Burnsides teorem kan brukes til å se at det finnes $\frac{1}{p}(n^p + (p-1)n)$ ekte forskjellige sirkelord av lengde p.

(c) Hva sier Fermats lille sats? Bruk resultatet i (b) til å vise Fermats lille sats.

Løsningsforslag

(a) Burnsides formel for virkningen av $\mathbb{Z}_m$ på mengden X av sirkelord av lengde m ved rotasjon gir at der er

$$r = \frac{1}{m} \sum_{a \in \mathbb{Z}_m} |X_a|$$

baner. Antallet av baner er antallet av ekte forskjellige sirkelord. Her er X_a mengden av sirkelord med samme bokstav på den i-te og den $a +_m i$-te plass for $i = 0, 1, \ldots, m-1$.

Hvis a deler m er et sirkelord i X_a entydig bestemt ved de første a bogstavene i ordet, så der er n^a slike sirkelord. Generelt har vi at hvis $g(x) = x$ så vil $g^n(x) = x$. Ulike generatorer for samme undergruppe vil derfor gi samme fikspunktmengde. Hvis c er største felles divisor av a og m, da er a og c generatorer for den samme undergruppen av $\mathbb{Z}_m$, så der er n^c sirkelord i X_a.

Skriver vi $\gcd(a, m)$ for største felles divisor av a og m er der altså

$$\frac{1}{m} \sum_{a=0}^{m-1} n^{\gcd(a,m)}$$

ekte forskjellige sirkelord av lengde m.

For $m = 3$ har vi $\gcd(0, 3) = 3$ og $\gcd(1, 3) = \gcd(2, 3) = 1$. Der er altså

$$\frac{1}{3}(n^3 + n + n) = \frac{1}{3}(n^3 + 2n)$$

ekte forskjellige sirkelord av lengde 3.

For $m = 12$ har vi

a	0	1	2	3	4	5	6	7	8	9	10	11
$\gcd(a, m)$	12	1	2	3	4	1	6	1	4	3	2	1

så det finnes

$$\frac{1}{12}(n^{12} + n^6 + 2n^4 + 2n^3 + 2n^2 + 4n)$$

ekte forskjellige sirkelord av lengde 12.

(b) For p et primtall og $0 < a < p$ er $\gcd(a,p) = 1$, så formelen over gir at det finnes

$$\frac{1}{p}(n^p + (p-1)n)$$

ekte forskjellige sirkelord av lengde p.

(c) Fermats lille sats sier at hvis p er et primtall som ikke deler et heltall n, da deler p tallet $n^{p-1} - 1$.

Fra (b) vet vi at for alle positive heltall n deler p tallet

$$n^p + (p-1)n = n(n^{p-1} + (p-1)).$$

Hvis p ikke deler n, da deler p tallet $n^{p-1} + (p-1) = (n^{p-1} - 1) + p$, så p deler også tallet $n^{p-1} - 1$. Dette gir Fermats lille sats for positive heltall. For $p = 2$ gjelder Fermats lille sats for alle odde heltall fordi $p - 1 = 1$ og hvis n er odde, da deler 2 deler $n^{p-1} - 1 = n - 1$. For p et odde primtall er $p - 1$ jevn, så

$$(-n)^{p-1} = (-1)^{p-1} n^{p-1} = n^{p-1}.$$

Derfor holder Fermats lille sats også for negative heltall n som ikke er delelige med p.

Oppgave 3

Formelen $\alpha(x,y) = (1-y, x-1)$ beskriver en isometri av planet.

(a) Beregn $\alpha^2(0,0)$ og gi en geometrisk beskrivelse av α^4. Er α en translasjon, en rotasjon, en refleksjon eller en glide-refleksjon?

(b) Finn to rotasjoner av planet slik at sammensetningen av dem blir en translasjon ulik identiteten. Forklar hvorfor dette viser at mengden av rotasjoner av planet under sammensetning ikke er en undergruppe av isometrigruppen.

Løsningsforslag

(a) Fra $\alpha(x,y) = (1-y, x-1)$ fås $\alpha(0,0) = (1,-1)$ og

$$\alpha^2(0,0) = \alpha(1,-1) = (2,0).$$

Generellt har vi $\alpha^2(x,y) = \alpha(1-y, x-1) = (2-x, -y)$ og at $\alpha^4(x,y) = \alpha^2(2-x,-y) = (x,y)$. Det vil si at α^4 er identitetsisometrien. Siden $\alpha^4 = \mathrm{id}$ må α enten være en rotasjon eller en speiling. Fra $\alpha^2(0,0) = (2,0) \neq (0,0)$ fås at $\alpha^2 \neq \mathrm{id}$ så α er ikke en speiling. Vi konkluderer at α er en rotasjon.

(b) La β være rotasjonen med 180 grader rundt $(0,0)$ og la γ være rotasjonen med 180 grader rundt $(1,0)$. I formler er $\beta(x,y) = (-x,-y)$ og $\gamma(x,y) = (1-(x-1), -y) = (2-x, -y)$. Da er $\beta\gamma(x,y) = (x-2, y)$, så $\beta\gamma$ er en translasjon med to enheter mot venstre langs x-aksen. Dette viser at mengden av rotasjoner av planet ikke er lukket under gruppeoperasjonen, så det er ikke en undergruppe av gruppen av isometrier av planet.

Oppgave 4

Hege og Kåre skal løse andregradsligninger over endelige kropper. Kåre lurer på om han kan bruke abc-formelen.

(a) Kåre løser $3x^2 + 4x + 3 = 0$ der koeffisientene ligger i $\mathbb{Z}_7$. Han får

$$x = \frac{3 \pm \sqrt{2-1}}{6}$$

Dvs at løsningene er $x = 3$ og $x = 5$.

Hege syns dette er mistenkelig og i hvert fall for kort. Sjekk at svaret er korrekt og fyll inn mellomregningene Kåre gjorde da han brukte abc-formelen.

(b) Kåre finner en utledning av abc-formelen i en av lærebøkene sine fra skolen. Der står det: Anta $a \neq 0$.

$$\begin{aligned}
ax^2 + bx + c &= 0 \\
x^2 + \frac{b}{a}x + \frac{c}{a} &= 0 \\
\left(x + \frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a} &= 0 \\
\left(x + \frac{b}{2a}\right)^2 &= \left(\frac{b}{2a}\right)^2 - \frac{c}{a} \\
\left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a^2} \\
x + \frac{b}{2a} &= \pm\sqrt{\frac{b^2 - 4ac}{4a^2}} \\
x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}
\end{aligned}$$

Kåre mener denne utledningen kan brukes mer generelt. Anta $ax^2 + bx + c \in F[x]$ hvor F er en kropp med karakteristikk forskjellig fra 2. Forklar for hvert av de 6 stegene i utledningen over hvilke egenskaper ved kroppen som brukes.

(c) Hege prøver å løse $x^2 + 1 = 0$ i $\mathbb{Z}_2$ og får $x = \pm\sqrt{-1}$. Hun lurer på om dette gir mening. Kan du lese denne formelen på en meningsfull måte? Hvilke løsninger finner du da? Bruk dette til å faktorisere $x^2 + 1$.

(d) Nå prøver Hege å løse $x^2 + 1 = 0$ i $\mathbb{Z}_3$ og får igjen $x = \pm\sqrt{-1}$, men dette gir ingen løsning. Finn en kroppsutvidelse $\mathbb{Z}_3 \subseteq E$ av minimal grad slik at $x^2 + 1$ har en rot i E. Hvor mange elementer har E?

Løsningsforslag

(a) For $x = 3$ i $\mathbb{Z}_7$ har vi $x^2 = -2$ og

$$3x^2 + 4x + 3 = -6 + 12 + 3 = 7 = 0.$$

For $x = 5$ i $\mathbb{Z}_7$ har vi $x = -2$ så $x^2 = 4$ og

$$3x^2 + 4x + 3 = 12 - 8 + 3 = 7 = 0.$$

Svaret stemmer altså. Kåre satte $a = 3$, $b = 4$, $c = 3$ og regnet

$$D = b^2 - 4ac = 16 - 36 = 2 - 1$$

i $\mathbb{Z}_7$. Siden $-4 = 3$ i $\mathbb{Z}_7$ gir abc-formelen

$$x = \frac{-b \pm \sqrt{D}}{2a} = \frac{-4 \pm \sqrt{2-1}}{6} = \frac{3 \pm \sqrt{2-1}}{6}.$$

(b) (1) Vi deler på a, eller ganger med $\frac{1}{a}$ ved bruk av den distributive loven. Siden F er en kropp og $a \neq 0$ er a en enhet, så elementet $\frac{1}{a}$ eksisterer. Siden enhver kropp er et intigritetsområde har vi at et element i F er 0 hvis og bare hvis $\frac{1}{a}$ ganget med dette elementet er 0. For at skrivemåten med brøker skal gi mening trenger vi alle egenskapene til et integritetsområde og at nevneren ikke er en null-divisor. For eksempel ligger det innebygget i skrivemåten at multiplikasjon i F er kommutativ og assosiativ.

(2) Ved å bruke at 2 er en enhet i F gir den distributive loven og kommutativitet av $+$ at

$$(x + \frac{b}{2a})^2 = x^2 + \frac{b}{a}x + (\frac{b}{2a})^2,$$

så ved eksistens av aditiv invers er

$$x^2 + \frac{b}{a}x + \frac{c}{a} = (x^2 + \frac{b}{a}x + (\frac{b}{2a})^2 - (\frac{b}{2a})^2 + \frac{c}{a} = (x + \frac{b}{2a})^2 - (\frac{b}{2a})^2 + \frac{c}{a}.$$

(3) Legg til $(\frac{b}{2a})^2 - \frac{c}{a}$ på begge sider av likhetstegnet. Her bruker vi at $< F, + >$ er en abelsk gruppe.

(4) For to brøker $\frac{c}{d}$ og $\frac{e}{f}$ er $\frac{c}{d} \cdot \frac{e}{f} = \frac{ce}{df}$. Den distributive loven gir at

$$(\frac{b}{2a})^2 - \frac{c}{a} = \frac{b^2}{4a^2} - \frac{4ac}{4a^2} = \frac{b^2 - 4ac}{4a^2}.$$

(5) Vi antar her at kvadratroten eksisterer, og at et polynom av grad 2 høyst har 2 Det er ikke alltid kvadratroten finnes. For eksempel finnes $\sqrt{-1}$ ikke i $\mathbb{R}$.

(6) Vi legger til $-\frac{b}{2a}$ på begge sider av likhetstegnet og bruker at

$$\pm\sqrt{\frac{b^2 - 4ac}{4a^2}} = \frac{\pm\sqrt{b^2 - 4ac}}{\sqrt{4a^2}} = \frac{\pm\sqrt{b^2 - 4ac}}{2a}$$

sammen med den distributive loven.

(c) I $\mathbb{Z}_2$ er $1^2 = 1 = -1$, så vi kan tolke $\sqrt{-1}$ som tallet 1. Siden $-1 = 1$ i $\mathbb{Z}_2$ finner vi bare løsningen $x = 1$. I $\mathbb{Z}_2$ har vi

$$x^2 + 1 = x^2 + 2x + 1 = (x + 1)^2.$$

(d) Polynomet $x^2 + 1$ er irredusibelt over $\mathbb{Z}_3$ fordi det ikke har noen rot i $\mathbb{Z}_3$. Derfor er $< x^2 + 1 >$ et maksimalt ideal i $\mathbb{Z}_3$ og $E = \mathbb{Z}_3[x]/ < x^2 + 1 >$ en kroppsutvidelse av $\mathbb{Z}_3$ av grad 2. Elementet $\alpha = x + \langle x^2 + 1 \rangle$ i E er rot i polynomet $x^2 + 1$ over E. Der er $9 = 3 \cdot 3$ elementer i E.

Oppgave 5

Avgjør om utsagnet er sant eller galt. Alle svar skal begrunnes.

(a) Gruppene $\mathbb{Z}_7^* \times \mathbb{Z}_{11}^*$ og $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ er ikke isomorfe.

