1. (10 points) Let $\{0\} \neq R$ be a commutative ring and $a \in R$. Show $R \cong R[t]/(t-a)R[t]$.

> **Solution:** Consider the map $ev_a : R[t] \to R, ev_a(f) = f(a)$ (2pts). This is a homomorphism (2 pts) and it is surjective since $a \in R$ (2 pts). Its kernel is $(t-a)R[t]$ (2 pts). This implies the assertion (2 pts).

2. (10 points) Let R be an integral ring and $f, g \in R$. Assume f is a prime such that $f \nmid g$. Show $fR \cap gR = fgR$.

> **Solution:** "$\subset$": $a \in fR \cap gR \implies fh = a = gk$ for some $h, k \in R$ (1 pt). Then we have $f \mid gk$ and since f is prime, $f \mid g$ or $f \mid k$ (3 pts). By assumption we have $f \mid k$ (2pts); thus $a = fgk'$ for some $k' \in R$ (1 pt).
> "$\supset$": trivial (3 pts).

3. Set $f := \frac{1}{3}t^4 - 2t^3 - t - 1 \in \mathbb{Q}[t]$.
   (a) (6 points) Show that f is irreducible in $\mathbb{Q}[t]$.

   > **Solution:** Consider $g := 3f \in \mathbb{Z}[t]$ (2 pts). g is irreducible by Eisenstein with $p = 3$ (3 pts). Since 3 is a unit in $\mathbb{Q}$ this shows the assertion (1 pt).

   (b) (4 points) Show that $K := \mathbb{Q}[t] / f\mathbb{Q}[t]$ is isomorphic to a subfield of $\mathbb{R}$.

   > **Solution:** We have $f(0) < 0$ and for $\alpha \in \mathbb{R}$ large we get $f(\alpha) > 0$ (2 pts). Since a polynomial function $\tilde{f} : \mathbb{R} \to \mathbb{R}$ is continuus, this implies f has a real root (1 pt). Let α be such a real root. This implies $ev_\alpha : \mathbb{Q}[t] \to \mathbb{R}$ has an image isomorphic to K (1 pt).

4. Consider the homomorphism

$$\begin{aligned} \mathrm{ev}_{\frac{1}{2}} : \quad \mathbb{Z}[t] &\longrightarrow \mathbb{Q} \\ f &\longmapsto f(\tfrac{1}{2}). \end{aligned}$$

   (a) (6 points) Show $\mathbb{Z}\left[\frac{1}{2}\right] := \mathrm{Im}\left(\mathrm{ev}_{\frac{1}{2}}\right) = \left\{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}_0\right\}$.

   > **Solution:** "$\subset$": Let $\sum^n f_i t^i f \in \mathbb{Z}[t]$. Then $ev_{\frac{1}{2}}(f) = \frac{2^n \cdot f(\frac{1}{2})}{2^n}$, where $2^n \cdot f(\frac{1}{2}) \in \mathbb{Z}$ (3 pts).
   > "$\supset$": We have $\frac{a}{2^n} = ev_{\frac{1}{2}}(at^n)$ (3 pts).

   (b) (8 points) Show $\mathbb{Z}\left[\frac{1}{2}\right]$ is a principal ideal ring.
   Hint: Show for an ideal $I \subset \mathbb{Z}\left[\frac{1}{2}\right]$: $I \cap \mathbb{Z} = a\mathbb{Z}$ for some $a \in \mathbb{Z}$ and conclude $I = a\mathbb{Z}\left[\frac{1}{2}\right]$.

Solution: Let $I \subset R$ be an ideal. Then $I \cap \mathbb{Z} \subset \mathbb{Z}$ is an ideal (2 pts). $\mathbb{Z}$ is a PIR. Thus $I \cap \mathbb{Z} = a\mathbb{Z}$ for some integer a (2 pts). Let $\frac{b}{2^n} \in I$. Then $b \in I \cap \mathbb{Z}$ and $b = ab'$ for some $b' \in \mathbb{Z}$ (2 pts). Thus $b \in a\mathbb{Z}\left[\frac{1}{2}\right]$ (1 pt). The other inclusion is trivial (1 pt).

5. (a) (8 points) Construct a field $\mathbb{F}_{32}$ with 32 elements.

