1. Let $G$ be a group and $G \to G \times G$ the diagonal map that sends $g$ to $(g, g)$ for each $g \in G$. When is the image a normal subgroup of $G \times G$, endowed with the componentwise operation?

2. (i) Show that any finite group with at least 3 elements admits an automorphism that is not the identity map.
(ii) Is the corresponding statement true if one replaces “group” with “ring”?

3. Let $G$ be the group of invertible $(2 \times 2)$–matrices with entries in the finite field with $p$ elements, $p$ a positive prime number.
(i) What is the size of a Sylow $p$–subgroup of $G$?
(ii) How many such Sylow $p$-subgroups are there in $G$?

4. Show that the index of the centre of a finite group is never a prime number (1 is not prime!)

5. If $H < G$ is a proper subgroup of a finite group $G$, show that $\cup_{g \in G} gHg^{-1}$ is not equal to $G$.

6. (i) Show that the matrices

$$A = \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix}$$

with $a, b, c$ integers, form a commutative ring $R$ under the usual addition and multiplication of matrices.
(ii) Determine all invertible elements as well as all zero divisors of $R$.

7. (i) Prove that the multiplicative group of a finite field must be cyclic. (You may use the Fundamental Theorem of abelian groups).
(ii) Suppose $p \in \mathbb{Z}$ is an odd prime. State and prove necessary and sufficient conditions on $p$ for $-1$ to be a square in $\mathbb{F}_p$.
(iii) State and prove necessary and sufficient conditions that $-1$ is a square in $\mathbb{F}_{p^2}$.
8. Find an example of an irreducible cubic polynomial in $\mathbb{F}_3[x]$.

9. (i) What is the Galois group of the splitting field of $f(x) = x^3 - 2x - 3$ over $\mathbb{Q}$?
(ii) Find an example of a cubic polynomial $f(x) \in \mathbb{Z}[x]$ whose splitting field has Galois group $S_3$ over $\mathbb{Q}$ but $A_3$ over $\mathbb{Q}(i)$.

10. Suppose $D, D'$ are distinct non-squares in $\mathbb{Q}$. Show that $\mathbb{Q}(\sqrt{D}, \sqrt{D'})/\mathbb{Q}$ is an extension of degree either 2 or 4.
(ii) Show that the extension is of degree 4 if and only if $DD'$ is a non-square in $\mathbb{Q}$.
(iii) In this case, where the extension is of degree 4, describe all the intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{D}, \sqrt{D'})$.

11. Prove or disprove: the fields $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{7})$ are isomorphic as fields over $\mathbb{Q}$.

12. Suppose $F$ is a field and $f(x) \in F[x]$ is irreducible of degree $n$. For any $g(x) \in F[x]$, consider $h(x) = f(g(x))$. Show that every irreducible factor of $h(x)$ has degree divisible by $n$. 