Opgave 1: Let p be prime.
(a) Show that any ring with unit and order $|R| = p^2$ is commutative.

Solution: Assume R is not commutative. Let $a, b \in R$ such that $ab \neq ba$. By Lagrange, the order of a, b must divide p^2. If the order of a is p^2 then a generates R so in particular $ab = aa^k = a^k a = ba$. Hence both a and b must have order p.

0.1 Eksamen 2021

Opgave 4: $f(x) = x^4 + 4x^2 + 6$.
(a) Vis, at $f(x)$ er irreducibelt i $\mathbb{Q}[x]$.
Solution: Brøklegemet for $\mathbb{Z}$ er $\mathbb{Q}$, så per Gauss' lemma er $f(x)$ irreducibelt i $\mathbb{Q}[x]$ hvis og kun hvis det er irreducibelt i $\mathbb{Z}[x]$ idet det er monisk. Men i $\mathbb{Z}$ er (2) et primideal, og $2 \mid 4, 6$, men $2^2 = 4 \nmid 6$, så per Eisensteins kriterium, er $f(x)$ irreducibelt i $\mathbb{Z}[x]$ og $\mathbb{Q}[x]$.

(b) Bestem en irreducibel opløsning af $f(x)$ i $(\mathbb{Z}/11\mathbb{Z})[x]$.

Solution: Vi har, at 1 og -1 er rødder modulo 11, så

$$x^4 + 4x^2 + 6 \equiv (x-1)(x+1)(x^2+5)$$

Vi har $\left(\frac{-5}{11}\right) = -1$, så højresiden er faktoriseringen i irreducible faktorer.

(c) Vis, at $f(x)$ har en faktorisering $f(x) = g(x)h(x)$ i $\left(\mathbb{Z}\left[\sqrt{-2}\right]\right)[x]$, hvor $g(x), h(x)$ har grad 2.

Solution: Vi har $x^4 + 4x^2 + 6 = 0$ i $\mathbb{C}$ hvis og kun hvis $x^2 = \frac{-4 \pm \sqrt{-8}}{2} = -2 \pm \sqrt{-2}$, så

$$x^4 + 4x^2 + 6 = \left(x^2 - \left(-2 + \sqrt{-2}\right)\right)\left(x^2 - \left(-2 - \sqrt{-2}\right)\right).$$

(d) Vis, at $f(x)$ ikke har nogen rod i $\mathbb{Z}\left[\sqrt{-2}\right]$.

Solution: $\mathbb{Z}\left[\sqrt{-2}\right]$ er UFD, dermed også et integritetsområde, så hvis f har rod i x_0, må højresiden i (c) være nul og dermed en af dets faktorer være nul og dermed reducibel med en lineær faktor.
Da $N\left(-2+\sqrt{-2}\right) = 4 + 2 = 6$, ville $N(x_0^2) = 6$, så hvis $x_0 = a + b\sqrt{-2}$, er $N(x_0^2) = N(x_0)^2 = (a^2 + 2b^2)^2 = 6$. Hvis $b = 1$, fås en modstrid ved at tjekke efter, og lignende hvis $b = 0$.

0.2 Reeksamen 2021

Opgave 4: $f(x) = x^4 - 6x^2 + 12$.

(a) Vis, at $f(x)$ er irreducibelt i $\mathbb{Q}[x]$.

Solution: Da $f(x)$ er monisk, er f irreducibelt i $\mathbb{Q}[x]$ hvis og kun hvis f er irreducibel i $\mathbb{Z}[x]$. I $\mathbb{Z}$ er (3) et primideal, og $3 \mid -6, 12$, men $3^2 \nmid 12$, så per Eisensteins kriterium, er f irreducibel i $\mathbb{Z}[x]$ og dermed også i $\mathbb{Q}[x]$.

(b) Det er klart, at ± 1 er rødder i $f(x)$, så

$$x^4 - 6x^2 + 12 \equiv (x-1)(x+1)(x^2-5) \pmod 7$$

De lineære faktorer er irreducible, da $\mathbb{Z}/7\mathbb{Z}$ er et integritetsområde, og da $\left(\frac{5}{7}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{24}{8}} = -1$, er $(x^2 - 5)$ også irreducibel i $\mathbb{Z}/7\mathbb{Z}[x]$.

$g(x) = x^3 + x + 4$.
(c) Vis, at $g(x)$ er irreducibelt i $\mathbb{Z}/5\mathbb{Z}[x]$.