(b) En nulldivisor i en kommutativ ring med 1 kan ikke ha en multiplikativ invers.

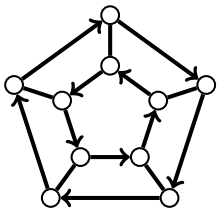
(c) Ligningen $45x \equiv 15 \pmod{24}$ har de samme løsningene som ligningen $15x \equiv 5 \pmod{8}$.

(d) Polynomringen $\mathbb{Z}_8[x]$ har ingen enheter av positiv grad.

(e) Ringen $\mathbb{Q}[x]/\langle 12x^3 + 119x^2 + 98x + 14\rangle$ er en kropp.

(f) Anta $\mathbb{Q} < E$ er en kroppsutvidelse av grad 7. Anta α er et element i E som ikke ligger i $\mathbb{Q}$. Da må $\mathbb{Q}(\alpha) = E$.

(g) En gruppe generert av to elementer er abelsk hvis Cayleygrafen ser slik ut:



Løsningsforslag

(a) Galt. Den abelske gruppen $\mathbb{Z}_7^*$ har 6 elementer. Strukturteoremet for endelig genererte abelske grupper forteller oss at der er en isomorfi $\mathbb{Z}_7^* \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. På samme måte ser vi at der er en isomorfi $\mathbb{Z}_{11}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_5$. Til sammen fås isomorfier

$$\mathbb{Z}_7^* \times \mathbb{Z}_{11}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5.$$

(b) Sant. La a være en nulldiviser i en kommutativ ring. Da finnes $b \neq 0$ i ringen slik at $ab = 0$. Anta motsetningsvis at c er en multiplikativ invers til a slik at $ca = 1$. Da får vi at

$$0 = c \cdot 0 = c(ab) = (ca)b = 1 \cdot b = b,$$

som er i motstrid med at $b \neq 0$.

(c) Oppgaven kan tolkes på to måter med to forskjellige svar. Galt: Både $x = 3$ og $x = 11$ i $\mathbb{Z}_{24}$ har $45x \equiv 15 \pmod{24}$, men 3 og 11 er like i $\mathbb{Z}_8$. Sant: Siden $\mathbb{Z}$ er et integritetsområde gjelder for et heltall x at $24 = 3 \cdot 8$ deler tallet $45x - 15 = 3(15x - 5)$ hvis og bare hvis 8 deler tallet $15x - 5$. Det vil si at for $x \in \mathbb{Z}$ er $45x \equiv 15 \pmod{24}$ hvis og bare hvis $15x \equiv 5 \pmod{8}$.

(d) Galt. I $\mathbb{Z}_8[x]$ er $1 + 4x$ en enhet fordi

$$(1 + 4x)^2 = 1 + 8x + 16x^2 = 1.$$

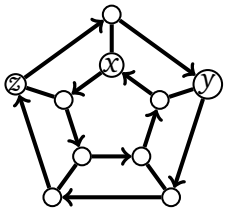
(e) Sant. Eisenstein med $p = 7$ gir at $12x^3 + 119x^2 + 98x + 14$ er irredusibel over $\mathbb{Q}$, og derfor er $< 12x^3 + 119x^2 + 98x + 14 >$ et maksimalt ideal, og kvotientringen er en kropp.

(f) Sant. Siden $\mathbb{Q}(\alpha) \neq \mathbb{Q}$ og

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [E : \mathbb{Q}(\alpha)] = [E : \mathbb{Q}] = 7$$

må vi ha $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 7$ og $[E : \mathbb{Q}(\alpha)] = 1$, så $\mathbb{Q}(\alpha) = E$.

(g) Galt. De to generatorer kommuterer ikke. Hvis strekene med pilspiss er multiplikasjon med generatoren a og strekene uten pil er multiplikasjon med generatoren b, da er $z = xab$ og $y = xba$ i figuren under. Siden y og z er forskjellige er gruppen ikke abelsk.



Morten Brun og Runar Ile

BOKMÅL

UNIVERSITETET I BERGEN

Det matematisk-naturvitenskapelige fakultet

Eksamen i emnet MAT220/MAUMAT644 - Algebra

Fredag 5. juni 2015, kl. 09-14

Tillatte hjelpemidler: Kalkulator i samsvar med fakultetets regler.
Oppgavesettet er på 2 sider.

Alle svar skal begrunnes.

Oppgave 1

Gitt to permutasjoner

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 5 & 4 & 1 & 6 & 2 & 8 \end{pmatrix} \quad \text{og} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 7 & 3 & 6 & 5 & 8 & 2 & 4 \end{pmatrix}$$

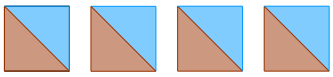
(a) Skriv σ og τ på sykelform. Finn ordenen til σ og ordenen til τ.

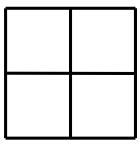
(b) La $G = \langle \sigma, \tau \rangle$ være den minste undergruppen av S_8 som inneholder både σ og τ. Forklar hvorfor G er en abelsk gruppe.

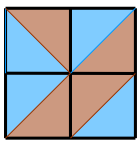
(c) Vis at $\sigma^3 = \tau^3$. La $N = \langle \tau \rangle$ være den minste undergruppen av S_8 som inneholder τ. Vis at kvotientgruppen G/N er isomorf med $\mathbb{Z}_3$.

(d) Finn ordenen til G og klassifisér G i henhold til fundamentalteoremet for endeliggenererte abelsk grupper.

Oppgave 2

Vi plasserer fire identiske kvadratiske brikker 

i følgende figur: 

Eksempel: 

La X være mengden av mønstre vi kan lage på denne måten. Gruppen av symmetrier til det store kvadratet er $D_4 = \{e, \rho, \rho^2, \rho^3, \tau_1, \tau_2, \mu_1, \mu_2\}$ der ρ er en rotasjon med 90^o, τ_1 og τ_2 er speilingene om den vertikale, henholdsvis horisontale symmetrilinjen, og μ_1, μ_2 er speilingene om de to diagonalene. Gruppen D_4 virker på mengden X.

(a) Tegn alle elementene i banen til eksempelet gitt i innledningen til oppgaven. Tegn elementene i fikspunktmengden X_ρ.

(b) Forklar hvorfor $|X| = 256$, $|X_{\rho^2}| = 16$ og $|X_{\mu_1}| = 16$.

(c) Beregn antall baner til virkningen av D_4 på X.

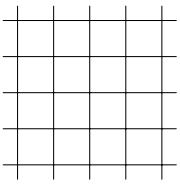
(d) Avgjør om noen av mønstrene i X har en symmetrigruppe som er isomorf med $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Oppgave 3

La G være gruppen av alle plane isometrier og la N være undergruppen til G som består av translasjoner og rotasjoner.

(a) Forklar hvorfor N er normal i G.

(b) La H være symmetrigruppen til tapetmønsteret



Avgjør om undergruppen $H \cap N$ (symmetriene til tapetet som ligger i N) er abelsk.

(c) Finn tre frisemønstre med tre ikke-isomorfe symmetrigrupper.

Oppgave 4

La $f(x) = x^3 + 2x + 1 \in \mathbb{Z}_7[x]$.

(a) Forklar hvorfor $F = \mathbb{Z}_7[x]/\langle f \rangle$ er en kropp.

(b) Vi har at $F = \mathbb{Z}_7(\alpha)$ for $\alpha = x + \langle f \rangle$ i F. Bruk α til å gi en basis for F over $\mathbb{Z}_7$. Bestem antall elementer i F.

(c) Vis at $\alpha^5 + \alpha^2 = 5\alpha^3$. Uttrykk α^5 ved hjelp av basisen du fant i (b).

(d) Beregn $(x^3 + 2x + 1) : (x + 6)$ i $\mathbb{Z}_7[x]$ med rest. Bruk dette til å uttrykke $(\alpha + 6)^{-1}$ i basisen fra (b).

Oppgave 5

(a) Bestem $\text{grad}(\sqrt{2}, \mathbb{Q})$ og $\text{irr}(\sqrt[3]{3}, \mathbb{Q})$.

(b) Sett $\alpha = 2 + \sqrt[3]{3}$. Forklar hvorfor $\text{grad}(\alpha, \mathbb{Q}) = \text{grad}(\sqrt[3]{3}, \mathbb{Q})$. Forklar hvorfor $\sqrt{2 + \sqrt[3]{3}}$ er algebraisk over $\mathbb{Q}$.

(c) Finn en basis for $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$. Uttrykk $(2\sqrt{3} - \sqrt{5})^{-1}$ i denne basisen. Forklar hvorfor $\mathbb{Q}(2\sqrt{3} - \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

(d) Vis at $2\sqrt{3} - \sqrt{5}$ er en rot i polynomet $g(x) = x^4 - 34x^2 + 49$. Forklar hvorfor $g(x)$ er irredusibelt over $\mathbb{Q}$.

(e) Anta m og n er positive heltall uten felles faktorer. Bestem $[\mathbb{Q}(\sqrt[m]{7}, \sqrt[n]{7}) : \mathbb{Q}]$.

UNIVERSITETET I BERGEN

Det matematisk-naturvitenskapelige fakultet

Eksamen i emnet MAT220/MAUMAT644 - Algebra

Fredag 5. juni 2015, kl. 09-14

Tillatte hjelpemidler: Kalkulator i samsvar med fakultetets regler.

Løsningsforslag.

Oppgave 1

(a) Leser av: $\sigma = (1,3,5)(2,7)$, $\tau = (2,7)(4,6,8)$ og dermed $|\sigma| = 3 \cdot 2 = |\tau|$.

(b) Beregner $\sigma\tau = (1,3,5)(4,6,8) = \tau\sigma$ så alle elementer i G er på formen $\sigma^n\tau^m$ for n og m heltall. Produktet av to slike elementer vil være et nytt element på samme form, uavhengig av rekkefølgen; $(\sigma^{n_1}\tau^{m_1})(\sigma^{n_2}\tau^{m_2}) = (\sigma^{n_1+n_2}\tau^{m_1+m_2}) = (\sigma^{n_2}\tau^{m_2})(\sigma^{n_1}\tau^{m_1})$, så G er abelsk.

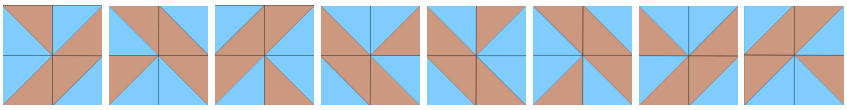
(c) Beregner $\sigma^3 = (2,7) = \tau^3$. Restklassene til N i G er $\{N, \sigma N, \sigma^2 N\}$ fordi $\sigma^3 \in N$. Multiplikasjonen er $(\sigma^n N)(\sigma^m N) = \sigma^{n+m \pmod 3} N$ så $G/N \cong \mathbb{Z}_3$.

(d) Fordi $|N| = 6$ og $|G/N| = 3$ vil $|G| = 6 \cdot 3$. Siden $18 = 2 \cdot 3 \cdot 3$ er det bare to muligheter i klassifikasjonen: Enten $G \cong \mathbb{Z}_2 \times \mathbb{Z}_9$ eller $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Men fordi et vilkårlig element $\sigma^n\tau^m$ i G har $(\sigma^n\tau^m)^6 = \mathrm{id}$ må alle elementer i G ha orden som deler 6. Dette utelukker $\mathbb{Z}_2 \times \mathbb{Z}_9$ som har elementer av orden 9.

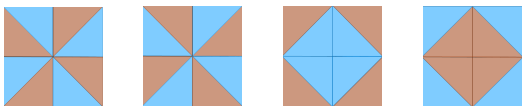
Oppgave 2

(a) Banen til eksemplet x innholder 8 elementer:

$x = e(x)$ $\rho(x)$ $\rho^2(x)$ $\rho^3(x)$ $\tau_1(x)$ $\tau_2(x)$ $\mu_1(x)$ $\mu_2(x)$



Fikspunktmengden X_ρ innholder 4 elementer – alt er bestemt av hvordan ett av de fire små kvadratene er satt:

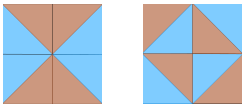


(b) Hvert lite kvadrat kan plasseres på 4 måter uavhengig av hverandre, det gir $|X| = 4^4 = 256$. De to øverste små kvadratene kan plasseres på 4^2 forskjellige måter og ρ^2 bestemmer de to andre så $|X_{\rho^2}| = 16$. For å være uendret under μ_1 må farvedelingslinjen i hvert av de to små kvadratene som dekker symmetrilinjen til μ_1 stå normalt på symmetrilinjen. Dette gir 2^2 muligheter. Ett av de andre kvadratene kan velges fritt, dvs $|X_{\mu_1}| = 2^2 \cdot 4$.

