Complete all 6 problems. In multi-part problems, you may assume the result of any part (even if you have not been able to do it) in working on subsequent parts. Please fully justify all your answers. (Points are distributed evenly between parts.)

1. (15 points) Suppose H and K are subgroups of a group G and $K \leq N_G(H)$, where $N_G(H)$ denotes the normalizer of H in G.

   (a) Prove that the subset $KH := \{xy \mid x \in K, y \in H\}$ is a subgroup of G.

   Solution: Denote by e the identity element of G. As H and K are subgroups of G, e is in both H and K, and so $e = ee$ is in KH.

   If $kh \in KH$ and $k'h' \in KH$, with $k, k' \in K$, and $h, h' \in H$, then

   $$(kh)(k'h') = kk'(k'^{-1}hk')h' .$$

   As K is contained in $N_G(H)$, we have $k'^{-1}hk' \in H$. Using that H is a subgroup of G, we obtain that $(k'^{-1}hk')h' \in H$. On the other hand, as K is a subgroup of G, we also have $kk' \in K$, and so one concludes that $(kh)(k'h') \in KH$.

   If $kh \in KH$ with $k \in K$ and $h \in H$, then

   $$(kh)^{-1} = h^{-1}k^{-1} = k^{-1}(kh^{-1}k^{-1}) .$$

   As H is a subgroup of G, $h^{-1} \in H$, and so, as K contained in $N_G(H)$, we have $kh^{-1}k^{-1} \in H$. On the other hand, as K is a subgroup of G, we also have $k^{-1} \in K$, and so $(kh)^{-1} \in KH$.

   This shows that KH contains the identity element, is stable under product and inverse. Therefore, KH is a subgroup of G.

   (b) Consider the subset $HK := \{yx \mid y \in H, x \in K\}$. Show that $KH = HK$.

   Solution: Let $kh \in KH$ with $k \in K$ and $h \in H$. As K is contained in $N_G(H)$, we have $khk^{-1} \in H$, and so $kh = (khk^{-1})k \in HK$. This proves the inclusion $KH \subset HK$.

   Conversely, let $hk \in HK$ with $h \in H$ and $k \in K$. As K is contained in $N_G(H)$, we have $k^{-1}hk \in H$, and so $hk = k(k^{-1}hk) \in KH$. This proves the inclusion $HK \subset KH$.

   The equality $KH = HK$ follows from the inclusions $KH \subset HK$ and $HK \subset KH$.

   (c) Show that $H \lhd KH$, and that $KH/H \cong K/K \cap H$.

   Solution: First note that for every $h \in H$, we have $h = eh$ with $e \in K$, because K is a subgroup of G, and so $h \in KH$. This shows the inclusion $H \subset KH$. As H is a subgroup of G and KH is a subgroup of G by a), H is a subgroup of KH.

   Let $kh \in KH$ with $k \in K$ and $h \in H$, and let $h' \in H$. Then, we have

   $$(kh)^{-1}h'(kh) = h^{-1}(k^{-1}h'k)h .$$

   As K is contained in $N_G(H)$, we have $k^{-1}h'k \in H$, and so $h^{-1}(k^{-1}h'k)h \in H$ because H is a subgroup of G. Hence, $(kh)^{-1}h'(kh) \in H$. Thus, H is stable by conjugation by elements of KH, and so H is a normal subgroup of KH.

   On the other hand, as K is contained in $N_G(H)$, the intersection $K \cap H$ is stable by conjugation by elements of K, and so $K \cap H$ is a normal subgroup of K.

   Let $\iota \colon K \to KH$ be the inclusion $k \mapsto k = ke$. In particular, ι is a group homomorphism. If $x \in K \cap H$, then $\iota(x) \in H$, that is, $\iota(K \cap H) \subset H$, and so ι induces a group homomorphism $f : K/(K \cap H) \to KH/H$.

   Let $x \in K/(K \cap H)$ such that $f(x) = e$. Let $k \in K$ be a lift of x. Then $k = \iota(k) \in H$, and so $x = e$. Hence, the kernel of f is trivial, and so f is injective.

   Let $y \in KH/H$. Let $kh \in KH$ be a lift of y, with $k \in K$ and $h \in H$. Denote by x the image of k in $K/(K \cap H)$. Then $f(x) = y$. Hence, f is surjective.

