All questions carry equal weight. State answers clearly and carefully, and justify all assertions with proofs or counterexamples. You may not use any books or notes.

(1) Suppose G is a group, and N a normal subgroup, not equal to all of G. Suppose that there are no subgroups H of G containing N and not equal to N or G. Show that N has finite index in G, and this index is a prime number.

Solution: recall that subgroups of G/N are in one-to-one corresponce with subgroups of G containing N (Prop. 3.8.7(b)), simply by considering images and preimages under the natural map $G \to G/N$. Thus, we see that the only subgroups of G/N are the trivial group and all of G/N. This means in particular that every non-trivial element $x \in G/N$ must satisfy $< x >= G/N$, so G/N is cyclic. We note that we cannot have $G/N \cong \mathbb{Z}$, since $\mathbb{Z}$ has many subgroups, so $|G/N|$ is finite. We also see that we must have $|G/N|$ prime, since if $|G/N| = ab$ with neither of a, b equal to 1, then x^a would have order b, and generate a subgroup of G/N not equal to either the trivial group or the whole thing.

(2) Let G be a group of order 12.

(a) Show that the number of subgroups of order 3 is either 1 or 4.

Solution: by the Sylow theorems, the number of subgroups of order 3 must be congruent to 1 mod 3, and must divide $12/3 = 4$. This only allows 1 or 4.

(b) Suppose that there are four subgroups of order 3, and write them $P_1, \dots, P_4$. Show that if $i \neq j$, then $P_i \cap P_j = \{e\}$.

Solution: Since the P_i each have order 3, they are cyclic, and generated by any non-trivial element in them. Hence if $x \neq e$ were in P_i and P_j, we would have $P_i = P_j = \{e, x, x^2\}$.

(c) Continuing from (b), show that $G \smallsetminus (P_1 \cup \dots P_4) \cup \{e\}$ is a subgroup of G having order 4.

Solution: from (b), we see that this is a set with $12-9+1 = 4$ elements, so we just need to check that it is a subgroup. However, by the Sylow theorems, we know that there exists (at least one) Sylow 2-subgroup, which has order 4. Except for e, the elements of this group must have order 2 or 4, so cannot be in the P_i, and must consist precisely of the set $G \smallsetminus (P_1 \cup \dots P_4) \cup \{e\}$.

(d) Conclude that G either has a normal subgroup of order 3, or of order 4.

Solution: in the case that there are 4 subgroups of order 3, we showed in (c) that there can be only one subgroup of order 4, which then must be normal, since any conjugate subgroup would also have order 4. On the other hand, in the case that there is only 1 subgroup of order 3, it must be normal for the same reason.

(3) Show that no commutative ring has its underlying additive group isomorphic to $\mathbb{Q}/\mathbb{Z}$.

Solution: let R be a commutative ring, and suppose we have an isomorphism of groups $f : (R, +) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$. First note that we cannot have $0 = 1$ in R, since this means $R = \{0\}$, and cannot be isomorphic to a non-trivial group. Consider the image $f(1)$ in $\mathbb{Q}/\mathbb{Z}$; this is necessarily $[a/b]$ for some $a/b \in \mathbb{Q}$. Note that $b[a/b] = 0$ in $\mathbb{Q}/\mathbb{Z}$, so since f is injective, we must have $b \cdot 1 = 0$ in R (where here we are considering multiplication by b in terms of repeated addition, since $b \in \mathbb{Z}$). But finally, consider $x := f^{-1}[a/(b^2)] \in R$. We have $f(b \cdot x) = b \cdot f(x) = [a/b]$, so since f is injective, we have $b \cdot x = 1$. But $b \cdot 1 = 0$, so $b \cdot x = b \cdot 1 \cdot x = 0$, and we find $0 = 1$ in R, which is a contradiction.

(4) Show that if R is an integral domain, and $G \subset (R^{\times}, \cdot)$ which is a multiplicative group of finite order n, then G must be cyclic. Hints: consider the least common multiple of the orders of elements of G. Also consider the roots of the polynomials $x^d - 1$ in $R[x]$.

Solution: Let m be the least common multiple of the orders of elements of G. G is a finite abelian group, so we can write it as isomorphic to $\mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \mathbb{Z}/p_k^{e_k}\mathbb{Z}$ for primes p_i, and using that the order of an element $(x_1, \ldots, x_k)$ in a product is the lcm of the orders of each of the x_i, we see that the element $(1, \ldots, 1)$ has order equal to the lcm of all the orders of elements of the group. That is, G actually has an element of order m.

We now claim that $m = n$. But this is easy: the elements of G all have order dividing m, so in R they are roots of the polynomial $x^m - 1$. This means there can be at most m of them, so $|G| \leqslant m$. But $|G| \geqslant m$ since G contains an element of order m, so we conclude $|G| = m$, and G is cyclic, as desired.