1 Sætninger om hovedidealområder (PID) og faktorielle ringe (UFD)

1. Introducér **ideal**, **hovedideal**
2. I kommutativt integritetsområde R introduceres **primelement**, **irreducibelt element**, **association**
3. Begrebet **PID (hovedidealområder)** introduceres. I forbindelse med dette nævnes eksempler på hovedidealområder: $\mathbb{Z}$, $L[X]$, og den **numeriske betingelse for PID** nævnes (euklidisk ring)
4. I **PID** er irreducible elementer primelementer (nævn, at det er nemt at vise, at primelementer er irreducible i komm. int. omr.)
5. Introducér **primopløsninger** og **irreducible opløsninger** (en fremstilling med faktorer i R, hvor faktorer er enten primelementer el. irreducible elementer)
6. Nævn, at primopløsninger er entydige (hvis to produkter af primelementer $a_1 \cdots a_s$ og $b_1 \cdots b_t$ er associerede, er $s = t$ og hver faktor a_i er associeret med b_i efter permutation af faktorer, $i = 1, \ldots, s$)
7. Bevis **hovedsætning 1:** I komm. int. omr. R er følgende betingelser ækvivalente:
   (a) Irred. opløsninger eksisterer for alle elt. $\neq 0$, enhed og disse er entydige.
   (b) Irred. opløsninger eksisterer for alle elt. $\neq 0$, enhed og alle irred. elt. er primelt.
   (c) Primopløsninger eksisterer for alle elt. $\neq 0$, enhed.

   Vis $(b) \Rightarrow (c)$, $(b) \Rightarrow (a)$, $(c) \Rightarrow (b)$ og $(a) \Rightarrow (b)$. Hvis følgende betingelser (dvs. én af dem) er opfyldt i en ring R, kaldes R **UFD (faktoriel ring)**
8. Nævn, at hvis der ikke eksisterer irred. opl. for alle elementer i et komm. int. omr., findes en uendelig følge af elementer i R $a_1, a_2, \ldots$, hvor a_{i+1} er en ikke-triviel divisor i a_i
9. **Hovedsætning 2: Et PID er et UFD.**
10. *Småting:* I UFD kan laves repræsentantsystem af primelementer, hvorpå ethvert element kan skrives som produkt af enhed og primelementpotenser. Er R faktoriel, er $R[X]$ også faktoriel (Gauss' sætning). Gauss' talring er PID, dermed UFD, og der findes kun 9 imaginære faktorielle kvadratiske talringe.

2 Kvadratiske talringe, fortrinsvist om irreducible opløsninger, primelementer og faktorielle, kvadratiske talringe

1. Introducér **kvadratiske talringe** $\mathbb{Z}[\xi]$ (normeret andengradspolynomium med heltalskoefficienter, kvadratfri diskriminant, (irrationale) rødder ξ, kvadratisk tal $x + y\xi$, mængden af disse $\mathbb{Z}[\xi]$)

2. **Norm** (multiplikativ, heltallig etc.), **irreducibelt element** og **primelement**

3. **Nævn** ε enhed i $\mathbb{Z}[\xi] \Leftrightarrow N(\varepsilon) = \pm 1$ og $\delta|\alpha \Rightarrow N(\delta)|N(\alpha)$, δ triviel divisor i $\alpha \Leftrightarrow N(\delta)$ triviel divisor i $N(\alpha)$

4. Vis lemma 6.14: lad $\pi = x + y\xi \in \mathbb{Z}[\xi]$, hvor $(x, y) = 1$. Da gælder π primelement i $\mathbb{Z}[\xi] \Rightarrow N(\pi) = \pm p$, p primtal $\Rightarrow \pi$ irreducibel i $\mathbb{Z}[\xi]$. Betingelserne er ækvivalente, hvis $\mathbb{Z}[\xi]$ er UFD

5. I en kvadratisk talring eksisterer **irreducible opløsninger** for alle elementer; de er bare **ikke altid entydige** (vælg eksempel $\mathbb{Z}[\sqrt{-5}]$ med $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$) (ikke alle kvadr. talringe er **UFD**)

6. Vis, at hvis p er et sædvanligt primtal i $\mathbb{Z}$ og et primelement i $\mathbb{Z}[\xi]$, så har kongruensen $z^2 - bz + c \equiv 0 \pmod{p}$ ingen løsninger i $\mathbb{Z}$ (6.19)