   This shows that f is a group isomorphism.

2. (Group Actions, 10 points) Let G be a finite p-group, with neutral element 1. Suppose that $\{1\} \neq H \lhd G$. Prove that $H \cap Z(G) \neq \{1\}$. (Hint: Consider a group action of G on H.)

   Solution:

   As H is a normal subgroup of G, G acts on H by conjugation: for every $g \in G$ and $h \in H$, $g.h := g^{-1}hg \in H$. If O is an orbit of the action, then

$$|O| = |G|/|S(x)|\,,$$

   where $|O|$ is the order of O, $|G|$ the order of G, and $|S(x)|$ the order of the stabilizer subgroup $S(x) \subset G$ of an element $x \in O$. If $S(x) \neq \{1\}$, then $|S(x)| \neq 1$, and so $|S(x)|$ is divisible by p, because $|S(x)|$ divides $|G|$ by Lagrange's theorem, and $|G|$ is a power of p because G is a p-group. On the other hand, $S(x) = \{1\}$ if and only if $O = \{x\}$, which is equivalent to $g^{-1}xg = x$ for all $g \in G$, that is $x \in H \cap Z(G)$.

   As H is the disjoint union of the orbits of the action, one concludes that $|H| = |H \cap Z(G)| \mod p$, where $|H|$ is the order of p and $|H \cap Z(G)|$ is the order of $H \cap Z(G)$. By assumption, $H \neq \{1\}$, so $|H| \neq 1$, and so $|H|$ is divisible by p by Lagrange's theorem because H is a subgroup of the p-group G. Hence, $|H \cap Z(G)|$ is also divisible by p. In particular, $|H \cap Z(G)| \neq 1$ and so $H \cap Z(G) \neq \{1\}$.

3. (Rings, 20 points) Let $\mathbb{C}$ denote the field of complex numbers. Choose a solution in $\mathbb{C}$ of the equation $x^2 + 3 = 0$ and call it $\sqrt{-3}$. Consider the set $R = \mathbb{Z}[\sqrt{-3}] := \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$.

   (a) Show that the addition law and multiplication law of $\mathbb{C}$ induce natural addition and multiplication laws on R. Prove that endowed with these laws, R is an integral domain.

   Solution: Let $a + b\sqrt{-3}$ and $c + d\sqrt{-3}$ be two elements of R. Note that since, $a, b, c, d \in \mathbb{Z}$ we have $a + c \in \mathbb{Z}$ and $b + d \in \mathbb{Z}$. Hence, the addition on $\mathbb{C}$ induces an addition on R given by

$$(a + b\sqrt{-3}) + (c + d\sqrt{-3}) = (a + c) + (b + d)\sqrt{-3} \in R\,.$$

   The multiplication on $\mathbb{C}$ induces a multiplication on R given by

$$\begin{aligned}(a + b\sqrt{-3}) \cdot (c + d\sqrt{-3}) &= ac + (ad + bc)\sqrt{-3} + bd\sqrt{-3}^2 \\ &= (ac + 3bd) + (ad + bc)\sqrt{-3} \in R,\end{aligned}$$

   since $ac + 2bd \in \mathbb{Z}$, and $ad + bc \in \mathbb{Z}$, for $a, b, c, d \in \mathbb{Z}$.

   Actually, R is a subring of $\mathbb{C}$, since we also have:

   - The identity for addition: $0 = 0 + 0\sqrt{-3} \in R$,
   - Inverses for addition: the additive inverse of $a + b\sqrt{-3} \in R$ is $-a - b\sqrt{-3} \in R$,
   - Identity for multiplication: $1 = 1 + 0\sqrt{-3} \in R$.

   Since R is a subring of the field $\mathbb{C}$, it is an integral domain: suppose $x, y \in R$ with $xy = 0$. Since $x, y \in \mathbb{C}$, and the zero element of $\mathbb{C}$ is the same as the zero element in R, either $x = 0 \in R$ or $x = 0 \in R$. Thus, R has no zero divisors. Since, it also contains 1, it is an integral domain.

   (b) What are the units in R? Justify your answer.

   Solution: First note that for every $x = a+b\sqrt{-3} \in R$, we have $|x|^2 = (a+b\sqrt{-3})(a-b\sqrt{-3}) = a^2+3b^2$, and so in particular $|x|^2 \in \mathbb{Z}$.