Solution: $\mathbb{Z}/5\mathbb{Z}$ er et legeme, så hvis $g(x)$ var reducibelt, ville den have rod i $\mathbb{Z}/5\mathbb{Z}$ - dvs. en lineær faktor -, men ved indsættelse ses $g(0) = 4, g(1) = 6, g(2) = 4, g(3) = 4, g(4) = 2$ alle modulo 5, så da g ikke har nogen rod, er g irreducibel i $\mathbb{Z}/5\mathbb{Z}[x]$.

(d) Vis, at $g(x)$ er irreducibelt i $\mathbb{Q}[x]$.

Solution: Per rationel rod testen, er de eneste mulige rødder i $\mathbb{Q}$ netop $\pm 1, \pm 2$ og ± 4.
Men det er klart, at for alle positive versioner, er $g(x) > 0$, og $g(-1) = 2, g(-2) = -6, g(-3) = -26$, så ingen af disse er rødder. Dermed har g ingen rødder i $\mathbb{Q}[x]$. Da $\mathbb{Q}$ er et legeme, følger derfor, at g ikke har nogen lineære faktorer og er dermed ikke reducibel.

0.3 Prøveeksamen

1:
(a) Vi har, at $0 \neq \overline{a} \in \mathbb{Z}/15\mathbb{Z}$ er en nuldivisor, hvis og kun hvis $ab \in 15\mathbb{Z}$ for et $\overline{b} \neq 0$. Da $\mathbb{Z}$ er UFD og $15 = 3 \cdot 5$, må $3, 5 \mid ab$. Vi kan ikke have, at $3, 5 \mid b$, da $\overline{b} \neq 0$, så enten må $3 \mid a$ eller $5 \mid a$. Vi kan heller ikke have $3, 5 \mid a$ af samme grund. Så vi får $\overline{a} = 3$ eller $\overline{a} = 5$.
For alle andre $\overline{a} \in \mathbb{Z}/15\mathbb{Z}$, må $(a, 15) = 1$, så per Bezout eksisterer $s, t \in \mathbb{Z}$ så $as + 15t = 1$, så $\overline{as} = 1$, hvormed a er en enhed.

(b) Vi har, at $N(2 + \sqrt{6}) = 4 - 6 = -2$, som er $\pm$ et primtal, hvormed den er irreducibel per Generel bemærkning 1.

(c) Det er det ikke. $\mathbb{C}$ er et legeme og dermed et integritetsområde. Vi har nu $x^2 \cdot x = x^3 \in (x^3)$. Hvis x^2 eller $x \in (x^3)$, ville $x^2 = x^3 q(x)$ eller $x = x^3 q(x)$, men da det er et integritetsområde, fås $2 = degx^2 = degx^3 + degq = 3 + degq \geq 3$, som er en modstrid.

(d) $\frac{x}{1}$ er ikke en enhed i $\mathbb{C}[x]_{(x)}$. Antag for modstrid, at $\frac{x}{1}\frac{r}{s} = \frac{1}{1}$, så må $xru(x) = su(x) \in \mathbb{C}[x] \backslash (x)$, men $xru(x) = su(x) \in (x)$; dermed modstrid, da s, u.

(e) 7 og x er ikke enheder og ikke nul i $\mathbb{Z}[x]$. De er desuden irreducible, da 7 er irreducibel i $\mathbb{Z}$ og dermed i $\mathbb{Z}[x]$ og da x er primitiv og irreducibel i $\mathbb{Q}[x]$ og dermed i $\mathbb{Z}[x]$. Dermed er $7x$ reducibel i $\mathbb{Z}[x]$. $7x$ er dog irreducibel i $\mathbb{Q}[x]$, da den er en lineær faktor og
Opgave 2:
(a)

$$x^7 + x^5 - 3x^2 - 3 = (x^6 + x^5 - 3x - 3)(x - 1) + 2x^5 - 6$$
$$(x^6 + x^5 - 3x - 3) = (2x^5 - 6)(\frac{1}{2}x + \frac{1}{2})$$

Så gcd er derfor $2x^5 - 6$, som er associeret til $x^5 - 3$.
(b) Vi har, at $x^5 - 3$ er monisk, så den er reducibel i $\mathbb{Q}[x]$ hvis og kun hvis den er reducibel i $\mathbb{Z}[x]$, men i $\mathbb{Z}[x]$ er den Eisenstein i 3, så dermed irreducibel.