(c) Vi har at $|X_{\tau_1}| = 4^2$ da de to kvadratene på venstresiden kan velges fritt og bestemmer de to andre. Tilsvarende vil $|X_{\tau_2}| = 4^2$. Dessuten har vi $|X_\rho| = |X_{\rho^3}| = 4$ fra (a). Burnside gir

$$\begin{aligned}\text{antall baner} &= \frac{1}{|D_4|}(|X| + |X_\rho| + |X_{\rho^2}| + |X_{\rho^3}| + |X_{\tau_1}| + |X_{\tau_2}| + |X_{\mu_1}| + |X_{\mu_2}|) \\ &= \frac{1}{2^3}(2^8 + 2 \cdot 2^2 + 5 \cdot 2^4) = 43\end{aligned}$$

(d) La $T = \{e, \tau_1, \tau_2, \rho^2\}$ og $M = \{e, \mu_1, \mu_2, \rho^2\}$. Da er T og M to undergrupper av D_4 som begge er isomorfe med $\mathbb{Z}_2 \times \mathbb{Z}_2$. T er symmetrigruppen til «timeglassmønsteret», M er symmetrigruppen til det andre mønsteret:



Oppgave 3

(a) Hvis $g \in G$ ikke ligger i N vil g være en speiling eller en glidespeiling. Det vil også g^{-1}. Spesielt vil g og g^{-1} begge snu planet. Anta h er et element i N, dvs at h er en rotasjon eller en translasjon. Isometrien $g^{-1}hg$ vil være en rotasjon eller en translasjon fordi planet ikke snus. Det vil si at $g^{-1}hg$ ligger i N som derfor er normal.

(b) $H \cap N$ er ikke abelsk. F. eks. kan vi ta to nabohjørner i gitteret, A og B, og rotere først om A og så om B med 180^o. Det gir en translasjon i retning fra A mot B med lengde $2|AB|$. Omvendt rekkefølge av rotasjonene gir inversen til denne translasjonen.

(c) For eksempel:
... L L L L L L ... har symmetrigruppe $\mathbb{Z}$ (ingen rotasjoner, speilinger eller glidespeilinger)
...DDDDDD... har symmetrigruppe $\mathbb{Z} \times \mathbb{Z}_2$ (ingen rotasjoner, horisontal speiling, glidespeilinger som er sammensetninger av translasjonene og speilingene)
...SSSSS... har symmetrigruppe D_∞ (rotasjoner, ingen speilinger, ingen glidespeilinger)

Oppgave 4

(a) Finner ved innsetting at f ikke har noen røtter i $\mathbb{Z}_7$. Fordi $\text{grad}(f) = 3$ betyr dette at f er irredusibelt. Da er $\langle f \rangle$ et maksimalt ideal og derfor er F en kropp.

(b) $\mathscr{B} = \{1, \alpha, \alpha^2\}$ er en basis for F fordi $\text{grad}(f) = 3$ og f er irredusibelt. Dvs at $F = \{b + c\alpha + d\alpha^2 \mid b, c, d \in \mathbb{Z}_7\}$ som gir $|F| = 7^3$.

(c) I F gjelder $\alpha^3 + 2\alpha + 1 = 0$. Ved å multiplisere med α^2 følger $\alpha^5 + 2\alpha^3 + \alpha^2 = 0$ og dermed $\alpha^5 + \alpha^2 = 5\alpha^3$. Det følger at $\alpha^5 = 5\alpha^3 + 6\alpha^2 = 5(-2\alpha - 1) + 6\alpha^2 = 6\alpha^2 + 4\alpha + 2$.

(d) Finner $f(x) = (x+6)(x^2 + x + 3) + 4$ ved divisjonsalgoritmen. Dermed er $0 = f(\alpha) = (\alpha + 6)(\alpha^2 + \alpha + 3) + 4$ som ved multiplikasjon med $(\alpha + 6)^{-1}$ gir $(\alpha^2 + \alpha + 3) = 3(\alpha + 6)^{-1}$, dvs $(\alpha + 6)^{-1} = 5\alpha^2 + 5\alpha + 1$.

Oppgave 5

(a) $\text{grad}(\sqrt{2},\mathbb{Q}) = 2$ fordi minimalpolynomet $\text{irr}(\sqrt{2},\mathbb{Q})$ er x^2-2 (irredusibelt over $\mathbb{Q}$ ved Eisenstein med $p=2$) har grad 2.
$\text{irr}(\sqrt[3]{3},\mathbb{Q}) = x^3-3$ fordi $\sqrt[3]{3}$ er en rot i x^3-3 og fordi x^3-3 er irredusibelt over $\mathbb{Q}$ (Eisenstein med $p=3$) og monisk.

(b) Fordi $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{3})$ vil $[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}]$. Generelt er $\text{grad}(\beta,\mathbb{Q}) = [\mathbb{Q}(\beta):\mathbb{Q}]$.
Vi har at $[\mathbb{Q}(\sqrt{\alpha}):\mathbb{Q}(\alpha)] \leqslant 2$ og dermed vil

$$[\mathbb{Q}(\sqrt{\alpha}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{\alpha}):\mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha):\mathbb{Q}] \leqslant 2 \cdot 3 < \infty$$

Altså er $\sqrt{\alpha}$ algebraisk med $\text{grad}(\sqrt{\alpha},\mathbb{Q}) \leqslant 6$.

(c) Vi har $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a,b \in \mathbb{Q}\}$. Så hvis $\sqrt{5} \in \mathbb{Q}(\sqrt{3})$ vil det finnes $a,b \in \mathbb{Q}$ slik at $\sqrt{5} = a + b\sqrt{3}$ som (etter kvadrering) medfører at $\sqrt{3} \in \mathbb{Q}$ som er galt. Altså er $[\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}(\sqrt{3})] = 2$ og

$$[\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2 \cdot 2$$

Ved å «multiplisere» basisene $\{1,\sqrt{5}\}$ for $\mathbb{Q}(\sqrt{3},\sqrt{5})$ over $\mathbb{Q}(\sqrt{3})$ og $\{1,\sqrt{3}\}$ for $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$ får vi basisen $\{1,\sqrt{3},\sqrt{5},\sqrt{15}\}$ for $\mathbb{Q}(\sqrt{3},\sqrt{5})$ over $\mathbb{Q}$.

Vi har

$$\begin{aligned}(2\sqrt{3}-\sqrt{5})^{-1} &= \frac{1}{(2\sqrt{3}-\sqrt{5})} \cdot \frac{(2\sqrt{3}+\sqrt{5})}{(2\sqrt{3}+\sqrt{5})} \\ &= \frac{2}{7}\sqrt{3} + \frac{1}{7}\sqrt{5}\end{aligned}$$

Dermed vil $\frac{1}{2}(2\sqrt{3}-\sqrt{5}) + \frac{7}{2}(2\sqrt{3}-\sqrt{5})^{-1} = \sqrt{3}$ være et element i $\mathbb{Q}(2\sqrt{3}-\sqrt{5})$. Det følger at $\sqrt{5} \in \mathbb{Q}(2\sqrt{3}-\sqrt{5})$ og derfor $\mathbb{Q}(2\sqrt{3}-\sqrt{5}) = \mathbb{Q}(\sqrt{3},\sqrt{5})$.

(d) Setter $\gamma = 2\sqrt{3}-\sqrt{5}$. Da er $\gamma^2 = 17 - 4\sqrt{15}$ og derfor $(\gamma^2-17)^2 = 240$ som gir at γ er en rot i $g(x)$. Fordi $\text{grad}(\gamma,\mathbb{Q}) = [\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}] = 4$ fra (c) vil $\text{irr}(\gamma,\mathbb{Q}) = g(x)$ og spesielt være irredusibelt over $\mathbb{Q}$.

(e) Multiplikasjonsformelen for kroppsutvidelser gir

$$[\mathbb{Q}(\sqrt[m]{7},\sqrt[n]{7}):\mathbb{Q}] = [\mathbb{Q}(\sqrt[m]{7},\sqrt[n]{7}):\mathbb{Q}(\sqrt[m]{7})] \cdot [\mathbb{Q}(\sqrt[m]{7}):\mathbb{Q}].$$

Fordi $[\mathbb{Q}(\sqrt[m]{7}):\mathbb{Q}] = m$ må m dele $[\mathbb{Q}(\sqrt[m]{7},\sqrt[n]{7}):\mathbb{Q}]$. Samtidig er $[\mathbb{Q}(\sqrt[m]{7},\sqrt[n]{7}):\mathbb{Q}(\sqrt[m]{7})] \leqslant n$. Vi har også

$$[\mathbb{Q}(\sqrt[m]{7},\sqrt[n]{7}):\mathbb{Q}] = [\mathbb{Q}(\sqrt[m]{7},\sqrt[n]{7}):\mathbb{Q}(\sqrt[n]{7})] \cdot [\mathbb{Q}(\sqrt[n]{7}):\mathbb{Q}]$$

så n må også dele $[\mathbb{Q}(\sqrt[m]{7},\sqrt[n]{7}):\mathbb{Q}]$ som derfor må være lik mn.

MAUMAT644 ALGEBRA vår 2015

Fjerde samling

Runar Ile

1 Kroppsutvidelser, geometriske konstruksjoner og Sylows teoremer

1.1 Hva har kroppsutvidelser med geometriproblemer å gjøre?

Avsnitt 29: *Kroppsutvidelser*

> *Stoff*: Utvidelseskropper og røtter til polynomer, Kroneckers teorem, algebraiske og transcendente elementer i utvidelseskropper, sammenhengen mellom algebraiske elementer og irredusible polynomer, graden til et algebraisk element, simple utvidelser
> *Oppgaver*: 2, 4, 6, 8, 17, 18, 23, 28

En kropp kan ligge som en underring i en større kropp. Et eksempel er kroppen av de reelle tall $\mathbb{R}$ som er en underring (eller underkropp) av kroppen av de komplekse tallene $\mathbb{C}$. Et polynom som er irredusibelt (ingen faktorisering) over den mindre kroppen kan faktorisere over den større kroppen. F. eks. er x^2-3 et irredusibelt polynom over kroppen av de rasjonale tallene $\mathbb{Q}$, men har to røtter, nemlig $\sqrt{3}$ og $-\sqrt{3}$ over de reelle tallene, dvs $x^2-3=(x-\sqrt{3})(x+\sqrt{3})$ er redusibelt over $\mathbb{R}$. Tilsvarende er x^2+1 irredusibelt over $\mathbb{R}$, men redusibelt over $\mathbb{C}$. Legg merke til at vi ikke behøver å utvide $\mathbb{Q}$ til $\mathbb{R}$ for å finne en rot til x^2-3. Det holder å utvide $\mathbb{Q}$ til ringen $\mathbb{Q}[\sqrt{3}]=\{a+b\sqrt{3}\,|\,a,b\in\mathbb{Q}\}$ som faktisk er en underkropp av $\mathbb{R}$. Gitt et polynom som er irredusibelt over en kropp så finnes alltid en slik kroppsutvidelse hvor polynomet har en rot, dvs kan faktoriseres som et produkt med en lineær faktor. Dette er essensen i Kronckers teorem.

En *kroppsutvidelse* av en kropp F er en kropp E som inneholder F som en underring (underkropp).

