1

(a) True; $\mathbb{Z}_{10}^{\times} = \{1,3,7,9\}$, and $\langle 3 \rangle = \{1,3,9,7\}$, so $\mathbb{Z}_{10}^{\times}$ is cyclic.

(b) True; $|S_n/A_n| = 2$, & 2 is prime, so S_n/A_n is cyclic (all groups of prime order are cyclic).

(c) False; this is only true if R has no nontrivial zero-divisors.

(d) True; in fact all subgroups of $(\mathbb{Z},+)$ have the form $n\cdot\mathbb{Z}$.

(e) True; x^3+x+1 has no roots since $\mathbb{Z}_2=\{0,1\}$, $0^3+0+1=1$ & $1^3+1+1=1$, hence it is irreducible since the degree is 3, and irred. polys. in $F[X]$ (F a field) generate maximal ideals, so the quotient $\mathbb{Z}_2[X]/(X^3+X+1)$ is a field.

② (a)

(i) it is useful to first write σ as a product of disjoint cycles:

$$\begin{aligned}\sigma &= (1\,5\,6)(1\,3\,4)^{-1}(2\,5\,4\,6)(3\,7)^{-1}\\ &= (1\,5\,6)(1\,4\,3)(2\,5\,4\,6)(3\,7)\\ &= (1\,4\,3\,5\,6)(2\,5\,4\,6)(3\,7)\\ &= (1\,4)(2\,6)(3\,5)(3\,7)\\ &= (1\,4)(2\,6)(3\,7\,5)\end{aligned}$$

Therefore $o(\sigma) = \mathrm{LCM}(2,2,3) = \boxed{6}$.

(ii) σ = odd · odd · even = even, so indeed $\underline{\sigma \in A_7}$.

(b) $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 7 & \underbrace{? \quad ?}_{\text{missing entries: 1 and 5.}} & & 6 & 3 \end{pmatrix}$

So there are two cases:

1) $\tau(4)=1$ & $\tau(5)=5$. Then as disjoint cycles:
$$\tau = (1\,2\,4)(3\,7) \quad \text{(which is odd)}$$

2) $\tau(4)=5$ & $\tau(5)=1$, Then
$$\tau = (1\,2\,4\,5)(3\,7) \quad \text{(which is even)}$$

So $\tau \in A_7 \Rightarrow$ case 2 is correct: $\tau(4)=5$ & $\tau(5)=1$.

(c) For $n \geq 3$, we can let $\sigma = (1\,2)$ $\tau = (2,3)$ in S_n.

Then $\sigma\tau = (1\,2\,3)$ & $\tau\sigma = (1\,3\,2)$,

so $\sigma\tau \neq \tau\sigma$; this shows that S_n is non-abelian.

③

(a) By Lagrange's theorem, any subgroup of a group G of order p^2 has order $1, p,$ or p^2. Hence any proper subgroup has order 1 or p.
The only order-1 subgroup is $\{e_G\}$, which is cyclic.
Any order-p subgroup is cyclic since all prime-order groups are cyclic.

(b) Let $H \leq \mathbb{Z}_8$ be the image of φ. Then we have a surjective group hom. $\mathbb{Z}_{24} \to H$ w/ kernel $\{0,8,16\}$,
so $\mathbb{Z}_{24}/\{0,8,16\} \cong H$ (fund. thm. of group homs)

$\Rightarrow |\mathbb{Z}_{24}|/|\{0,8,16\}| = |H|$

$\Rightarrow 24/3 = |H| \Rightarrow |H| = 8.$

So H must be all of $\mathbb{Z}_8$ (since $|\mathbb{Z}_8| = 8$), so φ is surjective.

(c) By the fund. thm. again,

$$G/K \cong \operatorname{im}\varphi$$

& by Lagrange's thm. $|\operatorname{im}\varphi|$ divides $|H| = 10$.
But $|G/K| = |G|/|K|$ divides $|G| = 6$; so $|\operatorname{im}\varphi|$ is a common divisor of 6 & 10... the only possibilities are 1 & 2.
So either $|\operatorname{im}\varphi| = 1$, in which case $\frac{6}{|K|} = 1$ & $|K| = 6$,
or $|\operatorname{im}\varphi| = 2$, in which case $\frac{6}{|K|} = 2$ & $|K| = 3$.

So indeed $|K|$ must be either 3 or 6.

④ $H \leq G$ s.t. $\forall x, y \in G,\ x^{-1}y^{-1}xy \in H$.

(a)

Suppose $h \in H$ & $g \in G$.

Then
$$ghg^{-1} = (ghg^{-1}h^{-1})h$$
& setting $x = g^{-1}$, $y = h^{-1}$, we see that
$$ghg^{-1}h^{-1} = x^{-1}y^{-1}xy \in H,$$

$\Rightarrow (ghg^{-1}h^{-1})h \in H$ since H is closed under mult.

Hence $ghg^{-1} \in H$. This is true for all $g \in G$, $h \in H$, so $\underline{H \trianglelefteq G.}$

(b) For any two elements Hx, $Hy \in G/H$,

$$HxHy = Hxy$$
$$\& \ HyHx = Hyx$$

So these are equal iff $Hxy = Hyx$,

which holds iff $xy(yx)^{-1} \in H$, ie. $xyx^{-1}y^{-1} \in H$.