   Let $\alpha = a + b\sqrt{-3} \in R$ be a unit of R. Then, $\alpha^{-1} \in R$. From $\alpha\alpha^{-1} = 1$, we deduce that

$$|\alpha|^2 \cdot |\alpha^{-1}|^2 = 1\,.$$

   Since $\alpha, \alpha^{-1} \in R$, we have $|\alpha|^2, |\alpha^{-1}|^2| \in \mathbb{Z}$. But the only way for a product of integers to be equal to 1 is for each factor to be either 1 or -1. Thus, we have either $|\alpha|^2 = a^2 + 3b^2 = 1$ or $|\alpha|^2 = a^2 + 3b^2 = -1$. As $-1 < 0$, there are no integers satisfying the latter equation. As $a^2 + 3b^2 \geq 3$ if $b \in \mathbb{Z} \setminus \{0\}$, integer solutions of the former equation $a^2 + 3b^2 = 1$ are $a = 1, b = 0$ or $a = -1, b = 0$. Therefore the only units are 1 and -1.

(c) Give the definition of what it means for $r \in R$ to be irreducible in R. Is the element $r = 2$ irreducible in R?

Solution: An element $r \in R$ is irreducible if, whenever we write $r = a \cdot b$ with $a, b \in R$, either a or b is a unit of R.

The element $r = 2$ is irreducible in R. To see this, consider a decomposition $2 = \alpha \cdot \beta$ with $\alpha, \beta \in R$. This implies that $4 = |2|^2 = |\alpha|^2|\beta|^2$. As noted in our solution to (b), we have $|\alpha|^2, |\beta|^2 \in \mathbb{Z}$ for $\alpha, \beta \in R$.

Hence, either $|\alpha|^2 = |\beta|^2 = 2$, or $|\alpha|^2 = 4$, $|\beta|^2 = 1$, or $|\alpha|^2 = 1$, $|\beta|^2 = 4$. We claim that the first case $|\alpha|^2 = |\beta|^2 = 2$ is not possible: there are no element $\alpha = a + b\sqrt{-3} \in R$ with $|\alpha|^2 = a^2 + 3b^2 = 2$: indeed $a^2 + 3b^2 \geq 3$ if $b \neq 0$, and $a^2 = 2$ has no integer solutions. Therefore, either $|\alpha|^2 = 4$, $|\beta|^2 = 1$, or $|\alpha|^2 = 1$, $|\beta|^2 = 4$. Up to relabeling α and β, one can assume that $|\alpha|^2 = 1$, $|\beta|^2 = 4$. But if $|\alpha|^2 = 1$, then α is a unit because, if $\alpha = a + b\sqrt{-3}$, $\alpha^{-1} = (a - b\sqrt{-3})/|\alpha|^2 = a - b\sqrt{-3} \in R$.

(d) If $x, y \in R$, and 2 divides xy, does it follow that 2 divides either x or y?

Solution: No: let $x = 1 + \sqrt{-3}$ and $y = 1 - \sqrt{-3}$. Then 2 divides $4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$, but 2 divides neither x nor y.

4. (Field extensions and Galois Theory, 20 points) Recall that an *automorphism* ϕ of a field F is a ring homomorphism $\phi : F \to F$ which is an isomorphism.

(a) Let K be an extension field of $\mathbb{Q}$, and let ϕ be an automorphism of K. Prove that $\phi(q) = q$ for all $q \in \mathbb{Q}$.

Solution: First note that $\phi(0) = 0$ and $\phi(1) = 1$ because ϕ is a ring homomorphism.

For every $n \in \mathbb{Z}$, $\phi(n) = \phi((n-1)+1) = \phi(n-1)+\phi(1) = \phi(n-1)+1$ because ϕ is a ring homomorphism. If follows by induction on n that $\phi(n) = n$ for all $n \in \mathbb{Z}_{\geq 0}$. As ϕ is a ring homomorphism, we also have $\phi(n) + \phi(-n) = \phi(n - n) = \phi(0) = 0$ for all $n \in \mathbb{Z}$, so $\phi(-n) = -\phi(n)$. This shows that $\phi(n) = n$ for all $n \in \mathbb{Z}$.

As ϕ is a ring homomorphism, we have $\phi(n)\phi(1/n) = \phi(n/n) = \phi(1) = 1$ for all non-zero $n \in \mathbb{Z}$, and so $\phi(1/n) = 1/n$.