Teorem 1.1 (Kronecker)**.** *Anta F er en kropp og f er et polynom over F av positiv grad. Da finnes det en kroppsutvidelse E av F slik at f har en rot i E, dvs det finnes et element α i E slik at $f(\alpha)=0$.*

Bevis. Vi kan faktorisere f som et produkt av irredusible polynomer i $F[x]$. Det er tilstrekkelig å finne en kroppsutvidelse som innholder en rot for et av disse irredusible polynomene. Det vil også gi en rot for f. Vi kan derfor anta at f er et irredusibelt polynom. Vi vet fra Teorem 1.73 i notat 3 at idealet $\langle f\rangle=\{gf\,|\,g\in F[x]\}$ generert av f er et maksimalt ideal i $F[x]$ og dermed er kvotientringen $F[x]/\langle f\rangle$ en kropp. Vi kaller den for E. Vi har en en-til-en ringhomomorfi $F\to F[x]$ og en ringhomomorfi $F[x]\to E$ fra Teorem 1.60 i notat 3 (fundamentalteoremet for ringhomomorfier). Sammensetningen av disse to ringhomomorfiene blir en ringhomomorfi $F\to E$ som avbilder a i F på restklassen $a+\langle f\rangle$ i E. Denne ringavbildningen er en-til-en: Hvis a og b avbilder på samme element er $a+\langle f\rangle=b+\langle f\rangle$, dvs $a-b$ er et element i $\langle f\rangle$, dvs at f er en faktor i

$a-b$. Men dette er umulig hvis $a-b \neq 0$ fordi $a-b$ har grad 0, mens f per antagelse har positiv grad i $F[x]$. Altså må $a=b$ og ringhomomorfien er derfor en-til-en.

Vi setter $\alpha = x + \langle f \rangle$. Så ser vi på evalueringsavbildningen $\varphi_\alpha \colon F[x] \to E$. Den setter inn α for x i polynomet. Anta $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Da får vi

$$\begin{aligned} \varphi_\alpha(f) = f(x+\langle f\rangle) &= a_n(x+\langle f\rangle)^n + a_{n-1}(x+\langle f\rangle)^{n-1} + \cdots + a_0 \\ &= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) + \langle f\rangle \\ &= f + \langle f\rangle \\ &= \langle f\rangle \end{aligned} \tag{1.1.1}$$

som er 0 i E. Altså er $\alpha = x + \langle f\rangle$ en rot for f i kroppsutvidelsen E av F. □

Føler du deg lurt?

Dette er et helt sentralt resultat for denne teorien. Det gir muligheten til å finne en kroppsutvidelse hvor f har en fullstendig faktorisering i lineære faktorer.

Eksempel 1.2. Vi setter $f = x^4 - 2x^2 - 3$. Da er $f = gh$ hvor $g = x^2+1$ og $h = x^2-3$. Men både g og h er irredusible over $\mathbb{Q}$. Vi utvider $\mathbb{Q}$ til $E = \mathbb{Q}[x]/\langle x^2+1\rangle$. Da er $\alpha = x + \langle x^2+1\rangle$ en rot for g og derfor også for f. Vi regner

$$\begin{aligned} g(\alpha) &= (x+\langle x^2+1\rangle)^2 + 1 \\ &= x^2 + x\langle x^2+1\rangle + \langle x^2+1\rangle x + \langle x^2+1\rangle^2 + 1 \\ &= (x^2+1) + \langle x^2+1\rangle \\ &= \langle x^2+1\rangle \\ &= 0 \text{ i } E. \end{aligned} \tag{1.2.1}$$

Men h har ingen røtter i E. Så vi må utvide E til $K = E[y]/\langle y^2-3\rangle$. Her er $\beta = y + \langle y^2-3\rangle$ en rot for h. Altså kan vi faktorisere f i et produkt av lineære faktorer over K. Nemlig $f = (x-\alpha)(x+\alpha)(x-\beta)(x+\beta)$.

Faktisk er K isomorf med ringen $\mathbb{Q}[i,\sqrt{3}] = \{a+bi+c\sqrt{3}+di\sqrt{3} \mid a,b,c,d \in \mathbb{Q}\}$.

Definisjon 1.3. Anta at E er en kroppsutvidelse av F og α er et element i E. Da er α *algebraisk over* F hvis det finnes et polynom f i $F[x]$ slik at $f(\alpha) = 0$. Hvis det ikke finnes noen slike polynomer er α *transcendent over* F.

Oppgave 1.4. Forklar hvorfor alle elementer i F er algebraiske over F.

Eksempel 1.5. Tallene e og π er transcendente over $\mathbb{Q}$. Det ble vist av Hermite (1873) for e og Lindemann (1882) for π.

Teorem 1.6. *Anta at E er en kroppsutvidelse av F og at $\alpha \in E$ er algebraisk over F. Da finnes det et* irredusibelt *polynom $f \in F[x]$ slik at $f(\alpha) = 0$ og dette polynomet er entydig bestemt opp til multiplikasjon med en konstant (element i F).*

Bevis. Vi ser på evaleringsavbildningen $\varphi_\alpha \colon F[x] \to E$. Siden den er en ringhomomorfi er kjernen (dvs de elementene som avbilder på 0) et ideal. Ved Teorem 1.72 i notat 3 er alle idealer i $F[x]$ prinsipale. Det betyr at kjernen til φ_α er

generert av et element som vi kaller f, dvs kjernen er $\langle f \rangle$. Vi påstår at f er et irredusibelt polynom. Anta $f = g \cdot h$. Siden $f(\alpha) = 0$ må enten $g(\alpha) = 0$ eller $h(\alpha) = 0$. Dvs at enten g eller h ligger i kjernen til φ_α, dvs at f enten deler g eller h. Men hvis f. eks. f deler g må $\text{grad}(f) = \text{grad}(g)$ og $\text{grad}(h) = 0$. Dvs at h er en konstant og f er derfor et irredusibelt polynom. □

Definisjon 1.7. Anta E er en kroppsutvidelse av F og $\alpha \in E$ er algebraisk over F. Da kaller vi det (entydige) irredusible polynomet f som har $f(\alpha) = 0$ og som har 1 som koeffisient foran den høyeste potensen av x for *det irredusible polynomet til α over F* og bruker skrivemåten $f = \text{irr}(\alpha, F)$. Graden til dette polynomet er *graden til α over F*. Vi skriver $\text{grad}(\alpha, F) = \text{grad}(f)$.

Avsnitt 30: *Vektorrom*

> *Stoff*: Definisjon av vektorrom over en kropp, lineær uavhengighet og basis, utvidelseskropper som vektorrom (særlig eksempel 4, 8, 11, 14, 22)
> *Oppgaver*: 4, 6, 8, 15

Definisjon 1.8. Et vektorrom V over en kropp F er en abelsk gruppe (vi skriver $+$ for gruppeoperasjonen) hvor det også er mulig å multiplisere elementene i V (kalt vektorer) med elementer i F (kalt skalarer) og få nye vektorer. Denne *skalarmultiplikasjonen* skal være assosiativ (dvs $a, b \in F$ og $\gamma \in V$ så er $a(b\gamma) = (ab)\gamma$. Videre skal den være distributiv over addisjonen (dvs $a(\gamma + \delta) = a\gamma + a\delta$) og $1 \in F$ skal virke som identiteten (dvs $1\gamma = \gamma$).

Når man lærer om vektorrom for første gang er kroppen gjerne de reelle tallene. Nesten alt man da lærer om vektorrom og lineære transformasjoner av vektorrom gjelder generelt, uavhengig av hva slags kropp vektorrommene er definert over. Dette stoffet regnes derfor mest som repetisjon. Vi skal bare fokusere på det vi trenger videre.

Eksempel 1.9. Vi har at $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ er en kroppsutvidelse av $\mathbb{Q}$. Men $\mathbb{Q}[\sqrt{3}]$ er dermed også et vektorrom over $\mathbb{Q}$. For det første er $\mathbb{Q}[\sqrt{3}]$ en abelsk gruppe under addisjon (en undergruppe av $\langle \mathbb{R}, + \rangle$ fordi den er lukket under addisjonen, innholder 0 og har inverser til alle elementer). Assosiativitet og distributivitet av skalarmultiplikasjonen holder fordi alt skjer i kroppen $\mathbb{R}$. Vi behøver bare å bekymre oss for om skalarmultiplikasjonen er lukket: Vi multiplisere et element $a + b\sqrt{3}$ i $\mathbb{Q}[\sqrt{3}]$ med et element c i $\mathbb{Q}$ og får et nytt element $ca + cb\sqrt{3}$ i $\mathbb{Q}[\sqrt{3}]$.

Samme type argument gir:

Lemma 1.10. *Hvis F er en kropp og E er en kroppsutvidelse så er E et vektorrom over F.*

Anta V er et vektorrom over en kropp F og $\mathscr{B} = \{\gamma_1, \gamma_2, \ldots \gamma_n\}$ er en mengde vektorer i V. Hvis enhver vektor δ i V kan utrykkes ved hjelp av vektorene i $\mathscr{B}$ (dvs $\delta = a_1\gamma_1 + \cdots + a_n\gamma_n$ for noen $a_1, \ldots, a_n \in F$) på en entydig måte (ingen andre måter å velge $a_1, \ldots, a_n$) sier vi at $\mathscr{B}$ er en *basis for V over F*. En annen basis $\mathscr{B}'$ vil ha det samme antall elementer. Dette tallet n kalles *dimensjonen* til V over F.

Eksempel 1.11. I Eksempel 1.9 er $\mathscr{B} = \{1, \sqrt{3}\}$ en basis for $\mathbb{Q}[\sqrt{3}]$ over $\mathbb{Q}$. Siden basisen har to elementer er dimensjonen til vektorrommet $\mathbb{Q}[\sqrt{3}]$ over kroppen $\mathbb{Q}$ lik 2.

Oppgave 1.12. Forklar hvorfor $\mathscr{B}' = \{1 + 2\sqrt{3}, 3 + 7\sqrt{3}\}$ er en annen basis.

Lemma 1.13. *Anta F er en kropp og α er et algebraisk element i en kroppsutvidelse E med* $\text{grad}(\alpha, F) = n$. *La $F(\alpha)$ betegne den minste underkroppen av E som innholder både F og α. Da er $\mathscr{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ en basis for $F(\alpha)$.*

Eksempel 1.14. Vi setter $\alpha = \sqrt[5]{2} = 2^{\frac{1}{5}}$. Da er $\mathbb{Q}(\sqrt[5]{2})$ et 5-dimensjonalt vektorrom over $\mathbb{Q}$ med basis $1, \sqrt[5]{2}, (\sqrt[5]{2})^2, (\sqrt[5]{2})^3, (\sqrt[5]{2})^4$. Dette betyr at $\mathbb{Q}(\sqrt[5]{2})$ er lik *underringen* av $\mathbb{R}$ generert av $\mathbb{Q}$ og $\sqrt[5]{2}$, som vi pleier å skrive som $\mathbb{Q}[\sqrt[5]{2}]$. Dvs

$$\mathbb{Q}(\sqrt[5]{2}) = \{a + b\sqrt[5]{2} + c(\sqrt[5]{2})^2 + d(\sqrt[5]{2})^3 + e(\sqrt[5]{2})^4 \mid a, b, c, d, e \in \mathbb{Q}\} = \mathbb{Q}[\sqrt[5]{2}].$$

Legg merke til at $\mathbb{Q}[\sqrt[5]{2}]$ er den minste underringen av $\mathbb{R}$ som innholder $\mathbb{Q}$ og $\sqrt[5]{2}$ mens $\mathbb{Q}(\sqrt[5]{2})$ er den minste underkroppen av $\mathbb{R}$ som innholder $\mathbb{Q}$ og $\sqrt[5]{2}$. Lemma 1.13 sier at $\mathbb{Q}(\sqrt[5]{2}) = \mathbb{Q}[\sqrt[5]{2}]$ og mer generelt at $F(\alpha) = F[\alpha]$.

Oppgave 1.15. Forklar hvorfor $\mathbb{Q}[\sqrt{5}, \sqrt[3]{2}]$ er en kroppsutvidelse av $\mathbb{Q}$. Finn en basis for $\mathbb{Q}[\sqrt{5}, \sqrt[3]{2}]$ over $\mathbb{Q}$.

