1. (6 points) Find the prime factorization of $2 \in \mathbb{Z}[i]$. Hint: We have $\mathrm{N}(1+i) = 2$.

Solution: $(1+i)(1-i) = 2$ in $\mathbb{Z}[i]$ (1 pt). $\mathbb{Z}[i]$ is euclidean (2 pt). $1 \pm i$ is irreducible (1 pt) since $1 \pm i = \alpha\beta \implies 2 = N(\alpha)N(\beta) \implies$ w.l.o.g. $\alpha \in \mathbb{Z}[i]^*$ (2 pt).

2. (8 points) Show that $R := \mathbb{Z}[\sqrt{-17}]$ is not an euclidean ring.

Solution: $2 \in R$ is irreducible since $\forall \alpha \in R : N(\alpha) \neq 2$ (4 pt). $9 \cdot 2 = 18 = (1+\sqrt{-17})(1-\sqrt{-17})$ (2 pt) and $2 \nmid (1 \pm \sqrt{-17})$ (2 pt).

3. (10 points) Find the minimal polynomial of $\alpha = \sqrt{-3} + \sqrt{2}$ over $\mathbb{Q}$. What is $[\mathbb{Q}(\alpha) : \mathbb{Q}]$?

Solution: $\alpha^2 = 2\sqrt{-6} - 1$ (1 pt) $\implies \alpha^4 + 2\alpha^2 + 25 = 0$ (1 pt). $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ (2 pt). Since $t^4 + 2t^2 + 25$ has degree 4 it has to be irreducible. (6 pt)

4. (10 points) Let $R := {}^{\mathbb{Q}[t]}\!/\!_{(t^4-1)\mathbb{Q}[t]}$. How many roots has the polynomial $X^2 - X \in R[X]$?

Solution: $t^4 - 1 = (t+1)(t-1)(t^2+1)$ (2 pt) $\implies R \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(i)$ (4 pt). Since every factor on the righthandside is a field, we get for each factor exactly 2 roots of $X^2 - X$ (2 pt). There are $2^3 = 8$ roots in R (2 pt).

5. (a) (6 points) Let $\{0\} \neq R$ be a finite integral ring and $a \in R \setminus 0$. Show that the map

$$\begin{array}{rccc} [a]: & R & \longrightarrow & R \\ & x & \longmapsto & ax \end{array}$$

is a bijective homomorphism.

Solution: $[a]$ is a homomorphism (2 pt). $\ker([a]) = \{0\}$ (2 pt) since R is integral. $[a]$ is injective (1 pt) $\implies [a]$ is bijective since R is finite (1 pt).

(b) (9 points) Let $\{0\} \neq R$ be a commutative ring and let $P \subsetneq R$ be a prime ideal of R. Use Part a) to show:

$${}^{R}\!/\!_{P} \text{ is finite} \implies P \text{ is a maximal ideal of } R$$

Solution: $S := {}^{R}\!/\!_{P}$ is integral (2 pt), finite $\implies [a] : S \to S$ is bijective (2 pt) for $0 \neq a \in S \implies \exists b \in S : [a](b) = a \cdot b = 1_S$ (2 pt) $\implies a \in S^*$ (1 pt) $\implies S$ is a field (1 pt) $\implies P$ is maximal (1 pt).

6. (10 points) Let $\{0\} \neq R$ be a commutative ring, $a \in R$ and $f \in R[t]$. Show:

$$fR[t] + (t-a)R[t] = R[t] \iff f(a) \in R^*.$$

> **Solution:** $I := fR[t] + (t-a)R[t]$
> "$\implies$": $I = R[t] \implies 1 \in I$ (1 pt) $\implies \exists g, h\mathbb{R}[t] : fg + (t-a)h = 1$ (1 pt) $\implies f(a)g(a) + (a-a)h = 1$ (2 pt) $\implies f(a) \in R^*$ (1 pt)
> "$\Leftarrow$": $(t-a)$ is monic $\implies \exists q, r \in R[t] : f = (t-a)q + r$ and $r = 0$ or $\deg(r) = 0$ (2 pt) $\implies f(a) = r \in I$ (2 pt) $\implies I = R[t]$ (1 pt).