But this holds, since $xyx^{-1}y^{-1} = u^{-1}v^{-1}uv$, where $u = x^{-1}$ & $v = y^{-1}$,

& this lies in H by assumption.

⑤

(a) $\varphi^{-1}(P)$ is nonempty since $\varphi(0_R)=0_S \in P \Rightarrow 0_R \in \varphi^{-1}(P)$.

$\varphi^{-1}(P)$ is closed under subtraction since

$\forall a,b \in \varphi^{-1}(P)$,

$$\varphi(a-b)=\varphi(a)-\varphi(b) \in P$$

since $\varphi(a), \varphi(b) \in P$ & P is closed under subtraction.

$\Rightarrow a-b \in \varphi^{-1}(P)$.

$\varphi^{-1}(P)$ is sticky, since

$\forall a \in \varphi^{-1}(P)$ & $r \in R$,

$\varphi(ar) = \varphi(a)\cdot\varphi(r) \in P$ since $\varphi(a) \in P$ & P is sticky

& $\varphi(ra) = \varphi(r)\cdot\varphi(a) \in P$ for the same reason.

$\Rightarrow ar$ & ra are both in $\varphi^{-1}(P)$.

(b) Suppose that $ab \in \varphi^{-1}(P)$. $(a, b \in R)$

Then $\varphi(ab) \in P$, so $\varphi(a)\varphi(b) \in P$.

Since P is prime, either $\varphi(a) \in P$ or $\varphi(b) \in P$.

Hence either $a \in \varphi^{-1}(P)$ or $b \in \varphi^{-1}(P)$.

This shows that $\varphi^{-1}(P)$ is a prime ideal of P

6 (a)

Observe that $2^2+4\cdot 2+2 = 4+1+2=0$ in $\mathbb{Z}_7$

so 2 is a root of x^2+4x+2.

Factoring it out gives

$$x^2+4x+2 = (x-2)(x+6),$$

or equivalently, $(x+5)(x+6)$.

(b) Let $J=(x+5)$.

Then $J \supseteq I$ since any multiple of $(x+5)(x+6)$ is a multiple of $(x+5)$, but $J \neq I$ since $x+5 \notin (x^2+4x+2)$ (no elt. of (x^2+4x+2) can have degree 1).

// $J=(x+6)$ is the other possible answer.

(c) Both $\overline{x+5}$ & $\overline{x+6}$ are zero-divisors in $\mathbb{Z}_7[x]/I$; both are nonzero, since I has no degree 1 elements, but their product is $\overline{x^2+4x+2} = \overline{0}$.

(d) Division algorithm:

$$\begin{array}{r|l} & \quad\quad\quad x+3 \\ \hline x^2+4x+2 & x^3+0x^2+2x-1 \\ & x^3+4x^2+2x \\ \hline & \quad\quad 3x^2 \quad\quad -1 \\ & \quad\quad 3x^2+5x+6 \\ \hline & \quad\quad\quad 2x+0 \end{array}$$

Remainder

So

$$x^3+2x-1 = (x^2+4x+2)\underbrace{(x+3)}_{\text{quotient}} + \underbrace{2x}_{\text{remainder}}$$

& thus

$\overline{x^3+2x-1} = \overline{2x}$ in $\mathbb{Z}_7[x]/I$,

since $(x^3+2x-1)-2x$ is a multiple of (x^2+4x+2).

7

(a) No such two groups exist, since any group of order 5 is cyclic (since 5 is prime) & hence isomorphic to $\mathbb{Z}_5$, so any two order-5 groups are isomorphic to each other.

(b) $\mathbb{Z}_6$ (or indeed any $\mathbb{Z}_n$ w/ n composite) is a commutative ring w/ 1 but not an integral domain; note that

$$2 \cdot 3 = 0, \text{ but } 2, 3 \neq 0 \text{ in } \mathbb{Z}_6.$$

(c) In $\mathbb{Z}$, $\{0\}$ is a prime ideal ($ab=0 \Rightarrow a=0$ or $b=0$), but it is not maximal since for example $2\mathbb{Z}$ is a larger proper ideal.

(d) $$x^2+x = \underline{x(x+1)},$$

& $$x^2+x = x^2+7x+12 = \underline{(x+3)(x+4)} \quad \text{in } \mathbb{Z}_6$$

So these give two different factorizations; one can check that the factors of $x(x+1)$ are not constant multiples of the the factors in $(x+3)(x+4)$.

(e) There is no root of x^4-2 in $\mathbb{Z}_5$, as we can check by trial & error.

$$0^4 = 0 \neq 2$$
$$1^4 = 1 \neq 2$$
$$2^4 = 4^2 = 1 \neq 2$$
$$3^4 = 4^2 = 1 \neq 2$$
$$4^4 = 1^2 = 1 \neq 2$$

(all arithmetic is in $\mathbb{Z}_5$)

Or, a quicker route:
Fermat's little theorem implies that $\forall x \neq 0$ in $\mathbb{Z}_5$, $x^4 = 1 \neq 2$.