Avsnitt 31 til og med 31.11: *Algebraiske kroppsutvidelser*

> *Stoff*: Graden til en kroppsutvidelse, multiplikasjonsformelen for kroppsutvidelser, «Lagrange» for graden til algebraiske elementer
> *Oppgaver*: 2–7, 10, 12, 19–21, 23–25, 27, 29, 30

Teorem 1.16. *Anta F er en kropp og E en kroppsutvidelse med endelig dimensjon n som vektorrom over F. Da er ethvert element γ i E algebraisk over F.*

Bevis. Fordi alle basiser for E over F har like mange elementer, må det være en relasjon mellom de $n + 1$ elementene $\{1, \gamma, \gamma^2, \ldots, \gamma^n\}$. Dvs at det finnes elementer $a_n, a_{n+1}, \ldots, a_0$ i F og ikke alle lik 0 slik at $a_n\gamma^n + a_{n-1}\gamma^{n-1} + \cdots + a_0 = 0$. Det betyr at $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$ er et ikke-konstant polynom med $f(\gamma) = 0$, dvs γ er algebraisk. □

Vi sier at en kroppsutvidelse er *endelig* hvis den har endelig dimensjon og at den er *algebraisk* hvis alle elementer er algebraiske over grunnkroppen. Teorem 1.16 sier at en endelig kroppsutvidelse er algebraisk. Vi skrive $n = [E : F]$ hvis kroppsutvidelsen E av F har dimensjon n og kaller det *graden til kroppsutvidelsen*.

Ved å se på beviset er det klart at Kroneckers teorem kan styrkes til: Det finnes alltid en endelig, algebraisk utvidelse av kroppen slik at polynomet har en rot.

Så kommer vi til et veldig viktig resultat i denne teorien som minner en god del om Lagrange' teorem i gruppeteori.

Teorem 1.17. *Anta F er en kropp, E er en endelig kroppsutvidelse av F og K en endelig kroppsutvidelse av E. Da er K en endelig kroppsutvidelse av F og*

$$[K : F] = [K : E] \cdot [E : F]$$

Bevis. Anta $\gamma_1, \ldots, \gamma_n$ er en basis for E over F og $\delta_1, \ldots, \delta_m$ er en basis for K over E. Vi viser at $\{\gamma_i\delta_j\}_{i=1,\ldots,n;\, j=1,\ldots,m}$ gir en basis for K over F. Produktene $\gamma_i\delta_j$ er i kroppen K.

Først viser vi at ethvert element α i K kan uttrykkes som en lineærkombinasjon av disse elementene over F. Vi vet at α kan uttrykkes ved en lineærkombinasjon av δ_j-ene over E, dvs det finnes elementer $b_1, \ldots, b_m$ i E slik at

$$\alpha = b_1\delta_i + \cdots + b_m\delta_m. \tag{1.17.1}$$

Men for hvert av elementene b_r finnes det elementer $c_{1,r}, c_{2,r}, \ldots, c_{n,r}$ i F slik

$$b_r = c_{1,r}\gamma_1 + c_{2,r}\gamma_2 + \cdots + c_{n,r}\gamma_n. \tag{1.17.2}$$

Vi substituerer dette utrykket inn for b_r i (1.17.1) og får at α kan uttrykkes som en lineærkombinasjon av elementene $\gamma_i\delta_j$.

Så viser vi at $\{\gamma_i\delta_j\}_{i=1,\ldots,n;\, j=1,\ldots,m}$ er uavhengige over F. Anta vi har elementer $a_{i,j} \in F$ slik at

$$\sum_{i,j} a_{i,j}\gamma_i\delta_j = 0 \tag{1.17.3}$$

i K. Vi har at $e_j = \sum_i a_{i,j}\gamma_i$ er et element i E for hver j. Fra (1.17.3) får vi altså

$$\sum_j e_j\delta_j = 0. \tag{1.17.4}$$

Men fordi $\{\delta_j\}_{j=1,\ldots,m}$ er en basis for K over E må alle $e_i = 0$. Dvs at vi få ligninger

$$e_j = \sum_i a_{i,j}\gamma_i = 0. \tag{1.17.5}$$

Fordi $\{\gamma_i\}_{i=1,\ldots,n}$ er en basis for E over F får vi at alle $a_{i,j} = 0$. □

Eksempel 1.18. I Eksempel 1.2 hadde vi to kroppsutvidelser, hver av grad 2. Satt sammen fikk vi en kroppsutvidelse av $\mathbb{Q}$ av grad $2 \cdot 2 = 4$ med basis gitt av produktene av elementene fra de to basisene som i beviset over.

Oppgave 1.19.
(a) Finn $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}]$.
(b) Forklar hvorfor $\sqrt{3} + \sqrt{5}$ og $\frac{\sqrt{3}}{1-\sqrt{5}}$ er algebraiske over $\mathbb{Q}$.
(c) Finn $\text{grad}(\sqrt{3} + \sqrt{5}, \mathbb{Q})$.
(d) Forklar hvorfor dette viser at $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

Dette korollaret minner aller mest om Lagrange:

Korollar 1.20. *Anta F er en kropp og α er et algebraisk element i en kroppsutvidelse E. Hvis β er et element i $F(\alpha)$ så er β også algebraisk over F og graden til β deler graden til α, dvs*

$$\text{grad}(\beta, F) \,|\, \text{grad}(\alpha, F)$$

Bevis. Siden α er algebraisk er $F(\alpha)$ endeligdimensjonal over F ved Lemma 1.13. Fordi $F(\beta)$ er innholdt i $F(\alpha)$ er $F(\beta)$ også endeligdimensjonal over F og β er algebraisk over F fra Teorem 1.16. Teorem 1.17 brukt på utvidelsene $F \leqslant F(\beta) \leqslant F(\alpha)$ gir

$$[F(\alpha) : F] = [F(\alpha) : F(\beta)] \cdot [F(\beta) : F]. \tag{1.20.1}$$

Men $\text{grad}(\alpha, F) = [F(\alpha) : F]$ og $\text{grad}(\beta, F) = [F(\beta) : F]$ ved Lemma 1.13 igjen. □

Korollar 1.20 er et sterkt og nyttig resultat.

Eksempel 1.21. Ved Korollar 1.20 kan ikke kroppen $\mathbb{Q}(\sqrt[5]{2})$ ha elementer av andre grader enn 1 og 5. F. eks. ligger ikke $\sqrt[3]{2}$ i $\mathbb{Q}(\sqrt[5]{2})$ fordi $\text{grad}(\sqrt[3]{2}, \mathbb{Q}) = 3$ og 3 deler ikke 5. Elementene av grad 1 er akkurat de rasjonale tallene. Fordi $\alpha = 23 - 8(\sqrt[5]{2})^4$ ikke er et rasjonalt tall (hvorfor?) må $\text{grad}(\alpha, \mathbb{Q}) = 5$.

Oppgave 1.22 (Eksamen vår 2010, oppgave 6).
(a) La $\omega \in \mathbb{C}$ være en av røttene til polynomet $x^2 + x + 1$ (velg selv hvilken rot). Hva er graden til utvidelsen $\mathbb{Q} \leqslant \mathbb{Q}(\omega)$? Hva er graden til utvidelsen $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[3]{3})$?
(b) Hva er graden til utvidelsen $\mathbb{Q}(\sqrt[3]{3}) \leqslant \mathbb{Q}(\sqrt[3]{3}, \omega)$? Finn en basis for denne utvidelsen.
(c) Finn graden til utvidelsen $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[3]{3}, \omega)$ og finn en basis for denne utvidelsen.

Oppgave 1.23 (Eksamen vår 2010, oppgave 5).
(a) La $p(x) = x^3 - x^2 - 1$ i $\mathbb{Z}_5[x]$. Vis at $p(x)$ er et irredusibelt polynom.
(b) La $F = \mathbb{Z}_5[x]/\langle x^3 - x^2 - 1\rangle = \mathbb{Z}_5(\alpha)$ der $\alpha = x + \langle x^3 - x^2 - 1\rangle$. Hvorfor er F en kropp? Hvor mange elementer har F? Angi en basis for F over $\mathbb{Z}_5$.
(c) Uttrykk α^4, α^5 og $1/(\alpha + 1)$ ved hjelp av basisen du fant i del b.
(d) Er $x^3 - x^2 - 1$ et irredusibelt eller et redusibelt polynom i $F[x]$? Hvis det er irredusibelt forklar hvorfor. Hvis det er redusibelt, angi en faktorisering av polynomet.

Avsnitt 32: *Geometriske konstruksjoner. Dobling av kuben, kvadrering av sirkelen og tredeling av vinkelen.*

> *Stoff*: Konstruerbare tall, kroppen av konstruerbare tall, graden til et konstruerbart tall, de klassiske konstruksjonsproblemene
> *Oppgaver*: 1–4

Anta at vi har gitt et linjestykke AB og et vilkårlig positivt rasjonalt tall α. Kan vi med passer og umerket linjal konstruere et linjestykke CD slik at forholdet mellom lengden til CD og lengden til AB er α? Anta $\alpha = \frac{n}{m}$. Fra AB kunne vi prøve å konstruere et linjestykke EF som hadde n ganger lengden til AB. Deretter kunne vi fra EF prøve å konstruere et linjestykket som hadde en m-tedels lengde av EF. Hvis vi setter lengden til AB til $|AB| = 1$ er spørsmålet om vi kan konstruere linjestykker med alle rasjonale tall som lengder.

Definisjon 1.24. Gitt et linjestykke AB med lengde 1. Et reelt tall α er *konstruerbart* hvis det finnes et linjestykke med lengde $|\alpha|$ som kan konstrueres fra AB ved å bruke passer og umerket linjal et endelig antall ganger.

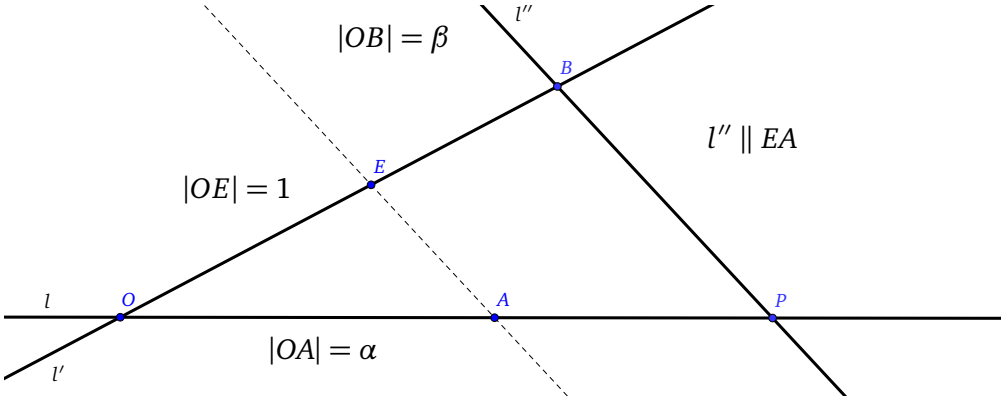
Da kan vi spørre mer generelt: Hvilke reelle tall er konstruerbare? Et mer subtilt (og matematikkhistorisk moderne) spørsmål er: Har mengden av de konstruerbare tallene en interessant struktur? Det følgende resultatet svarer på dette spørsmålet.

Teorem 1.25. *Mengden av konstruerbare tall er en underkropp av* $\mathbb{R}$.