Solution: Consider the polynomial $f := t^5 + t^3 + t^2 + t + 1 \in \mathbb{F}_2[t]$. f is irreducible in $\mathbb{F}_2[t]$ since it has no roots and is not divisible by $t^2 + t + 1$ (4 pts). Therefore, $\mathbb{F}_{32} := \mathbb{F}_2[t]/(f)$ is a field with 32 elements (4 pts).

(b) (6 points) Let $\psi : \mathbb{Z} \to \mathbb{F}_{32}$ be a homomorphism. Find an element $\alpha \in \mathbb{F}_{32} \setminus \psi(\mathbb{Z})$.

Solution: There exists a unique hom. $\psi : \mathbb{Z} \to \mathbb{F}_{32}$ (2 pts). The image of this unique homomorphism is $\mathbb{F}_2 \subset \mathbb{F}_{32}$ (2 pts). Therefore, $\alpha := \bar{t}$ is not in the image of ψ (2 pts).

6. (12 points) Let $\mathbb{F}_q$ be a finite field with $q > 2$ elements. Compute $\prod_{\alpha \in \mathbb{F}_q^*} \alpha$ and $\sum_{\alpha \in \mathbb{F}_q^*} \alpha$. Hint: Try to factor $t^{q-1} - 1 \in \mathbb{F}_q[t]$.

Solution: $\mathbb{F}_q^*$ is a group with $q-1$ elements (2 pts). Therefore, $\alpha^{q-1} = 1$ for $\alpha \in \mathbb{F}_q^*$ and $t^{q-1} - 1 = \prod_{\alpha \in \mathbb{F}_q^*}(t - \alpha)$ (4 pts). Comparing coefficients yields $\prod_{\alpha \in \mathbb{F}_q^*} \alpha = -1$ (3 pts) and $\sum_{\alpha \in \mathbb{F}_q^*} \alpha = 0$ (3 pts).

7. Let $R \subset \mathbb{C}$ be a subring.

(a) (6 points) Show: $\mathbb{Z}$ is a subring of R.

Solution: Since $\mathrm{char}(R) = \mathrm{char}(\mathbb{C}) = 0$ (2 pts) we have $\ker(\mathbb{Z} \to R) = \{0\}$ (2 pts) implying injectivity of this homomorphism (2 pts).

(b) (8 points) Let $a, b \in \mathbb{Z}$. Show: If $d := \gcd(a, b) \in \mathbb{Z}$, then d is a greatest common divisor of a and b in R.

Solution: Need to show: If δ is a common divisor of a, b in R, then $\delta \mid d$ (1 pt). Since $\mathbb{Z}$ is a PIR (1 pt), we have $d = ax + by$ for some $x, y \in Z$ (1 pt). Let $\delta \in R$ be a common divisor of a and b (1 pt). Then we can write $d = \delta\alpha x + \delta\beta y = \delta(\alpha x + \beta y)$ for some $\alpha, \beta \in R$ (2 pts). This implies the assertion (2 pts).

8. Let $f_1, f_2, f_3, f_4 \in \mathbb{F}_2[t]$ be the degree two polynomials over $\mathbb{F}_2$. Define $R_i = {}^{\mathbb{F}_2[t]}\!/\!_{f_i\mathbb{F}_2[t]}$ for $i = 1, \dots, 4$.

(a) (8 points) Which of the rings R_i are isomorphic?

Solution: $f_1 := t^2 + t + 1, f_2 := t(t + 1), f_3 := t^3, f_4 := (t + 1)^2$. f_1 is irreducible; thus R_1 is a field (1 pt). $1 \in R_2$ is the only unit (1 pt). R_3, R_4 have both two units (1 pt). Thus, only R_3 and R_4 can be isomorphic (1 pt). Such an isomorphism is uniquely determined by the image of $\bar{t}$ and it has to send nilpotent elements to nilpotent elements. Thus, the only possible isomorphism fulfills $\bar{t} \mapsto \overline{t+1}$ (2 pt). This indeed is an isomorphism of R_3 and R_4 (2 pts).

(b) (8 points) Show R_i is not isomorphic to $\mathbb{Z}/4\mathbb{Z}$ for $i = 1, \dots, 4$.

Solution: We have $\mathrm{char}(R_i) = 2$ (3 pts) and $\mathrm{char}(\mathbb{Z}/4\mathbb{Z}) = 4$ (1 pt). Therefore, non of the R_i is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ (4 pts).