Note: Unless otherwise indicated, all claims have to be justified. Final answers without or with wrong justification will not be given any credit.

1. [4 points] (a) [1 point] Give an example of an integral domain which is not a field. No explanation is necessary.

(b) [3 points] Show that a finite integral domain is a field.

Solution: (a) $\mathbb{Z}$

(b) Let R be a finite integral domain. Let $a \in R - \{0\}$. Since R is finite, there are positive integers m and n, say $m < n$, such that $a^m = a^n$. Since R is a domain and $a \neq 0$, we have $a^m \neq 0$. Combining with $a^m \cdot 1 = a^m \cdot a^{n-m}$ and the fact that R is a domain, we get $a^{n-m} = 1$. Thus a is a unit.

2. [5 points] Let $\phi : R \to S$ be a ring homomorphism. Let I be an ideal of S.

(a) [3 points] Show that $\phi^{-1}(I)$ is an ideal of R. You may take it for granted that $\phi^{-1}(I)$ is a subgroup of R under addition.

(b) [2 points] Suppose I is a prime ideal. Show that $\phi^{-1}(I)$ is also prime.

Solution: (a) Let $a \in \phi^{-1}(I)$ and $r \in R$. We need to check that $ar \in \phi^{-1}(I)$, or equivalently, that $\phi(ra) \in I$. We have $\phi(ra) = \phi(r)\phi(a)$. Since $\phi(a) \in I$ and I is an ideal, it follows that $\phi(ra) \in I$.

(b) Let $ab \in \phi^{-1}(I)$. We shall show that a or b is in $\phi^{-1}(I)$. Indeed, $ab \in \phi^{-1}(I)$ tells us that $\phi(ab) \in I$. Combining with $\phi(ab) = \phi(a)\phi(b)$ and the fact that I is a prime ideal, we get that $\phi(a)$ or $\phi(b)$ are in I. Thus a or b is in $\phi^{-1}(I)$, as desired.

3. [5 points] (a) [3 points] Let R be a PID. Suppose $r \in R$ is an irreducible element. Show that the ideal (r) is maximal.

(b) [2 points] Give an example that shows that the ideal generated by an irreducible element need not be maximal in an arbitrary integral domain.

Solution: (a) Suppose J is an ideal of R with $(r) \subset J$. Since R is a PID, $J = (a)$ for some $a \in R$. Now $(r) \subset (a)$ implies that $r = ab$ for some $b \in R$. Since r is irreducible, a or b is a unit. In the former case, $J = (a) = R$. In the latter case, $J = (a) = (r)$.

(b) The element x of the ring $\mathbb{Z}[x]$ is irreducible, but the ideal generated by x is not maximal (as $(x) \subsetneq (x, 2) \subsetneq \mathbb{Z}[x]$, or alternatively $\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$ is not a field).

4. [5 points] Let $f(x) = x^3 + x^2 - 1 \in \mathbb{F}_3[x]$. Let $K = \mathbb{F}_3[x]/(f(x))$.

(a) [2 points] Show that K is a field.

(b) [2 points] How many elements does K have?

(c) [1 points] Show that the equation $X^3 + X^2 - 1 = 0$ has a solution in K.

Solution: (a) It is enough to show that $f(x)$ is irreducible in $\mathbb{F}_3[x]$ (as the ideal generated by an irreducible element in a PID is maximal, and the quotient by a maximal ideal is a field). Since $f(x)$ has degree 3, it suffices to check that $f(x)$ does not have any roots in $\mathbb{F}_3$. We have $f(0) = -1$, $f(1) = 1$ and $f(-1) = -1$ so indeed f has no roots in $\mathbb{F}_3$.

(b) Since $f(x)$ has degree 3, the dimension of K as a vector space over $\mathbb{F}_3$ is 3. (Indeed, $\{1, \overline{x}, \overline{x}^2\}$ is a basis of K over $\mathbb{F}_3$, where here as well as below for any $g(x) \in \mathbb{F}_3[x]$ we denote by $\overline{g(x)}$ the image of $g(x)$ under the quotient map $\mathbb{F}_3[x] \to K$). Thus $|K| = |\mathbb{F}_3|^3 = 27$.

(c) $X = \overline{x}$ is a solution:

$$\overline{x}^3 + \overline{x}^2 - 1 = \overline{f(x)} = 0.$$

5. [6 points] Determine if the following polynomials are irreducible in the given polynomial rings.