Bevis. Gitt positive konstruerbare tall α og β må vi vise at $\alpha+\beta$, $\alpha-\beta$, $\alpha\cdot\beta$ og α/β er konstruerbare. Tallet 0 er konstruerbart og regnelovene for kropper holder fordi de holder for relle tall straks vi vet at operasjonene på mengden er lukket.
$(\alpha\cdot\beta)$: Anta linjestykket OA har lengde α. La l' være en linje gjennom O som er forskjellig fra linjen l gjennom O og A. Avsett E på l' med lengde 1 fra O og avsett B på l' med lengde β fra O og på samme side av O som E. Trekk linjen l'' gjennom B og parallell med linjen gjennom E og A. Da skjærer l'' og l i punktet P. Trekantene ΔOAE og ΔOPB er formlike. Derfor er forholdene like:

$$\frac{|OP|}{\alpha}=\frac{|OP|}{|OA|}=\frac{|OB|}{|OE|}=\frac{\beta}{1} \tag{1.25.1}$$

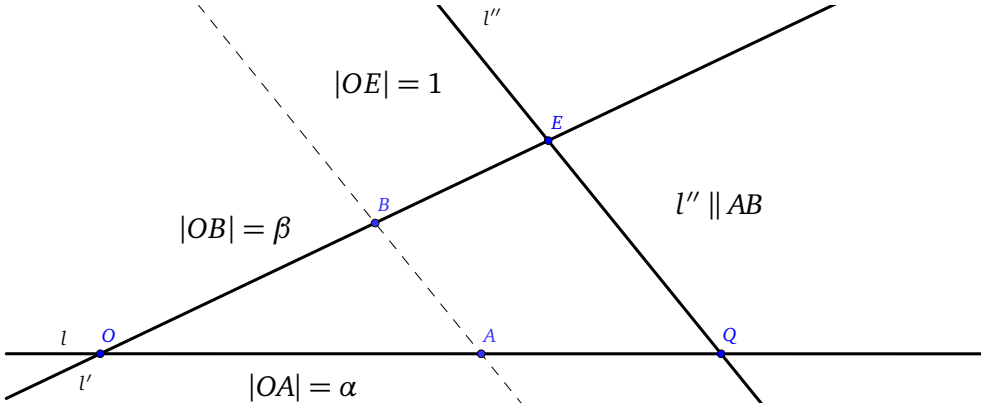
Altså er $|OP|=\alpha\cdot\beta$ et konstruerbart tall.



(α/β): Anta linjestykket OA har lengde α. La l' være en linje gjennom O som er forskjellig fra linjen l gjennom O og A. Avsett E på l' med lengde 1 fra O og avsett B på l' med lengde β fra O og på samme side av O som E. Trekk linjen l'' gjennom E parallell med linjen gjennom A og B. Da skjærer l'' og l i punktet Q. Trekantene ΔOAB og ΔOQE er formlike. Derfor er forholdene like:

$$\frac{\alpha}{\beta}=\frac{|OA|}{|OB|}=\frac{|OQ|}{|OE|}=|OQ| \tag{1.25.2}$$

Altså er $|OQ|=\alpha/\beta$ er et konstruerbart tall.



Addisjon og subtraksjon overlates til leseren. □

Spesielt innholder altså de konstruerbare tallene de rasjonale tallene.

Spørsmål 1.26. Hvorfor?

Så hvilke andre reelle tall (enn de rasjonale) har kroppen av de konstruerbare tallene?

Teorem 1.27. *Et tall α er konstruerbart hvis α kan lages fra rasjonale tall ved å bruke operasjonene kvadratrot (av positivt tall), addisjon, subtraksjon, multiplikasjon og divisjon et endelig antall ganger.*

Bevis. La F betegne mengden av tall som kan konstrueres på den måten som beskrives i teoremet. Da er F en kropp. La K betegne kroppen av konstruerbare tall.
Vi viser først at K er innholdt i F.
Med passer-og-linjalkonstruksjoner konstruerer man punkter i planet som er skjæringspunkter mellom
(1) to linjer
(2) en linje og en sirkel
(3) to sirkler
Linjer er gitt at to punkter og sirkler av et punkt (sentrum) og en lengde (radius). Disse punktene skal ha koordinater i K og radius skal også være et tall i K. Anta koordinatene og radius også ligger i F. Er det da mulig med konstruksjonene (1-3) å konstruere punkter og lengder som ikke ligger i F? (Dette er det essensiell spørsmålet siden konstruksjonene av K og F begge tar utgangspunkt i $\mathbb{Q}$.)
Hvis A og B er punkter i planet med koordinater i $K \cap F$, vil avstanden mellom dem være gitt ved Pytagoras setning, dvs som en kvadratrot av et tall i $K \cap F$ som altså er et tall i F per definisjon av F. En linje gjennom A og B vil være beskrevet av en lineær ligning i x og y med koeffisienter i A og B fra topunktsformelen. En sirkel er gitt ved en kvadratisk ligning i x og y med koeffisienter i $K \cap F$. Ny punkter vil dermed ha koordinater som er gitt som løsninger på ligningssytemer med to slike ligninger:
(1) to lineære ligninger
(2) en lineær og en kvadratisk ligning
(3) to kvadratiske ligninger

I tilfelle (1) vil løsningen være gitt som et rasjonalt uttrykk med tall fra F, tenk f. eks. på Cramers regel. Fordi F er en kropp vil dette gi løsninger i F.

I tilfelle (2) vil løsningene være gitt ved abc-formelen hvor a, b og c vil være rasjonale uttrykk i tall fra F og altså gi løsninger i F per definisjon av F.

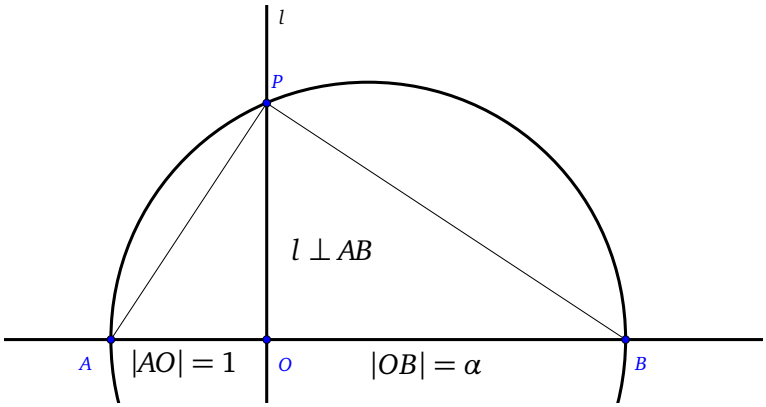
I tilfelle (3) vil løsningene være gitt som i tilfelle (2).

Konklusjon: Vi kommer ikke utenfor F ved passer-og-linjalkonstruksjoner. Altså har vi vist at K er innholdt i F.

Nå viser vi at alle kvadratrøtter av positive tall i K finnes i K. Fordi K er en kropp vil dette bety at F er innholdt i K. Anta $\alpha \in K$ og $\alpha > 0$. La AB være et linjestykke med lengde $\alpha + 1$. La O på dette linjestykket ligge 1 fra A. Oppreis normalen l på AB i O. La P være et av skjæringspunktene mellom l og sirkelen med diameter $\alpha + 1$ som går gjennom A og B. Ved Thales' setning er trekant ΔABP rettvinklet og dermed formlik med trekantene ΔAPO og ΔPBO. Derfor er forholdene like:

$$|OP| = \frac{|OP|}{|OA|} = \frac{|OB|}{|OP|} = \frac{\alpha}{|OP|} \tag{1.27.1}$$

dvs $|OP|^2 = \alpha$, så $\sqrt{\alpha}$ er et konstruerbart tall.



Dermed har vi også vist at F er innholdt i K. Altså er $K = F$. □

Korollar 1.28. *Hvis γ er et konstruerbart tall finnes det en følge av kroppsutvidelser $\mathbb{Q} = F_0 \leqslant F_1 \leqslant \ldots \leqslant F_n$ slik at $\gamma \in F_n$ og $[F_{i+1} : F_i] = 2$ for alle $i = 0, \ldots, n-1$. Spesielt vil $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2^r$ for et tall r med $0 \leqslant r \leqslant n$.*

Bevis. Følgen av kroppsutvidelser følger av Teorem 1.27, med en mulig ny kroppsutvidelse for hver ny kvadratrot som brukes i konstruksjonen av γ. Fra Teorem 1.17 får vi at $2^n = [F_n : \mathbb{Q}] = [F_n : \mathbb{Q}(\gamma)] \cdot [\mathbb{Q}(\gamma) \cdot \mathbb{Q}]$ □

Nå skal vi høste av denne teoriutviklingen. Korollar 1.28 medfører at de klassiske konstruksjonene er umulige.

Teorem 1.29 (Dobling av kuben)**.** *Med passer og umerket linjal er det umulig å konstruere sidekanten i en kube med volum 2.*

Bevis. Sidekanten må ha lengde $\sqrt[3]{2}$ som er en rot i polynomet $x^3 - 2$ som er irredusibelt ved Eisensteinkriteriet med $p = 2$. Dermed er $\text{grad}(\sqrt[3]{2}, \mathbb{Q}) = 3$, dvs $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Ved Korollar 1.28 kan ikke $\sqrt[3]{2}$ være konstruerbart. □

Teorem 1.30 (Tredeling av vinkelen)**.** *Med passer og umerket linjal er det umulig å konstruere en vinkel på* 20^o.

Bevis. Hvis en vinkel på 20^o kan konstrueres så er $\cos 20^o$ et konstruerbart tall (sjekk!). Vi viser at $\cos 20^o$ ikke er et konstruerbart tall. Vi har generelt at

$$\begin{aligned}\cos 3\theta + i\sin 3\theta = e^{i\cdot 3\theta} = (e^{i\cdot\theta})^3 = (\cos\theta + i\sin\theta)^3 \\ = \cos^3\theta - 3\cos\theta\sin^2\theta + i(3\cos^2\theta\sin\theta - \sin^3\theta)\end{aligned} \tag{1.30.1}$$

Altså er $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$. Med $\theta = 20^o$ og $\alpha = \cos 20^o$ får vi etter multiplikasjon med 2 ligningen

$$\begin{aligned} 8\alpha^3 - 6\alpha - 1 &= 0 \\ &\quad \text{vi substituerer } \alpha = y/2 \text{ og får ligningen} \\ y^3 - 3y - 1 &= 0 \\ &\quad \text{vi substituerer } x = y + 1 \text{ og får ligningen} \\ x^3 + 3x^2 - 3 &= 0 \end{aligned} \tag{1.30.2}$$

Eisensteinkriteriet med $p = 3$ gir at $x^3 + 3x^2 - 3$ er irredusibelt. Altså er også $8\alpha^3 - 6\alpha - 1$ irredusibelt (vi tenker for et øyeblikk at α er en variabel), altså er $\text{grad}(\alpha, \mathbb{Q}) = 3$, dvs $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Ved Korollar 1.28 kan ikke $\alpha = \cos 20^o$ være konstruerbart. □

Fordi 60^o er en vinkel som *kan* konstrueres kan ved Teorem 1.30 ikke alle konstruerbare vinkler tredeles med passer og linjal.

Oppgave 1.31. La $\theta = 72^o$ og sett $\alpha = \sin\theta$.
(a) Vis at α er en rot til polynomet $16x^4 - 20x^2 + 5$. (Bruke trigonometriske identiteter til å uttrykke $0 = \sin 5\theta$ ved hjelp av $\sin\theta$)
(b) Bruk (a) til å vise at den regulære 5-kanten er konstruerbar med passer og linjal.

Teorem 1.32 (Kvadrere sirkelen)**.** *Med passer og umerket linjal er det umulig å konstruere et kvadrat med samme areal som en sirkel med radius* 1.

Bevis. Sidenkanten i kvadratet må ha lengde $\sqrt{\pi}$. Hvis dette tallet er konstruerbart er også π konstruerbart ved Teorem 1.25. Spesielt må π være et algebraisk tall ved Korollar 1.28 og Teorem 1.16. Men Lindemann har vist at π er transcendent. □

Her bruker vi Lindemanns resultat. Men uten å vite at de konstruerbare tallene er algebraiske hjelper ikke Lindemann.

