Abstract Algebra

Solutions of Final

1.

a) True.

(1) Closure: For $x, y \in \mathbb{R}\backslash\{-1\}$

$$\begin{aligned} x \circ y &= x + y + xy \\ &= (x+1)(y+1) - 1 \neq -1 \text{ since } x, y \neq -1 \end{aligned}$$

$$\Rightarrow x \circ y \in \mathbb{R}\backslash\{-1\}$$

(2) Associativity: Let $x, y, z \in \mathbb{R}\backslash\{-1\}$

$$\begin{aligned} (x \circ y) \circ z &= (x + y + xy) \circ z \\ &= x + y + xy + z + xz + yz + xyz \end{aligned}$$

$$\begin{aligned} x \circ (y \circ z) &= x \circ (y + z + yz) \\ &= x + y + z + yz + xy + xz + xyz \end{aligned}$$

$$\Rightarrow (x \circ y) \circ z = x \circ (y \circ z)$$

(3) Identity: Let $x \in \mathbb{R}\backslash\{-1\}$

$$x \circ 0 = x + 0 + 0 \cdot x = x = 0 \circ x$$

(4) Inverse: Let $x \in \mathbb{R}\backslash\{-1\}$

$$0 = x \circ x^{-1} = x + x^{-1} + x \cdot x^{-1}$$

$$\Rightarrow x^{-1} = \frac{-x}{1+x}$$

$\Rightarrow \langle \mathbb{R}\backslash\{-1\}, \circ \rangle$ is a group.

b) $\mathbb{Z}_3 \times \mathbb{Z}_6$ is NOT isomorphic to $\mathbb{Z}_{18}$ since $\mathbb{Z}_{18}$ has an element of order 18, but the elements in $\mathbb{Z}_3 \times \mathbb{Z}_6$ have orders at most 6.

c)

(1) Closed: For $a, b \in G_y$, $(ab) * y = a * (b * y) = a * y = y$, we have $ab \in G_y$.

(2) Identity: $e \in G_y$ since $e * y = y$ by the definition of group action.

(3) Inverse: For $g \in G_y$, $g^{-1} * y = g^{-1} * (g * y) = e * y = y$, hence $g^{-1} \in G_y$.

$\Rightarrow G_y$ is a subgroup of G.

d) True. Every finite integral domain is a field.

Proof. Let $R = \{a_0 = 1, a_1, \ldots, a_{100}\}$. For any $a_i \neq 0 \in R$, let ϕ_{a_i} be a map from R to $a_i R$ defined by $\phi_{a_i}(a) = a_i a$, then ϕ_{a_i} is a bijection since if $a_i a_j = a_i a_k$ then $a_j = a_k$ (R is an integral domain, so we have cancelation law). Now $a_i a \in R$ since R is a ring, we have $a_i R = \{a_i a_0, a_i a_1, \ldots, a_i a_{100}\} = R$, and hence $a_i a_j = 1$ for some j, therefore a_i is invertible, thus R is a field. $\square$

e) False: $|\mathbb{Z}_4| = 4 = |\mathbb{Z}_2 \times \mathbb{Z}_2|$. But $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ since $\overline{1} \in \mathbb{Z}_4$ has order 4, but there is no element in $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 4.

f) False: Let $f(x) = x^3 + x + 1$, consider $f(1) = 3 = 0$ in $\mathbb{F}_3$, we have $f(x) = (x+2)(x^2+x+2)$, hence $f(x)$ is reducible over $\mathbb{F}_3$.

g) True: If $N \neq \{0\}$, then there is an element $u \neq 0$ in N. Now $u \in F$ is a unit, so $u^{-1} \in F$, hence $u^{-1}u = 1 \in N$. Then for any $a \in F$, $a * 1 = a \in N$, hence $F = N$.

h)

$$\varphi_\alpha(f(x) + g(x)) = f(\alpha) + g(\alpha) = \varphi_\alpha(f(x)) + \varphi_\alpha(g(x))$$

$$\varphi_\alpha(f(x)g(x)) = f(\alpha)g(\alpha) = \varphi_\alpha(f(x))\varphi_\alpha(g(x))$$

$\Rightarrow \varphi_\alpha$ is a ring homomorphism.

i) False. Counterexample: If $N = \langle x^2 + 1 \rangle$, consider

$$\langle x^2 + 1 \rangle = \{(x^2+1)g(x) \mid g(x) \in \mathbb{Q}[x]\}.$$

All polynomials except 0 in N has degree at least 2, thus $x - 1$ not in N.

j) Observe that $1 \nmid 5$, $5 \mid 5, -15 \mid 5, 30 \mid 5, -70 \mid 5$, and $-70 \nmid 25$, by Eisenstein Criterion, it is irreducible over $\mathbb{Q}$.

