[10] 1)(a) Find polynomials $q, r \in \mathbb{Z}_6[x]$ ($\deg r < 1$) s.th.

$$4x^4+3x^3+x+1 = q(x^2+3x+1)+r$$

[2] Solution

$$(4x^2+3x+5)(x^2+3x+1) = 4x^4+3x^3+5x^2+0+3x^2+3x+4x^2+3x+5$$
$$= 4x^4+3x^3+0+5$$

$q = 4x^2+3x+5$, $r = x+2$

[2] (b) For which primes $p$ is $x-1$ a factor of $f = 3x^5+5x^3+4x+2$ in $\mathbb{Z}_p[x]$?

Solution: $x-1$ is a factor $\Leftrightarrow$ $0 = f(1) = 3+5+4+2 = 14$ in $\mathbb{Z}_p$, i.e. $p \mid 14$. Thus for $p=2$ and $p=7$.

[3] (c) Find all irreducible $f \in \mathbb{Z}_2[x]$ with $\deg f = 3$

Solution Since $\deg(f)=3$, we must have $f = x^3+a_2x^2+a_1x+a_0$

By irreducibility $a_0 \neq 0$ (else $x \mid f$), so $f = x^3+a_2x^2+a_1x+1$

Also, by Thm 1 in §4.2, $f$ does not have a root in $\mathbb{Z}_2$, so

$0 \neq f(1) = 1+a_2+a_1+1 = a_2+a_1$, whence $a_1+a_2 = 1$, i.e.

$$f = x^3+x+1 \quad \text{or} \quad f = x^3+x^2+1$$

Using again Thm 1 in §4.2 above, it follows that both polynomials $x^3+x+1$ and $x^3+x^2+1$ are irreducible in $\mathbb{Z}_2[x]$.

[2] (d) Show that $7x^3+3x^2+2x+5$ is irreducible in $\mathbb{Q}[x]$

Solution. We apply the modular irreducibility test with $p=2$. The reduction of the polynomial in $\mathbb{Z}_2[x]$ is $x^3+x^2+1$ which is irreducible by (c), whence $7x^3+3x^2+2x+5$ is irreducible in $\mathbb{Q}[x]$

Alternative: Show $f = 7x^3+3x^2+2x+5$ does not have a root in $\mathbb{Q}$ (applies the Rational Roots Criterion)

15 min [10] (2) (a) Determine the units in $\mathbb{Z}(\sqrt{-3})$. (Hint: Use $N(m+n\sqrt{-3}) = m^2+3n^2$ for $m+n\sqrt{-3} \in \mathbb{Z}(\sqrt{-3})$ with $m,n \in \mathbb{Z}$.)

[4] Solution: Suppose $a = m+n\sqrt{-3} \in R^\times$. Then there exists $b \in R = \mathbb{Z}(\sqrt{-3})$ with $ab = 1$. But then $1 = N(1) = N(ab) = N(a)N(b)$ forces $1 = N(a) = m^2+3n^2$. Hence $m = \pm 1$, $n = 0$, ie $a = \pm 1$. It is clear that, conversely, $\pm 1 \in R^\times$. Therefore $R^\times = \{\pm 1\}$.

[6] (b) Show that $1+\sqrt{-3}$ is irreducible in $\mathbb{Z}[\sqrt{-3}]$, but not prime.

Solution Clearly, $0 \neq 1+\sqrt{-3} = : p$. Also $p \notin R^\times$ by (a). Suppose $p = ab$ for some $a, b \in R$. Then $N(a)N(b) = N(p) = 1+3 = 4$ follows. Because $N(c) \neq 2$ for all $c \in R$, we must have $N(a) \in \{1,4\}$. If $N(a) = 1$ then $a = \pm 1 \in R^\times$. If $N(a) = 4$ then $N(b) = 1$ and so $b \in R^\times$.