1.2 Når har en gruppe en undergruppe?

Avsnitt 36: *Sylows teoremer*

> *Stoff*: Eksistens av Sylow p-grupper (Sylows første teorem), alle Sylow p-grupper er konjungerte (Sylows andre teorem), hvor mange Sylow p-grupper kan det være? (Sylows tredje teorem)
> *Oppgaver*: 1–6, 10, 12, 13, 17–19

Lagrange' teorem sier at hvis H er en undergruppe av en endelig gruppe G så må ordenen $|H|$, dvs antall elementer i H dele $|G|$. Dette resultatet begrenser hvilke mulige undergrupper en endelig gruppe kan ha bare ved å bruke ordenen til gruppen. Men hva med det omvendte spørsmålet: Hvis n deler $|G|$, har G da en undergruppe av orden n? Dette er generelt et mye vanskeligere spørsmål. Men for endelige abelske grupper er svaret faktisk ja. Dette følger av klassifikasjonsteoremet for endeliggenererte abelske grupper som reduserer gruppens struktur til primtallsfaktoriseringen av $|G|$ og de ulike mulige abelske gruppene av orden p^n hvor p er prim. Men det finnes ikke alltid undergrupper hvis G ikke er abelsk.

Eksempel 1.33. La $G = A_4$, gruppen av jevne (alternerende) permutasjoner av fire elementer. Fordi $|G| = 12$ er 6 er en divisor i $|G|$. Påstand: G har ingen undergruppe av orden 6. Anta H er en slik undergruppe. Da må H være en normal undergruppe av G fordi det bare er to restklasser: $\sigma H = H$ hvis $\sigma \in H$, men σH er komplementet til H hvis $\sigma \notin H$, dvs $\sigma H = G \setminus H$. Det samme gjelder for de høyre restklassene, altså er $\sigma H = H\sigma$ for alle $\sigma \in G$ og dette er en av karateriseringene av en normal undergruppe. Altså er kvotienten G/H en gruppe med to elementer: $G/H = \{H, \sigma H\}$ for en $\sigma \in G \setminus H$ og G/H er isomorf med $\mathbb{Z}_2$ pga fundamentalteoremet for endelige abelske grupper. Siden H er en undergruppe vil $\tau \in H$ medføre at τ^2 også et element i H. Fra multiplikasjonen i G/H har vi $\sigma H *_{G/H} \sigma H = H$. Altså vil alle $\rho \in \sigma H$ også gi $\rho^2 \in H$. Så alle kvadrater av permutasjoner i $G = A_4$ er elementer i H. Vi ramser opp noen:

1. $(1,3,2)^2 = (1,2,3)$
2. $(1,2,3)^2 = (1,3,2)$
3. $(1,4,2)^2 = (1,2,4)$
4. $(1,2,4)^2 = (1,4,2)$
5. $(1,3,4)^2 = (1,4,3)$
6. $(1,4,3)^2 = (1,3,4)$
7. $(2,3,4)^2 = (2,4,3)$
8. $(2,4,3)^2 = (2,3,4)$

Dette gir 8 ulike elementer i H i tillegg til identiteten. Dette er en motsigelse.

Vi må derfor begrense oss når vi leter etter undergrupper. Denne definisjonen vil gi den riktige begrensningen:

Definisjon 1.34. Anta p er et primtall. En gruppe kalles for en *p-gruppe* hvis alle elementer i gruppen har orden lik potenser av p. En undergruppe H av en gruppe G er en *p-undergruppe av G* hvis H selv er en p-gruppe.

Lemma 1.35. *Anta G er en endelig gruppe og p et primtall. Da er G en p-gruppe hvis og bare hvis $|G|$ er en potens av p.*

Ved Lagrange er naturligvis G en p-gruppe hvis $|G| = p^n$. Men det omvendte er ikke opplagt.

Teorem (Sylows første teorem)**.** *Anta p er et primtall og G er en endelig gruppe av orden $|G| = p^n \cdot m$ hvor $n \geqslant 1$ og p ikke deler m. Da gjelder:*

(i) *For hver i med $1 \leqslant i \leqslant n$ finnes det en undergruppe av G med orden p^i.*

(ii) *For hver i med $1 \leqslant i \leqslant n-1$ og hver undergruppe H av orden p^i har G en undergruppe H' av orden p^{i+1} slik at H er en normal undergruppe av H'.*

Definisjon 1.36. Anta p er et primtall og G en endelig gruppe. En undergruppe H kalles for en Sylow p-undergruppe hvis H er en maksimal p-undergruppe.

Sylows første teorem sier at hvis p deler ordenen til gruppen G så har G en Sylow p-undergruppe og ordenen til denne er den største potensen av p som deler $|G|$.

Teorem (Sylows andre teorem)**.** *Hvis H_1 og H_2 er to Sylow p-undergrupper av G finnes det et element g i G slik at $H_2 = gH_1g^{-1}$.*

Vi sier at H_1 og H_2 er *konjungerte* undergrupper.

Teorem (Sylows tredje teorem)**.** *Anta p er et primtall som deler ordenen til gruppen G. La m være antall Sylow p-undergrupper i G. Da gjelder:*

$$m \equiv 1 \pmod{p} \quad \text{og} \quad m \text{ deler } |G|$$

Legg merke til at hvis $|G|$ er en potens av p er det bare en Sylow p-undergruppe, nemlig G selv. Sylows andre og tredje teorem gir da ingenting.

Eksempel 1.37. La oss først se hva Sylows teoremer gir for en endelig abelsk gruppe (hvor vi altså påstår at disse resultatene følger av klassifikasjonsteoremet). La $G = \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Da har vi $|G| = 24$. Vi velger $p = 2$. Sylow 1(i) sier da at det finnes undergrupper av orden 2, 4 og 8. F. eks.

- $H_1 = \{0\} \times \{0\} \times \{0\} \times \mathbb{Z}_2$
- $H_2 = \{0\} \times \{0\} \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- $H_3 = \{0\} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Undergruppene er nøstet: $H_1 \leqslant H_2 \leqslant H_3$ slik som i Sylow 1 (ii). Gruppe H_i er normal i H_{i+1} fordi i en abelsk gruppe er alle undergrupper abelske og spesielt normale. Sylow 1(ii) holder derfor.

Sylows andre teorem sier at alle undergruppene av orden 8 er konjungerte. Men siden alle undergrupper er normale kan det ved Sylows andre teorem altså bare være en Sylow 2-undergruppe i G. Dette passer godt med Sylows tredje teorem.

Hvis vi istedet betrakter $G' = \mathbb{Z}_3 \times \mathbb{Z}_8$ har vi $|G'| = 24$ som før, men gruppene er ikke strukturlike (det vet vi fra klassifikasjonsteoremet). Sylows teoremer utaler seg om hvordan de allikevel ligner fordi de har samme orden. Vi finner nøstede undergrupper av orden 2, 4 og 8:

- $H_1' = \{0\} \times 4\mathbb{Z}_8$
- $H_2' = \{0\} \times 2\mathbb{Z}_8$
- $H_3' = \{0\} \times \mathbb{Z}_8$

Ved Sylows andre teorem finnes det ingen andre undergrupper av orden 8 enn H_3'.

Oppgave 1.38. Finn hvor mange Sylow 3-undergrupper G og G' har henholdsvis.

Oppgave 1.39. Finn hvor mange Sylow 3-undergrupper A_4 har. Er noen av disse normale?

Oppgave 1.40. Anta G er en gruppe med 51 elementer. Finn hvor mange Sylow 17-undergrupper G kan ha. Er noen av disse normale? Finn hvor mange Sylow 3-undergrupper G kan ha. Er noen av disse normale?

Oppgave 1.41. Anta gruppen G har 66 elementer. Forklar hvorfor G må ha en normal Sylow 11-undergruppe. Hvor mange Sylow 3-undergrupper kan G ha? Hvor mange Sylow 2-undergrupper kan G ha?

VID-MAUMAT 2. semester våren 2014

I hvilken grad du fornøyd med de praktiske rammene for studiet i vår, f.eks. informasjon, tid og sted for samlinger, studieveiledning, systemer som Mi side og StudentWeb?

- Svært fornøyd
- Godt fornøyd! Torsdag-lørdag samlingene passer godt både for meg og arbeidsgiver. Da dette nå blir onsdag-fredag er jeg redd for at jeg ikke vil få innvilget alle disse dagene.
- god inf
- Mi side er ikke et særlig godt system - men det funker helt ok. Informasjon har vært bra. Jeg er veldig glad for at alle samlingene blir på hverdager til høsten!
- I det store og heile bra. Einaste negative er at det var noko krøkete å finne fram til vurderingane på miside
- Veldig fornøyd
- Informasjonen er tilstrekkelig, men de elektroniske systemene oppleves som tungrodde. StudentWeb fungerer men fremstår som vanskelig å forstå og vanskelig tilgjengelig.

Hvor mange prosent stilling har du ved siden av studiet i vår?

- 100%
- 100
- 100
- 120%
- 107
- 100
- 125%

Har du mottatt noe støtte f.eks. fra videreutdanningsprogrammet Kompetanse for kvalitet, som kan brukes til frikjøp fra lærerjobb?

- Nei
- Nei
- nei
- nei. Men jeg får neste år.
- Ikkje dette semesteret, men dei to neste er eg frikjøpt gjennom Kompetanse for kvalitet.
- Nei, men får det neste skoleår.
- Nei

Hvor mange av samlingene har du deltatt på?

- Alle, men kunne ikke delta to lørdager
- Alle
- 4
- alle
- Alle, med unntak av dei to siste dagane på første samling.
- alle
- 4

Gi kommentarer til opplegg og innhold på samlingene, samt oppfølging i periodene mellom samlingene.

- Opplegg og innhold har vært svært bra! Engasjerte og faglig dyktige forelesere i begge fagene, interessante og lærerrike samlinger!
- Godt opplegg. Litt krevende pensum i Algebra, men ellers bra.
- Angående diff likninger aå kunne det med fordel vært lagt ut videoløsninger av flere oppgaver. Hadde det vært slike av alle oppgavene så hadde det ikke vært nødvendig med forelesninger
- Jeg synes de funker bra - hoppet av algebraen halvveis fordi jeg hadde for mye å gjøre med mer enn full jobb og differensialligningene i tillegg, så kan ikke uttale meg så mye om det, funket bra så lenge jeg hang med.

  Forelesningene i Maumat 643 (historie)har vært gode og interessante, og det er kjekt at de punktene som ikke fungerte så godt i høst har fungert supert i vår, som oppg. i god tid osv.

  jeg syns kanskje at arbeidskravene er i overkant til 5 studiepoeng.
- Det har vore svært gode og engasjerte forlesarar, som begge har vore lett å få tak ved behov. Eg tykkjer likevel at arbeidsmengda i Maumat 644 ikkje står i samsvar med talet på studiepoeng. To store innleveringar og ein skuleeksamen er for mykje for berre 5 studiepoeng. Faget sin natur tilseier og,etter mi meining, at ein heimeeksamen er ei betre løysing enn skuleeksamen.

Fra konteksten: Dette gjelder 643, ikke 644 (skrivefeil).

- Gode forelesninger.
  Veldig gode kompendier i MAUMAT 644
  MAUMAT 643 er egentlig for stort for 5 sp. Men opplegget med oppgaver og Mappeinnleverimng og frister var bra nå i vår.

Opplever du at du har tilstrekkelig bakgrunn i matematikk for å ta MAUMAT643 og MAUMAT644?

- Ja.
- Ja
- ja
- ja.
- Ja
- Ja. Jeg har kjent på at jeg skulle vært noe bedre i linær algebra.

Har du andre kommentarer, råd, ønsker for høstsemesteret,...?

- Jeg har til nå hatt Kirfel, Ihle og Christensen som faglærere, alle tre svært dyktige. Kunne gjerne ønsket en eller flere av dem i flere fag.
- Ønsker: torsdag-lørdag samlinger. Dette gjør det enklere for de som ikke mottar noen støtte til å få tilatelse fra jobben til å reise på samlingene. Og man føler ikke at man "mister" for mye tid med elevene.
- Fint om vi snart får vite klokkeslett for samlingene til høstsemester slik at transport kan bestilles
- Jeg er glad for at samlingene blir på hverdager.