7. Skitser beviset for, at $\mathbb{Z}[i]$ er et UFD (foregår ved at vise, at $\mathbb{Z}[i]$ er en euklidisk ring) - rund af med lidt om **forgrening** og løsning på **diofantisk ligning** $x^2 + y^2 = p$, hvor p enten er et primtal eller ej

3 Kvadratiske talringe, fortrinsvist om forgrening i kvadratiske talringe

1. Introducér **kvadratiske talringe** $\mathbb{Z}[\xi]$ (normeret andengradspolynomium med heltalskoefficienter, kvadratfri diskriminant, (irrationale) rødder ξ, kvadratisk tal $x + y\xi$, mængden af disse $\mathbb{Z}[\xi]$)

2. Fortæl meget lidt om **UFD** og egenskaber (at **irred. opløsninger** eksisterer for alle elt. og er entydige, fx). Led over i, at nogle kvadratiske talringe kan ses ikke at være UFD ved ikke at opfylde ovenstående, men nogle er UFD, da de er **PID**

3. Sætning 6.20: **Forgrening i faktorielle kvadratiske talringe** - overvej hvorfor der er nødt til at blive gjort forskel på type 2 og speciel type. Led derfor videre til et eksempel, nemlig Gauss' talring

4. Sætning 6.21: **Forgrening i Gauss' talring** (som er UFD - forklar at dette kan vises, ved at vise at den er euklidisk).

5. Forklar slutteligt hvorfor ligningen $x^2 + y^2 = p$ hvor $p = 2$ eller $p \equiv 1 \pmod 4$ altid har heltalsløsninger $(x, y) \in \mathbb{Z} \times \mathbb{Z}$

6. Led eventuelt ind på hvordan mere komplicerede **diofantiske ligninger** kan løses ved brug af forgreningsegenskaben og nævn fordelen UFD giver (repræsentantsystem af primelementer)

4 Forgrening i Gauss' talring og anvendelser på diofantiske ligninger

1. Introducér **kvadratiske talringe** $\mathbb{Z}[\xi]$ (normeret andengradspolynomium med heltalskoefficienter, kvadratfri diskriminant, (irrationale) rødder ξ, kvadratisk tal $x + y\xi$, mængden af disse $\mathbb{Z}[\xi]$)

2. Idet $\mathbb{Z}[\xi] \ni \alpha$ kan ses som talpar $(x, y) \in \mathbb{Z}\times\mathbb{Z}$, er der en bijektiv korrespondance mellem α, hvor $N(\alpha) = k$ og talpar der opfylder $x^2 - bxy + cy^2 = k$ - led lidt videre til **Pells ligning** ($k = \pm 1$) (enheder i $\mathbb{Z}[\xi]$) og ligninger som $x^2 - 2y^2 = -1$, der kan vises at have uendelig mange løsninger

3. Mange gode egenskaber ved at betragte faktorielle, kvadratiske talringe. Sætning 6.16: Vis, at $\mathbb{Z}[i]$ er et **UFD** (ved at vise, at den er euklidisk)

4. I faktorielle kvadr. talringe kan man tale om **forgrening**

5. Sætning 6.21: **Forgrening i Gauss' talring** (som er UFD - forklar at dette kan vises, ved at vise at den er euklidisk).

6. 6.22: Den **diofantiske ligning** $x^2 + y^2 = k$ (forklar, hvornår og hvorfor denne har løsninger, hvis $k = 2^l q_1^{m_1} \cdots q_s^{m_s} p_1^{n_1} \cdots p_r^{n_r}$; $q_j \equiv 3, p_i \equiv 1$ modulo 4; m_j skal være lige!)

5 Cirkeldelingspolynomier

1. Introducér begrebet **(primitiv) n'te enhedsrod** i et legeme L og specielt i legemet $\mathbb{C}$ - **komplekse n'te enhedsrødder** (setup er altså præcis som i 3.1)

2. Definition på det **n'te cirkeldelingspolynomium** - normeret og af grad $\varphi(n)$ (antal elementer af orden n i C_n)

3. Vis meget hurtigt sætning $X^n - 1 = \prod_{d|n} \Phi_d$ - fortæl, at den har koefficienter i $\mathbb{Z}$

4. Cirkeldelingspolynomierne er irreducible over $\mathbb{Q}[X]$ - vis **EVT.** (forklar idéen) at de p'te er irreducible vha. **Eisensteins irreducibilitetskriterium** (betragt $\Phi_p(X+1)$, vis, at dette er irreducibelt idet $p \mid p$, men $p^2 \nmid p$)