(a) [2 points] $x^6 + 18x - 12$ in $\mathbb{Q}[x]$

(b) [2 points] $x^{14} + x^{13} + x^{12} + \cdots + x^2 + x + 1 = \frac{x^{15}-1}{x-1}$ in $\mathbb{Q}[x]$

(c) [2 points] $x^{p^2} + ax^p + b$ in $\mathbb{F}_p[x]$, where $a, b \in \mathbb{F}_p$.

Solution: (a) Irreducible by Eisenstein criterion for prime 3.

(b) Not irreducible. Let $f(x) = x^{14} + x^{13} + x^{12} + \cdots + x^2 + x + 1$. Let ω be a primitive 3rd root of unity. Then ω is a root of $x^{15} - 1$. Since $x^{15} - 1 = (x-1)f(x)$ and $\omega \neq 1$, we have $f(\omega) = 0$. Combining with $f(x) \in \mathbb{Q}[x]$ it follows that the minimal polynomial of ω over $\mathbb{Q}$, i.e. $x^2 + x + 1$ divides $f(x)$. (Similarly, working with a primitive 5th root of unity we get that $x^4+x^3+x^2+x+1$ also divides $f(x)$.)

(c) Not irreducible. Since $\mathbb{F}_p[x]$ is a ring of characteristic p (which is a prime number), we have

$$(x^p + ax + b)^p = x^{p^2} + a^p x^p + b^p = x^{p^2} + ax^p + b,$$

where the last equality is because $a^p = a$ for any $a \in \mathbb{F}_p$.

6. [6 points] Let $K \subset \mathbb{C}$ be the splitting field of $x^{16} - 1$ over $\mathbb{Q}$. Let $\zeta = e^{2\pi i/16}$.

(a) [2 points] Show that $K = \mathbb{Q}(\zeta)$.

(b) [3 points] Find the minimal polynomial of ζ over $\mathbb{Q}$.

(c) [1 point] Give a basis for K as a vector space over $\mathbb{Q}$. No explanation is necessary.

Solution: (a) We have

$$x^{16} - 1 = \prod_{j=1}^{16} (x - \zeta^j).$$

Thus $x^{16} - 1$ splits over $\mathbb{Q}(\zeta)$. It follows that $K \subset \mathbb{Q}(\zeta)$. On the other hand, since ζ is a root of $x^{16} - 1$, we have $\zeta \in K$. Thus $\mathbb{Q}(\zeta) \subset K$.

(b) ζ is a root of the polynomial $x^{16} - 1 = (x^8 - 1)(x^8 + 1)$. Since $\zeta^8 \neq 1$, it follows that ζ must be a root of $x^8 + 1$. We show that $x^8 + 1$ is irreducible over $\mathbb{Q}$; it will then follow that $x^8 + 1$ is the minimal polynomial of ζ over $\mathbb{Q}$.

To show irreducibility of $f(x) = x^8 + 1$, it is enough to show that $f(x + 1) = (x + 1)^8 + 1$ is irreducible. The latter polynomial is irreducible by Eisenstein criterion for prime 2. Indeed, its leading coefficient is 1 and the constant term is 2. Denoting the quotient map $\mathbb{Z} \to \mathbb{F}_2$ by π and the induced map $\mathbb{Z}[x] \to \mathbb{F}_2[x]$ by π^*, we have

$$\pi^*((x + 1)^8 + 1) \overset{(\dagger)}{=} (x + 1)^8 + 1 \overset{(\ddagger)}{=} (x + 1 + 1)^8 = x^8.$$

(Here the second $(x + 1)^8 + 1$ is an element of $\mathbb{F}_2[x]$ and ($\dagger$) is by the fact that π^* is a ring map. Equality ($\ddagger$) is because 8 is a power of the characteristic of $\mathbb{F}_2[x]$ (which is a prime number).) Thus all the coefficients of $(x + 1)^8 + 1$ are even except the leading coefficient.

(c) Since the minimal polynomial of ζ over $\mathbb{Q}$ has degree 8, the set $\{1, \zeta, \zeta^2, ..., \zeta^7\}$ is a basis of $\mathbb{Q}(\zeta)$ (= K) over $\mathbb{Q}$.

