1. Short answer questions (3 points each).

(a) How many elements are in the group A_5?

Solution: $5!/2 = 60$

(b) Give an example of a simple group with more than 2 elements.

Solution: $\mathbb{Z}/3\mathbb{Z}$.

(c) What does the Jordan-Hölder theorem say?

Solution: For any finite group G, there exists a composition series $G = G_n \geq G_{n-1} \geq \cdots \geq G_1 \geq G_0 = \{e\}$ where each $G_{i+1} \geq G_i$ is normal and G_{i+1}/G_i is simple. Furthermore, the length of such a composition series is independent of the series chosen, furthermore, the factors G_{i+1}/G_i are independent up to ordering and isomorphism.

(d) What does the class equation say?

Solution: If G is a finite group then $|G| = |Z(G)| + \sum_x [G : C_G(x)]$ where the sum is over x in distinct conjugacy classes of size ≥ 2.

(e) Give an example of a group G acting on a set S such that $S \neq G$.

Solution: The invertible 2×2 matrices acting on vectors in $\mathbb{R}^2$ by left multiplication.

(f) Is every finite subgroup of the multiplicative monoid of an integral domain cyclic?

Solution: yes.

(g) Compute the inverse of $\overline{x+1}$ in the field $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2 + x + 1)$.

Solution: x

(h) Give two equivalent definitions of a prime ideal in a commutative ring.

Solution: An ideal $P \subseteq R$ is prime f $ab \in P$ implies $a \in P$ or $b \in P$. Equivalently, P is prime if R/P is an integral domain.

(i) What is the stabilizer of $(12) \in S_3$ where S_3 acts on itself by conjugation?

Solution: $\{1, (12)\}$

2. Suppose G acts transitively in a finite set X and let H be a normal subgroup of G. Let $O_1, \ldots, O_r$ denote the distinct orbits of H.

(a) Prove that G acts transitively on $\{O_i\}$ by left multiplication. Use this to deduce that all the orbits have the same cardinality. (10 points)

Solution: Fix some $a_i \in O_i$. We define $g \cdot O_i = \{g.x \mid x \in O_i\}$. We need to show that $g \cdot O_i = O_j$ for some j. But

$$\{g.x \mid x \in O_i\} = \{gh.a_i \mid h \in H\} = \{h'.(g.a_i) \mid h' \in H\}$$

where the second equality comes from normality of H. But $g.a_i$ is in some orbit O_j and hence the right side is exactly that orbit.

(b) Prove that if $a \in O_1$ then $|O_1| = |H : H \cap \mathrm{Stab}_G(a)|$ and show that $r = |G : H \cdot \mathrm{Stab}_G(a)|$. (16 points)

Solution: We know that $|O_1| = |H|/|\mathrm{Stab}_H(a)|$ since H acts transitively on O_1 but $\mathrm{Stab}_H(a) = \mathrm{Stab}_G(a) \cap H$. So the first part follows.

For the second part, $H \cdot \mathrm{Stab}_G(a)$ as a goal, viewed as the stabilizer of Gs action on an orbit. Certainly H stabilizes any orbit, but we need to show that $H \cdot \mathrm{Stab}_G(a)$ does as well. Choose an arbitrary $y = h \cdot a \in O_1$ and $h'g \in H \cdot \mathrm{Stab}_G(a)$. Thus

$$(h'g).y = (h'gh).a = (h'h''g).a = (h'h'').(g.a) = (h'h'').a \in H.a = O_1$$

where we used normality of H in the second equality and we used that $g \in \mathrm{Stab}_G(a)$ in the 4th equality. So $H \cdot \mathrm{Stab}_G(a) \subseteq \mathrm{Stab}_G(O_1)$. For the other containment, choose $g \in \mathrm{Stab}_G(O_1)$. Hence $g.a = h.a$ for some $h \in H$. Thus $h^{-1}g.a = a$. So $h^{-1}g \in \mathrm{Stab}_G(a)$ and hence $g \in H \cdot \mathrm{Stab}_G(a)$.

3. Show there is no simple group of order $224 = 2^5 \cdot 7$. (21 points)

Solution: Suppose G is simple of order 224. Then n_7 is 1 mod 7 and divides 32. The possibilities are $1, 8$. If 8, then there are $6 \cdot 8 = 48$ elements. Next note n_2 is equal to 1 mod 2 and divides 7. So there are 7. This gives a map $G \to S_7$. But 7! is divisible by at most 2^4.

4. **(a)** Find all the prime ideals of $\mathbb{Z}[x]/(6, x^2+1)$. (16 points)

Solution: This is the same as finding the primes of $\mathbb{Z}[x]$ that contain $(6, x^2+1)$. Suppose Q is such a prime. If Q contains 2 then $x^2+1 \in Q$, so $x^2+2x+1 \in Q$ so $x+1 \in Q$ and $Q = (2, x+1)$. Next if Q contains 3, then Q contains x^2+1 which is irreducible mod 3. So then $Q = (3, x^2+1)$. Thus the primes are

$$\{(3, x^2+1), (2, x+1)\}.$$

(b) Suppose that R is an integral domain and $Q \subseteq R$ is a prime ideal and let $W = R \setminus Q$ be a multiplicative set. Show that $W^{-1}R$ has a unique maximal ideal. (10 points)

Solution: Recall that the bijection from primes in R that intersect W trivially with those primes of W^{-1} is order preserving since the bijection is either given by $Q \mapsto W^{-1}Q$ or $P \subseteq W^{-1}R$ is mapped to $P \cap R$. Now, suppose that $Q' \subseteq R$ is a prime such that $Q' \cap W = \emptyset$. Since W is the complement of Q, we see that $Q' \subseteq Q$, thus $W^{-1}Q' \subseteq W^{-1}Q$ and so $W^{-1}Q$ is the unique maximal ideal of $W^{-1}R$.