To show that $p$ is not prime, we consider

$$p(1-\sqrt{-3}) = (1+\sqrt{-3})(1-\sqrt{-3}) = 1-(-3) = 1+3 = 4 = 2\cdot 2$$

If $p$ is prime then $p \mid 2$, i.e. $pq = 2$ for some $q \in R$. Then $4 = N(2) = N(p)N(q) = (1+3)N(q) = 4N(q)$, whence $N(q) = 1$ and thus $q = \pm 1$, ie $2 = \pm(1+\sqrt{-3})$, contradiction.

[10] 3) Let $R$ be a PID. Prove that the following are equivalent for $0 \neq p \in R$, $p \notin R^\times$:

(1) $p$ is a prime element,

(2) $R/\langle p \rangle$ is a field,

(3) $R/\langle p \rangle$ is an integral domain

[6] Solution: (1) $\Rightarrow$ (2): Let $0 \neq x = a + \langle p \rangle \in R/\langle p \rangle$. Then $a \notin \langle p \rangle$ since $x \neq 0$. The set $A = \{ ra + sp : r, s \in R \}$ is an ideal, whence generated by some $d \in R$, because $R$ is a PID. Because $p \in A$ we have $p = sd$ for some $s \in R$. But $p$ is a prime element, so either $s \in R^\times$ or $d \in R^\times$. If $s \in R^\times$, then $\langle p \rangle = \langle d \rangle = A$ and therefore $a \in A = \langle p \rangle$, contradiction. Therefore $d \in R^\times$ which means that $A = \langle d \rangle = R$. Hence there exist $r, s \in R$ s.t. $1 = ra + sp$. But then $1 + \langle p \rangle = ra + \langle p \rangle = (r + \langle p \rangle)(a + \langle p \rangle)$ and so $x = a + \langle p \rangle$ is invertible in $R/\langle p \rangle$.

[1] (2) $\Rightarrow$ (3) Every field is an integral domain

[3] (3) $\Rightarrow$ (1) Since $0 \neq p \in R - R^\times$ we only need to show $p \mid ab \Rightarrow p \mid a$ or $p \mid b$. Then, suppose $p \mid ab$. Then $ab + \langle p \rangle = \langle p \rangle = 0_{R/\langle p \rangle}$. But $ab + \langle p \rangle = (a + \langle p \rangle)(b + \langle p \rangle)$. Because $R/\langle p \rangle$ is an integral domain we get $a + \langle p \rangle = 0_{R/\langle p \rangle}$ or $b + \langle p \rangle = 0_{R/\langle p \rangle}$. In the first case $a \in \langle p \rangle$, i.e. $p \mid a$, and in the second case $p \mid b$.

[11] 4 (a) Let $E/F$ be a field extension. Define the notion of an algebraic element $u \in E$ and its minimal polynomial.

(b) Show that $\sqrt[3]{1-i}$ is algebraic over $\mathbb{Q}$, determine its minimal polynomial

(c) Let $E/F$ be an algebraic extension and let $R \subset E$ be a subring with $F \subset R$. Show that $R$ is a field.

[2] Solution (a) We call $u \in E$ algebraic over $F$ if there exists $0 \neq f \in F[x]$ s.th. $f(u) = 0$. In this case, $\{f \in F[x] : f(u) = 0\}$ is a non-zero ideal of $F[x]$, whence generated by a unique monic polynomial, called the minimal polynomial.

[4] (b) Let $u = \sqrt[3]{1-i}$. Then $u^3 = 1-i$, so $(u^3-1)^2 = (-i)^2 = -1$, whence $u^6 - 2u^3 + 1 = -1$, ie $u^6 - 2u^3 + 2 = 0$. The polynomial $f = x^6 - 2x^3 + 2 \in \mathbb{Q}[x]$ is irreducible by Eisenstein ($p=2$) and has $f(u) = 0$. It is therefore the minimal polynomial of $u$.