2. Let $G = \{e, a, a^2, \cdots, a^{n-1}\}$, the number of generators is equal to $\#\{m | 1 < m < n, \gcd(m,n) = 1\} = \phi(n)$, since if $\gcd(i,n) = 1$, then $1 = is + nt$ for some $s, t \in \mathbb{Z}$, thus $g^1 = g^{is+nt} = g^{is}g^{nt} = g^{is}$
$\Rightarrow g \in \langle g^i \rangle$
$\Rightarrow \langle g^i \rangle = G$
If $\gcd(i,n) = d > 1$, then exists $s, t \in \mathbb{Z}$ such that $i = sd, n = td$ with $s, t < n$.
Now $(g^i)^t = g^{it} = g^{sdt} = g^{sn} = 1$
$\Rightarrow |\langle g^i \rangle| < n = |G|$
$\Rightarrow \langle g^i \rangle \neq |G|$

3. It's easy to verify it is a commutative ring with unity (verify yourself). Now for $a + bi \in \{a + bi \mid a, b \in \mathbb{Q}\}$,

$$(a+bi)^{-1} = \frac{a - bi}{a^2 + b^2}.$$

Hence $\{a + bi \mid a, b \in \mathbb{Q}\}$ is a commutative division ring.

4. First, we are going to show for any $g \in G$, $|gH| = |H|$. Let $\phi_g : H \to gH$ defined by $\phi_g(h) = gh$, then
(1) for any $gh \in gH$, we have $\phi_g(h) = gh$, hence ϕ_g is onto;
(2)For $\phi_g(h_1) = \phi_g(h_2)$, we have $gh_1 = gh_2$, which implies $h_1 = h_2$, thus ϕ_g is one-to-one.
By(1)(2), we have $|H| = |gH|$.
Second, we are going to show for any $g_1, g_2 \in G$, either $g_1H = g_2H$ or $g_1H \cap g_2H = \phi$. Suppose $g_1H \cap g_2H \neq \phi$, let $c \in g_1H \cap g_2H$, then $c = g_1h_1 = g_2h_2$

for some $h_1, h_2 \in H$. Now $g_1h_1 = g_2h_2$ implies $g_1 = g_2h_2h_1^{-1} \in g_2H$, hence $g_1H = g_2H$.
The union of all cosets of H is G, hence the cosets of H partition G into same cardinality parts, thus $|H|||G|$.

5. Consider $\mathbb{Z}$ is a cyclic group generated by 1, any subgroup N of $\mathbb{Z}$ is also cyclic, says $N = \langle a \rangle$ for some $a \in \mathbb{Z}$ (note that we can choose a be the smallest positive integer in N), now from the definition of ideal ($rn \in N$ for all $r \in \mathbb{Z}, n \in N$), we have all multiples of a are all in N.

6. Example 1: $M_{2\times 2}(\mathbb{R})$ is a noncommutative ring. (You need to verify it is a ring). It is noncommutative since

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Example 2: Let

$$Q = \{a + b * i + c * j + d * k \mid a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ij = -ji = k\}$$

Then clearly, it is noncommutative since $ij = -ji$. (Verify it is a ring yourself).

7. ($\Rightarrow$) Define $\psi : R \to R/M$ by $\psi(r) = r + M$, which is easily seen to be a ring homomorphism. Suppose we have $M \subseteq N \subseteq R$, where N is an ideal. Then $\psi(N)$ is an ideal of R/M, but since R/M is a field the only ideals are $\langle 0 + M \rangle$ and R/M. If $\psi(N) = \langle 0 + M \rangle$ then we have $N \subseteq ker(\psi) = M \Rightarrow M = N$. On the other hand, if $\psi(N) = R/M$ then we must have $N = R$. To see this note that if for all $r \in R$ there is some $r_1 \in N$ such that $\psi(r_1) = r + M = \psi(r)$, then we must have $\psi(r - r_1) = (r - r_1) + M = 0 + M$. But this means that $r - r_1 = m \in M \Rightarrow r = r_1 + m \in N$. Thus $R \subseteq N \Rightarrow N = R$. Therefore M is a maximal ideal.

($\Leftarrow$) suppose M is a maximal ideal. We already know that R/M is a commutative ring with unity, so all that remains is to show that every non-zero element has a multiplicative inverse. To this end, let $r + M \in R/M$ with $r \notin M$. Now consider the ideal $\langle r + M \rangle \in R/M$. Since ψ is a homomorphism we know that $\psi^{-1}(\langle r + M \rangle)$ is an ideal of R. Furthermore, this ideal properly contains M since $r \in \psi^{-1}(\langle r + M \rangle)$. Since M is maximal, it must be the case that $\psi^{-1}(\langle r + M \rangle) = R$. Thus $\psi(1) = 1 + M \in \langle r + M \rangle$, which means we can write $1 + M = (r + M)(s + M)$ for some $s \in R$. Hence $r + M$ has a (multiplicative) inverse and so we conclude R/M is a field.