  Jeg er litt skeptisk til at det legges så stor vekt på differensialligninger - det er et marginalt område i skolematematikken og er kun relevant i R2. Er også litt skeptisk til samarbeid da studentene bor så spredt og har så ulike ordninger for studiene. Men det skal vel gå.
- Eg har eit strekt ønskje om at didaktikkdelen i Maumat 645 vert tona ned så mykje som råd saman med eit tilsvarande auka fokus på matematikk. Aller helst såg eg at didaktikken vart fjerna heilt. Grunnen for dette er at eg etter 15 år som lærar meiner eg er i stand til å ta dei relevante didaktiske grepa der det er behov,og når det er behov.
  Det eg har lyst til er å lære meir matematikk.
- MAUMAT 643 hevet seg på system, rammer og tidsfrist fra MAUMAT 642, så det var bra! MAUMAT 644 var et virkelig godt gjennomført kurs. Siden dette siste kurset er vanskelig er nok det nødvendig for at vi studenter skal kunne lykkes godt.

Vår 2015.

I hvilken grad du fornøyd med de praktiske rammene for studiet i vår, f.eks. informasjon, tid og sted for samlinger, studieveiledning, systemer som Mi side og StudentWeb?

- Veldig fornøyd, vet på forhånd hva som skjer.
- Godt fornøyd
- Veldig bra. Flott at man kan bruke deler av helger til samlinger slik at belastningen ikke blir så stor for elevene om man er borte fra jobb.
- Veldig fornøyd- Litt kronglete på VilVite når vi ikke kommer inn med kortene våre
- Meget fornøyd.

Hvor mange prosent stilling har du ved siden av studiet i vår?

- 62,5
- 100
- 78 %
- 100
- ca 70

Har du mottatt noe støtte f.eks. fra videreutdanningsprogrammet Kompetanse for kvalitet, som kan brukes til frikjøp fra lærerjobb?

- Har mottatt 37,5% frikjøp
- Nei
- Ja, jeg har fått 100000 i stipend
- Nei
- Full støtte.

Hvor mange av samlingene har du deltatt på?

- Alle
- 2
- alle
- Alle
- 4

Gi kommentarer til opplegg og innhold på samlingene, samt oppfølging i periodene mellom samlingene.

- Greit nok. Har kun tatt et fag denne våren.
- Veldig bra
- Flinke og engasjerte forelesere. En del krevende innleveringer, men god oppfølging, spesielt på MAUMAT 644
- Veldig flink foreleser. Tydelige kommentarer og tilbakemeldinger. Litt lite tid til eksempler på samlingene, slik at innleveringene ble meget tøffe.
  Stort pensum til 10 stp.

Opplever du at du har tilstrekkelig bakgrunn i matematikk for å ta MAUMAT643 og MAUMAT644?

- Ja
- Ja
- Ja
- Ja
- JA. Har tatt mye av fagene før. Men fint med oppfrisking. Også en del nytt i 644.

Har du andre kommentarer, råd, ønsker for høstsemesteret,...?

- Ser at samlingene nå ligger onsdag-fredag, noe som gir større belastning for skolen i form av vikarutgifter, og for elevene. Jeg er sosialrådgiver i tillegg og mister mye rådgivertimer der jeg skal være tilgjengelig for elevene. Ingenting å gjøre noe med nå, men det kan være lurt å tenke på senere. Min skole ble ikke superbegeistret og jeg tror at det er vanskeligere å få støtte for

utdanningen dersom dette blir det vanlige tidspunktet for samlinger i resten av studiet. Det er også uheldig med start på første samling 1.skoleuka på høsten. Det blir en dårlig oppstart for elevene når læreren er borte nesten hele uka. Det er det også for sent å gjøre noe med. Vet det er et puslespill å få til dette.

- Ønsker mulighet til å begynne å "tenke" på masteroppgave.

Utdanning

Studieplan for VID-MAUMAT Erfaringsbasert master i undervisning med fordjupning i matematikk (/nb/studieprogram/VID-MAUMAT), vår 2015

Omfang og studiepoeng

Studiet er organisert som eit deltidsstudium på til sammen 120 studiepoeng der ein føreset at det vert avlagt eksamen i 15 studiepoeng pr. semester. Normert studietid er 3,5-4 år. Undervisninga er organisert som kombinasjon av nettkommunikasjon og samlingar. Sjå elles opplegg for einskilde emne i studiet.

Det inngår 3-4 samlingar pr. semester. Kvar samling er 2-3 dagar (torsdagar og fredagar, samt enkelte laurdagar).

Studiestart - semester

Haust

Hausten 2015 vil førstesemesteremna MAUMAT641 (/nb/emne/MAUMAT641) og 642 ha samlinger torsdag-laurdag i veke 35, 38, 43 og 46. Torsdagar kl 10.00-16.00 og kl 09.00-15.00 på fredagar og laurdagar.

Mål og innhald

Masterstudiet i undervisning med fordjuping i matematikk er eit toårig studium der målet er å vidareutdanne lærarar for mellomtrinnet og ungdomstrinnet i grunnskulen og for den vidaregåande skulen.

Gjennom masterstudiet skal studentane tileigne seg teoretisk og erfaringsbasert kunnskap og dugleik som kan bidra til å utvikle deira kompetanse for å undervise i matematikk i skulen. Studiet har ei innretning som er relatert til praksis i skulen, og det er ei overordna målsetjing å kunne byggje bru mellom erfaringskunnskap frå matematikkfaget i skulen, den forskingsbaserte disiplinkunnskapen i matematikkfaget og den fagdidaktiske kunnskapen. Alle emne i studiet skal bidra til auka dugleik og refleksjon i høve til å undervise faget og kunne leggje til rette for at elevar kan lære i faget.

Studiet er praksisnært og masteroppgåva skal vere fagdidaktisk.

Programmet har tre delar: fellesemne, fag/ fagdidaktiske emne og masteroppgåve.

1. Profesjon, refleksjon og erfaringsdeling, fellesseminar, del av masteroppgåva
2. Faglige og fagdidaktiske emne på 200- og 300-nivå, 45 studiepoeng
3. Vitskapleg metode og vurderingsteori, fellesemne 15 studiepoeng

4. Forskingsbasert masteroppgåve 60 studiepoeng

Studiet vil gi ei innføring i vitskapelege arbeidsmåtar og forskingsmetodar knytte til masterfaget, og inneheld trening i sjølvstendig arbeid med faglege oppgåver. Studiet skal dessutan gi ei grunnleggjande forståing av matematikkfaget i ein samfunnsmessig og kulturell samanheng.

I studiet vert det lagt vekt på å utvikle kompetanse til vidare fagleg og profesjonell utvikling, slik at studentane kan bidra til å vidareutvikle matematikkfaget. Såleis er det eit mål å fremje kritisk refleksjon og samtalekulturar kring fag, undervisning og læring.

Studentane skal gjennom det faglege innhaldet få møte fordjupingsemne innanfor matematikk og matematikkhistorie slik at dei kan få eit teoretisk grunnlag for å gå vidare med masteroppgåvene.

Læringsutbyte

A) Fagleg kunnskap

Studentane skal

- ha tileigna seg den matematikkunnskapen som gjeld i studiet og kunne relatere denne til skulematematikken
- ha utvikla ei sjølvstendig og kritisk haldning til innhaldet i skulematematikken og til den rolla faget spelar i skulen og i samfunnet
- kunne gjere greie for og drøfte grunnlagsspørsmål og teoriar i matematikkdidaktikk, og bruke det som grunnlag for kritisk refleksjon over eigen undervisningspraksis og tilrettelegging for elevars læring
- kunne planleggje og gjennomføre eit matematikkdidaktisk masterprosjekt på ein sjølvstendig og systematisk måte i tråd med gjeldande forskingsetiske normer

B) Tilrettelegging for elevars læring i faget

Studentane skal

- kunne undersøke læring i eige klasserom i matematikkundervisninga ved hjelp av fagkunnskap og fagdidaktisk teori og presentere refleksjon over dette
- kunne vurdere læremiddel og arbeidsformer i matematikk i høve til dei ulike emna i skulefaget, og kunne grunngi val og vurderingar i høve til kunnskap om fag og fagdidaktikk, og eige fagsyn.

Opptakskrav

Søkjarane må ha

- lærarutdanning; allmennlærarutdanning eller bachelor/cand.mag+PPU (eller tilsvarende).
- Matematikkdidaktikk fra allmenn-/grunnskolelærarutdanning eller PPU (eller tilsvarande)
- Minst 60 studiepoeng matematikk på universitetsnivå. Dei 60 studiepoenga må dekke fagstoff tilsvarande MAT111 (/nb/emne/MAT111), MAT112 (/nb/emne/MAT112), MAT121 (/nb/emne/MAT121) og deler av MAT131

(/nb/emne/MAT131).
- Minimum 2 års relevant undervisningserfaring

Obligatoriske emne

I kursdelen i programmet inngår sju obligatoriske emne:

- Matematikkens historie - matematikken i oldtida (5 sp)
- Matematikkens historie - matematikken i nyare tid (5 sp)
- Diskret matematikk (10 sp)
- Algebra (10 sp)
- Didaktisk modellering (15 sp)
- Metodekurs i utdanningsforskning (15 sp)

I tillegg kjem masteroppgåva på 60 studiepoeng. Seminaret Profesjon, refleksjon og erfaringsdeling er eit obligatorisk seminar som strekkjer seg over fleire semester av studiet. Seminaret utgjer undervisningsdelen av arbeidet med masteroppgåva og skal munne ut i ei prosjektskisse til masteroppgåva. Prosjektskissa for masteroppgåva skal vere godkjent før sjølve arbeidet med masteroppgåva tek til.

Rekkefølgje for emne i studiet

Studiet er organisert som eit deltidsstudium der føresetnaden er at studentane tek 15 studiepoeng kvart semester.

Masterstudiet med fordjuping i matematikk har følgjande emne:

1. semester (haust):

- Matematikkens historie - matematikken i oldtida (5 sp)
- Diskret matematikk (10 sp)

2. semester(vår):

- Matematikkens historie - matematikken i nyare tid (5 sp)
- Algebra (10 sp)

3. semester(haust)

- Didaktisk modellering (15 sp)

4. semester (vår) fellesemne:

- Metodekurs i utdanningsforskning (15 sp)

5. - 8. semester

Masteroppgåve (60 sp)

Krav til progresjon i studiet

Emna i kursdelen må avleggjast og gjennomsnittleg karakter på emna i kursdelen må ikkje vere dårlegare enn C for å ta til med skriving av sjølve masteroppgåva i

femte semester av studiet.

Prosjektskissa knytt til fellesseminaret "Profesjon, refleksjon og erfaringsdeling" må også vere godkjent før arbeidet med sjølve masteroppgåva tek til.

Undervisningsmetodar

Undervisninga er forskingsbasert og omhandlar det teoretiske grunnlaget for faget, så vel som fagets metodar. Studenten skal gjennom studiet få møte ulike undervisningsmetodar, t.d. førelesingar, seminar, gruppearbeid, skriftlege og munnlege presentasjonar, omgreps- og problemfokuserte oppgåve, skriveoppgåver, rettleiing og praktisk bruk av digitale verkty. For nærmare informasjon, sjå dei einskilde emneplanane. Ein viktig del av arbeidet i studiet vil skje gjennom nettbasert kommunikasjon.

Eit gjennomgåande trekk ved undervisninga skal vere å kombinere tileigning av fagleg kunnskap med kompetanse i å kunne leggje til rette for elevars læring og utvikling.

I tillegg til den undervisninga som vert tilbydd, vert studentane oppmoda om også sjølve å organisere eigne kollokviegrupper og skrivegrupper.

Relevans for arbeidsliv

Fullført og greidd studium kvalifiserer som lektor i matematikk med høve til å undervise i 5.-10. trinnet i grunnskulen og i vidaregåande skule.

Evaluering

Evaluering blir gjennomført i tråd med Universitetet i Bergen sitt kvalitetssikringssystem. Det kan nyttast ulike evalueringsformer.

Programansvarleg

Matematisk institutt, Det matematisk-naturvitskaplige fakultetet, Universitetet i Bergen

Adminstrativt ansvarleg

Senter for etter- og videreutdanning, via.uib.no og Matematisk institutt, www.uib.no/math

Dersom du har spørsmål om programmet, ta gjerne kontakt med studieveileder for programmet, studieveileder@math.uib.no, 55 58 28 41.