Finally, for a general element $a/b \in \mathbb{Q}$ with $a \in \mathbb{Z}$ and non-zero $b \in \mathbb{Z}$, we obtain

$$\phi(a/b) = \phi(a)\phi(1/b)\,,$$

because ϕ is a ring homomorphism, and so $\phi(a/b) = a1/b = a/b$.

(b) Define the *Galois group* $G(K/F)$ for a field extension $F \subseteq K$.

Solution: Given a field extension $F \subseteq K$, the Galois group $G(K/F)$ is the group of automorphisms ϕ of K fixing F, that is, such that $\phi(x) = x$ for all $x \in F$.

(c) Show that $G(\mathbb{Q}(i)/\mathbb{Q})$ is a cyclic group of order two. Your proof should be complete and self-contained except that you may assume part (a). In particular, your proof should not rely on the Fundamental Theorem of Galois Theory.

Solution: Let ϕ be an automorphism of $\mathbb{Q}(i)$ fixing $\mathbb{Q}$. We have $\phi(i)^2 = \phi(i^2) = \phi(-1) = -1$, so $\phi(i) = i$, or $\phi(i) = -i$. If $\phi(i) = i$, then, for every $a, b \in \mathbb{Q}$, $\phi(a + ib) = a + \phi(i)b = a + ib$, and so ϕ is the identity. If $\phi(i) = -i$, then, for every $a, b \in \mathbb{Q}$, $\phi(a+ib) = a+\phi(i)b = a-ib$ and so ϕ is necessarily the restriction to $\mathbb{Q}(i)$ of the complex conjugation on $\mathbb{C}$. Conversely, the complex conjugation is an automorphism of $\mathbb{C}$ fixing $\mathbb{Q}$, and so its restriction to $\mathbb{Q}(i)$ is an automorphism of $\mathbb{Q}(i)$ fixing $\mathbb{Q}$.

Therefore, the Galois group $G(\mathbb{Q}(i)/\mathbb{Q})$ consists of two elements: the identity and the complex conjugation. Finally, note that a group of order two is automatically cyclic, generated by the non-identity element.

(d) Give an example of a field extension $F \subseteq K$ so that $[K : F] = 4$, but $|G(K/F)| = 2$. Justify your example.

Solution: We can take $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt[4]{2})$.

Let us show that $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}] = 4$. First, we have $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$, because $(\sqrt{2})^2 = 2$ and $\sqrt{2} \notin \mathbb{Q}$. We claim that $\sqrt[4]{2} \notin \mathbb{Q}(\sqrt{2})$. Indeed, if we had $\sqrt[4]{2} = a + \sqrt{2}b$ with $a, b \in \mathbb{Q}$, we would have $\sqrt{2} = (a+\sqrt{2}b)^2 = a^2 + 2b^2 + 2\sqrt{2}ab$, and so $\sqrt{2}$ would be rational, contradiction. From $(\sqrt[4]{2})^2 = \sqrt{2}$ and $\sqrt[4]{2} \notin \mathbb{Q}(\sqrt{2})$, we deduce that $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}(\sqrt{2})] = 2$, and so finally $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}] = 4$.

Finally, we show that $|G(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})| = 2$. If ϕ is an automorphism of $\mathbb{Q}(\sqrt[4]{2})$ fixing $\mathbb{Q}$, then $\phi(\sqrt{2})^2 = \phi(2) = 2$, so $\phi(\sqrt{2}) = \sqrt{2}$ or $-\sqrt{2}$. But we also have $\phi(\sqrt[4]{2})^2 = \phi(\sqrt{2})$, and $\phi(\sqrt[4]{2})^2 \geq 0$ because $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$, so necessarily $\phi(\sqrt{2}) = \sqrt{2}$ and ϕ is the identity in restriction to $\mathbb{Q}(\sqrt{2})$. Similarly, $\phi(\sqrt[4]{2})^4 = 2$ and $\phi(\sqrt[4]{2}) \in \mathbb{R}$ imply that either $\phi(\sqrt[4]{2}) = \sqrt[4]{2}$ or $\phi(\sqrt[4]{2}) = -\sqrt[4]{2}$. If $\phi(\sqrt[4]{2}) = \sqrt[4]{2}$, then ϕ is the identity. If $\phi(\sqrt[4]{2}) = -\sqrt[4]{2}$, then ϕ is the automorphism sending $a + b\sqrt[4]{2}$ to $a - b\sqrt[4]{2}$ for every $a, b \in \mathbb{Q}(\sqrt{2})$.