(c) Vi har, at $\mathbb{Q}[x]$ er Euklidisk så specielt PID, da $\mathbb{Q}$ er et legeme. Dermed for $(f(x), g(x)) = (d(x))$, og da $d(x)$ er irreducibel, er $\mathbb{Q}[x]/(d(x))$ et legeme per en opgave.
Opgaven: Hvis $\mathbb{F}$ er et legeme, og $f(x) \in \mathbb{F}[x]$ er irreducibel, da er $\mathbb{F}[x]/(f(x))$ et legeme.
Bevis: I et PID er et ikke-nul primideal et maksimalideal og irreducible elementer er primelementer, så $(f(x))$ er et maksimalideal.

(d) Vi har

$$x^5 - 3 = x \cdot x^4 - 3,$$

så i legemet, er $\overline{x} \cdot \frac{1}{3}\overline{x^4} = \overline{1}$.

Opgave 3:
(a) Vi har $x^2 - (x+1)x = -x$ og $x + 1 + -x = 1$, så for $a_1 = x^2$ og $a_2 = -(x+1)x + (x+1)$, fås $a_1 + a_2 = 1$. Dermed er (x^2) og $(x+1)$ komaksimale.

(b) Vi har, $(x^2)(x+1) = \big((x^2)(x+1)\big) = \big(x^3 + x^2\big)$, så per den kinesiske restklassesætning, er

$$\mathbb{R}[x]/\left(x^3 + x^2\right) \cong \mathbb{R}[x]/(x^2) \times \mathbb{R}[x]/(x+1)$$

ved $[f(x)] \to \big([f]_{(x^2)}, [f]_{(x+1)}\big)$.

(c) Den inverse afbildning er givet ved

$$([a],[b]) \to [aa_2 + ba_1]\,,$$

så $(x,1) \to \left[x(x+1)(1-x)+x^2\right] = \left[-x^3+x^2+x\right]$.

(d) Lad $\varphi\colon R[x] \to \mathbb{R}$ ved evaluering i -1.
Denne er klart surjektiv og har kerne $(x+1)$.
Da $\varphi(f+g) = (f+g)(-1) = f(-1)+g(-1) = \varphi(f)+\varphi(g)$ og $\varphi(fg) = (fg)(-1) = f(-1)g(-1) = \varphi(f)\varphi(g)$ er φ en ringhomomorfi, som etablerer den givne isomorfi.

Opgave 4: $f(x) = x^5 + 21x + 63$.

(a) Da f er primitiv, er f irreducibel i $\mathbb{Q}[x]$ hvis og kun hvis den er irreducibel i $\mathbb{Z}[x]$. Men f er Eisenstein i 7 i $\mathbb{Z}[x]$, og dermed irreducibel.

(b) Da $\lim_{x\to\infty} f(x) = \infty$ og $\lim_{x\to-\infty} f(x) = -\infty$ og f er kontinuert, har f en rod i $\mathbb{R}$. Dermed har den en lineær faktor $(x-\alpha)$ for et $\alpha \in \mathbb{R}$.

(c) I $(\mathbb{Z}/2\mathbb{Z})[x]$ er $f(x) = x^5 + x + 1$. f har ingen rod i $\mathbb{Z}/2\mathbb{Z}$, så en faktorisering ville skulle have form

$$x^5+x+1 = (x^3+ax^2+bx+c)(x^2+dx+e) = x^5+ax^4+(e+ad+b)x^3+(a+bd+c)x^2+(be+cd)x+ce$$

så $a = 0$, og $e+b = 0, bd+c = 0, be+cd = 1, ce = 1$.
Da må $cd - b^2 = 1$. Vi har $e = 1$, så $b = 1$, så $cd = 0 \implies d = 0$. Dette giver

$$x^5+x+1 = (x^3+x+1)(x^2+1).$$

(d) Da $N(7) = 49 = 7^2$, ville en faktorisering have faktornorm 7, men $a^2 + 2b^2 = 7$ er umuligt, så 7 er irreducibel i $\mathbb{Z}\left[\sqrt{-2}\right]$ og dermed også i $\mathbb{Z}\left[\sqrt{-2}\right][x]$. Da f er Eisenstein i 7, som dermed også er et primelementer, da $\mathbb{Z}\left[\sqrt{-2}\right]$ er PID, er f irreducibelt.