5. Da legeme L enten har **karakteristik** 0 eller p (primtal), kan $\mathbb{Z}$ eller $\mathbb{Z}p$ opfattes som delring af legeme L, ved isomorfisætningen - af dette følger **Freshman's Dream**

6. **Hovedsætning:** Lad p være karakteristikken af legemet L. Da gælder for $\xi \in L$ og $n \in \mathbb{N}$, at ξ har orden n i L^*, hvis og kun hvis $\Phi_n(\xi) = 0$ og $p \nmid n$

7. Perspektiver til konstruktion af **endelige legemer** (irreducible divisorer i ϕ_n, polynomiumskvotient $\mathbb{F}_p[X]/(f)$)

6 Endelige legemer (eksistens og entydighed)

Alt det første skal gå meget hurtigt her, da eksistens og entydighed kommer til at tage noget tid.

1. Formål: vil konstruere legeme ud fra legeme L hvor L er dellegeme, og hvor normeret og irreducibelt $f \in L[X]$ har rod ξ

2. Tal om struktur af polynomiumskvotient $R[X]/(f)$, hvor f er et normeret polynomium i $R[X]$ af positiv grad n

   (a) Enhver ækvivalensklasse har entydig fremstilling $\alpha = b_0 + b_1\xi + \cdots + b_{n-1}\xi^{n-1}$, hvor $\xi = [X]_{(f)}$ og $X \in R[X]$

   (b) Ud fra denne konstruktion kan for eksempel $\mathbb{C}$ konstrueres, hvor vi benytter $X^2 + 1$ i $\mathbb{R}[X]$

   (c) Ud fra hovedidealsætning, er $L[X]$ PID, hvis L legeme

   (d) Lemma før 5.9: f irred. i $L[X]$ (eks. $\mathbb{F}_p[X]$). $L[X]/(f)$ legeme (f irred. (f) maks.id.)

3. Husk sætning 3.6: Lad p være karakteristikken af legemet L. Da gælder for $\xi \in L$ og $n \in \mathbb{N}$, at ξ har orden n i L^*, hvis og kun hvis $\Phi_n(\xi) = 0$ og $p \nmid n$

Godset er:

1. **Sætning (lemma):** Lad p være et primtal, primisk med $n \in \mathbb{N}$ ($p \nmid n$). Betragt nu $\Phi_n \in \mathbb{F}_p[X]$ og en irreducibel divisor f i $\Phi_n \in \mathbb{F}_p[X]$. Sæt $r := \deg(f)$. $K := \mathbb{F}_p[X]/(f)$ er et legeme med p^r elementer, og $\xi := [X]_{(f)}$ er en primitiv n'te enhedsrod i K. Endvidere er $r = |[p]_n|$ i $(\mathbb{Z}/n)^*$.

   Husk her, at K er et legeme ud fra valg af ξ og $\deg(f)$, hvorpå $\#K = p^r$. Vis, at $\Phi_n(\xi) = 0$. Vis, at hvis $s \in \mathbb{N}$ med $[p]^s = 1$ i $(\mathbb{Z}/n)^*$, da er $s \geq r$. Se på fremstilling af α^p, hvor $\alpha \in K$, og dermed α^{p^s} i sammenhæng med rødder i pol. $X^{p^s} - X$.

2. **Eksistens:** Lad p være primtal, $r \in \mathbb{N}$. Der findes et endeligt legeme med p^r elementer, nemlig $K := \mathbb{F}_p[X]/(f)$, hvor f er irreducibel faktor i Φ_{p^r-1}, opfattet som polynomium i $\mathbb{F}_p[X]$.

   Hvis L er et legeme med p^s elementer, findes en inj. homomorfi $K \hookrightarrow L$ hviss $r \mid s$.

   Vis, at f har grad r. Benyt foregående sætning. Lad L være et sådant legeme, L vektorrum over K, endelig basis med d vektorer i L. Ved antagelse af $r \mid s$, vis da $f \mid X^{p^s-1}$ i $\mathbb{F}_p[X]$. Injektiv homomorfi $\mathbb{F}_p[X] \hookrightarrow L[X]$ (da $\mathbb{F}_p \hookrightarrow L$). Alle $\alpha \in L$ er rødder i $X^{p^s-1} - 1$. f har rod alpha i L som polynomium i $L[X]$. Få inj. homomorfi $K \hookrightarrow L$.

3. **Entydighed:** Der er en isomorfi mellem alle legemer med p^r elementer.