7. (10 points) Let $\phi : R \to S$ be an isomorphism of rings and $a \in R$ an irreducible element. Show that $\phi(a) \in S$ is irreducible.

> **Solution:** Assume $\phi(a) = \beta \cdot \gamma, \beta, \gamma \in S \setminus S^*$ (2 pt) $\implies \exists b, c \in R : \beta = \phi(b), \gamma = \phi(c)$ (ϕ is surjective) (2 pt) $\implies \phi(a) = \phi(bc) \implies a = bc$($\phi$ is injective) (2 pt). Since $\phi(R^*) \subset S^*$ (4 pt), this is a contradiction.

8. (8 points) Construct a field with 27 elements.

> **Solution:** $f := t^3 - t + 1 \in \mathbb{F}_3[t]$ is irreducible (2 pt) $\implies L := \mathbb{F}_3[t]/(f)$ is a field with $[L : \mathbb{F}_3] = 3$ (4 pt) $\implies \#L = 3^3 = 27$ (2 pt).

9. (10 points) Let K be a field and $A, B \in K$. Show that $f := X^3 + AX + B \in K[X]$ is separable if and only if $4A^3 + 27B^2 \neq 0$. Hint: Use the equality

$$(-9AX + 27B) \cdot f + (3X^2 + A) \cdot (3AX^2 - 9BX + 4A^2) = 4A^3 + 27B^2.$$

> **Solution:** $f' = (3X^2 + A)$ (2 pt). f is separable iff $\gcd(f, f') = 1$ (2 pt). Let α be a root of f. Evaluating at α gives $(3\alpha^2 + A) \cdot (3A\alpha^2 - 9B\alpha + 4A^2) = 4A^3 + 27B^2$ (2 pt). $4A^3 + 27B^2 \neq 0 \implies f'(\alpha) \neq 0$ (2 pt) and $f'(\alpha) = 0$ implies $4A^3 + 27B^2 = 0$ (2 pt).

10. Let $f := t^6 - t^5 + t^4 - 2t^3 + 2t^2 - 2t - 1 \in \mathbb{Z}[t]$.
    (a) (3 points) Find a prime factorization of $\bar{f} \in \mathbb{F}_2[t]$, where $\bar{\cdot}$ is the reduction of the coefficients modulo 2. Hint: What are the irreducible polynomials of degree two in $\mathbb{F}_2[t]$?

Solution: $\bar{f} = (t+1)(t^5+t^3+t^2+t+1)$ (1 pt) and $(t^5+t^3+t^2+t+1)$ is irreducible since $(t^2+t+1) \nmid (t^5+t^3+t^2+t+1)$ (2 pt).

(b) (2 points) Has f a root in $\mathbb{Z}$?

Solution: The only possible roots are ± 1 (2 pt).

(c) (8 points) Use Parts a) and b) to conclude that f is irreducible in $\mathbb{Q}[t]$.

Solution: Assume $f = gh$ with $g, h \in \mathbb{Z}[t]$ monic (1 pt). Then $\bar{f} = \bar{g}\bar{h} = (t+1)(t^5 + t^3 + t^2 + t + 1)$ with $\deg(\bar{g}) = \deg(g), \deg(\bar{h}) = \deg(h)$ (2 pt). $\mathbb{F}_2[t]$ is a faktorial ring (1 pt), thus, w.l.o.g. $(t^5+t^3+t^2+t+1) \mid \bar{g}$ (1 pt) $\implies 5 \leq \deg(\bar{g}) = \deg(g)$ (1 pt) $\implies f$ is irreducible (since f is primitive) or f has a root (this is impossible by Part b)) (1 pt). $f \in \mathbb{Q}[t]$ is irreducible (1 pt).