7. [4 points] Let F be a field of characteristic zero. Let $f(x) \in F[x]$ be an irreducible polynomial. Show that $f(x)$ has no repeated roots in any extension of F.

Solution: Suppose $f(x)$ has a repeated root α in some extension K/F. Then $f'(\alpha) = 0$. Combining the facts that (i) $f(x)$ is irreducible in $F[x]$, (ii) $f(\alpha) = 0$, and (iii) $f'(x) \in F[x]$ and (iv) $f'(\alpha) = 0$ it follows that $f(x) \mid f'(x)$. (Indeed, the first two imply that $f(x)$ generates the kernel of $ev_\alpha : F[x] \to K$, and the last two say that $f'(x) \in \ker(ev_\alpha)$). Since $f(x)$ is a polynomial of positive degree, we have $\deg(f'(x)) < \deg(f(x))$. Putting $\deg(f'(x)) < \deg(f(x))$ and $f(x) \mid f'(x)$ together it follows that $f'(x) = 0$. But this is absurd since F has characteristic zero and hence the derivative of $f(x)$ is a nonzero polynomial.

(Common misconception: To say $f(x) \in F[x]$ has a repeated root α in some extension K/F means that $f(x) = (x - \alpha)^2 g(x)$ for some $g(x)$ in $K[x]$. Note that $g(x)$ need not be in $F[x]$. In fact, looking at the coefficient of the second highest power of x you can see that $g(x)$ will not be in $F[x]$ if α is not in F and $char(F) \neq 2$.)

8. [Bonus, 4 points] Let p be a prime number and n, m positive integers. Let K be a field with p^n elements. Show that K has a subfield with p^m elements if and only if $m \mid n$.

Solution: $\Rightarrow$: Suppose K has a subfield F with p^m elements. Then K is a vector space over F. Since K is a finite set, $\dim_F(K)$ (= the dimension of K as a vector space over F) is finite: just start with all of K as a spanning set and then cut it down to a linearly independent spanning set β. If $\dim_F(K) = d$, then $|K| = |F|^d$ (as every element of K can be uniquely expressed as an F-linear combination of the elements of β). This implies that $n = md$.

$\Leftarrow$: Let m be a divisor of n. Identify the prime field of K with $\mathbb{F}_p$. Consider the polynomial

$$f(x) = x^{p^m} - x \in \mathbb{F}_p[x].$$

Let

$$L = \{\alpha \in K : f(\alpha) = 0\}.$$

We claim that L is a field with p^m elements. Indeed, it is clear that L contains 1 and is closed under multiplication and taking additive inverses. That L is closed under addition follows easily from the fact that

$$(\alpha + \beta)^p = \alpha^p + \beta^p$$

(and hence by iteration, $(\alpha+\beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$)) for any $\alpha, \beta \in K$. This shows that L is a subring of K. But then being a finite integral domain, L is a field.

It remains to show that L has p^m elements. That is, we want to show that the number of distinct roots of $f(x)$ in K is equal to $\deg(f(x))$. This follows from the following two facts: (i) $f(x)$ splits over K, and (ii) $f(x)$ has no repeated roots. To see (ii), note that $f'(x) = -1$ (and hence $f'(x)$ has no roots). To see (i), first note that since $m \mid n$, we have $p^m - 1 \mid p^n - 1$ (if $n = md$, then substitute $X = p^m$ in $X^d - 1 = (X-1)(1 + X + \cdots + X^{d-1})$). It then follows that

$$x^{p^m-1} - 1 \mid x^{p^n-1} - 1$$

(by the same token: if $p^n - 1 = (p^m - 1)d$, substitute $X = x^{p^m-1}$ in the same formula). Multiplying by x, we get

$$x^{p^m} - x \mid x^{p^n} - x.$$

This holds in $\mathbb{Z}[x]$, and hence also in $\mathbb{F}_p[x]$. Since $x^{p^n} - x \in \mathbb{F}_p[x]$ splits over K, it follows that so does $x^{p^m} - x$.

Extra space for rough work or to continue your solution to a question. What you write here will not be graded unless you write “Continued on page 10” in the original question space.

Extra space for rough work or to continue your solution to a question. What you write here will not be graded unless you write “Continued on page 11” in the original question space.

Extra space for rough work or to continue your solution to a question. What you write here will not be graded unless you write “Continued on page 12” in the original question space.

The end.
Total points excluding the bonus question = 35.