5. (Modules, 10 points) Let R be a ring. A left R-module N is called *simple* if it is not the zero module and if it has no left R-submodules except N and the zero submodule.

   (a) Prove that any simple left R-module N is isomorphic to R/M, where M is a maximal left ideal of R.

   Solution: Let $n \in N$ be a non-zero element of N. Define

$$\begin{aligned} \varphi : R &\longrightarrow N \\ r &\longmapsto r \cdot n, \end{aligned}$$

   which is a nonzero map (since n is nonzero). Since the image is a submodule of N, and N is simple, the image needs to be N: $\mathrm{Im}(\varphi) = N$.

   By the first isomorphism theorem, we get

$$R/\ker(\varphi) \cong \mathrm{Im}(\varphi) \cong N.$$

   Under this isomorphism left R-submodules of N correspond to left R-submodules of $R/\ker(\varphi)$. Since, N is simple, this implies that $R/\ker(\varphi)$ has no left R-submodules except the zero submodule and itself. This enforces

$$M := \ker(\varphi),$$

   to be a maximal ideal. Elsewise, there would be an ideal $J \neq R$ containing $\ker(\varphi)$, such that R/J is a left R-submodule of R, which is a contradiction.

   (b) Prove *Schur's Lemma*: Let $\phi : S \to S'$ be a homomorphism of simple left R-modules. Then either ϕ is zero, or it is an isomorphism.

   Solution: The image $\mathrm{Im}(\phi)$ of ϕ is a left R-submodule of S'. As S' is simple, either $\mathrm{Im}(\phi) = \{0\}$ or $\mathrm{Im}(\phi) = S'$. If $\mathrm{Im}(\phi) = \{0\}$, then $\phi = 0$.

   From now on, assume that $\mathrm{Im}(\phi) = S'$. Then, ϕ is surjective. On the other hand, the kernel $\ker(\phi)$ of ϕ is a left R-submodule of S, and so, as S is simple, either $\ker(\phi) = \{0\}$ or $\ker(\phi) = S$. The second option $\ker(\phi) = S$ would imply $\phi = 0$, in contradiction with the assumption $\mathrm{Im}(\phi) = S'$. Hence, we have $\ker(\phi) = \{0\}$, and so ϕ is also injective. We conclude that ϕ, being injective and surjective, is an isomorphism.

6. (Linear Algebra, 15 points) Let $A \in M_r(F)$ be a square $(r \times r)$-matrix with entries in a field F. Let I denote the identity matrix in $M_r(F)$. Fix an algebraic closure $\overline{F}$ of F.

   (a) If $A^n = I$ for some positive integer n, show that the eigenvalues of A are nth roots of unity in $\overline{F}$.

   Solution: Let λ be an eigenvalue of A. Then, there exists a (non-zero) eigenvector v such that $Av = \lambda v$. In particular, $A^n v = \lambda A^{n-1} v = \cdots = \lambda^n v$ for all positive integers n. Hence, the assumption $A^n = I$ implies $v = \lambda^n v$, so $\lambda^n = 1$, that is λ is a nth root of unity.

   (b) Prove that if A is nilpotent, then 0 is the only eigenvalue of A.

   Solution: Let λ be an eigenvalue of A. Then, there exists a (non-zero) eigenvector v such that $Av = \lambda v$. In particular, $A^n v = \lambda A^{n-1} v = \cdots = \lambda^n v$ for all positive integers n. If A is nilpotent, there exists a positive integer n such that $A^n = 0$, so $0 = \lambda^n v$, so $\lambda^n = 0$, and so $\lambda = 0$.

(c) If 0 is the only eigenvalue of A in F, must A be nilpotent? Justify your answer.

Solution: The matrix A is not necessarily nilpotent if F is not algebraically closed, because A can have other non-zero eigenvalues in $\overline{F}$. For example, if

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$$

and $F = \mathbb{R}$, then 0 is the only eigenvalue of A in $\mathbb{R}$, but A is not nilpotent by (b) because A has two other non-zero eigenvalues i and $-i$ in $\mathbb{C}$.