[5] (c) Let $0 \neq u \in R$. Then $u^{-1}$ exists in $E$, and we need to show that $u^{-1} \in R$. By assumption, $u$ is algebraic over $F$. Let $m = a_0 + \dots + a_{n-1}x^{n-1} + x^n$ be its minimal polynomial. Since $m$ is irreducible, we have $a_0 \neq 0$ (otherwise $x \mid m$!) Also $n \geq 1$. From

$$0 = m(u) = a_0 + a_1 u + \dots + a_{n-1}u^{n-1} + u^n$$

we set $-a_0 = u(a_1 + \dots + a_{n-1}u^{n-2} + u^{n-1})$, whence

$$-a_0 u^{-1} = a_1 + \dots + a_{n-1}u^{n-2} + u^{n-1} \in R,$$

and then $u^{-1} \in R$ because $(-a_0)^{-1} \in F \subset R$.

[13] 5 (a) Give the definition of a splitting field of a polynomial $f \in F[x]$ of degree $n \geq 1$, $F$ a field.

(b) Find a splitting field $E$ of $f = (x^2-2)(x^2+1) \in \mathbb{Q}[x]$; determine $[E:\mathbb{Q}]$ and a basis of the $\mathbb{Q}$-vector space $E/\mathbb{Q}$

(c) Let $F$ be a field with $|F| = p^n$, $p$ a prime. Prove that $F$ is a splitting field of $f = x^{p^n} - x$ over $\mathbb{Z}_p$ (identified with the prime field of $F$

[2] Solution (a) A field $E$ is a splitting field of $f$ if there are $a \in F$, $u_1, \dots, u_n \in E$ s.th. $E = F(u_1, \dots, u_n)$ and $f = a(x-u_1)\cdots(x-u_n)$

[5] (b) We have $E = \mathbb{Q}(\sqrt{2}, i)$, $[E:\mathbb{Q}] = [E:\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$, where clearly $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$. Since $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ and $i \notin \mathbb{R}$, it follows that $[\mathbb{Q}(\sqrt{2})(i):\mathbb{Q}(\sqrt{2})] = 2$. So $[E:\mathbb{Q}] = 2\cdot 2 = 4$

[6] (c) Since $F \setminus \{0\}$ is a group of order $p^n - 1$, we know $a^{p^n-1} = 1$ for all $a \in F \setminus \{0\}$, a consequence of Lagrange's Theorem. Hence, multiplying by $a$, we get $a^{p^n} = a$ for all $a \in F \setminus \{0\}$. But this also holds for $a = 0$, whence $f(a) = 0$ for all $a \in F$. Since $\deg(f) = p^n$, $f$ has at most $p^n$ roots in any field. But the $p^n$ distinct elements in $F$ are all roots of $f$, so $f = \prod_{a \in F}(x-a)$ splits over $F$. Clearly $F = \mathbb{Z}_p(\{a \in F\})$ (we identify $\mathbb{Z}_p$ with the prime field of $F$)

[2] A basis of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is $1, \sqrt{2}$, and a basis of the $\mathbb{Q}(\sqrt{2})$-vector space $E$ is $1, i$. Therefore, by the Multiplication Theorem, a basis of the $\mathbb{Q}$-vector space $E/\mathbb{Q}$ is $\{1, \sqrt{2}, i, i\sqrt{2}\}$

6) Give an example of the following (without proof)

(1) an algebraically closed field, different from $\mathbb{C}$:
$\mathbb{A}$ = field of algebraic numbers

(2) a primitive element of $\mathbb{Z}_7$:
$\overline{3}$ since $\overline{3}^2 = \overline{2}$, $\overline{3}^4 = \overline{2}^2 = \overline{4}$, $\overline{3}^6 = \overline{2}\cdot\overline{4} = \overline{8} = 1$.

(3) an algebraic extension of infinite degree:
$\mathbb{A} / \mathbb{Q}$

(4) a transcendental element: $\pi$

(5) a UFD which is not a PID: $\mathbb{Z}[x]$

(6) an Euclidean domain: $F[x]$

(7) an extension of degree 5

(8) a irreducible $f \in \mathbb{R}[x]$, $\deg(f) \geq 2$

(9) a maximal ideal in $\mathbb{C}[x]$

(10) a division ring which is not a field