Final Exam

Instructions: Solve *two* problems from Part 1 and *two* problems from Part 2. You may use any results proved in class or in the problem sets, except for the specific question being asked. You should clearly state any facts you are using. You are also allowed to use anything stated in one problem to solve a different problem, even if you have not yet proved it. Remember to show all your work, and to write clearly and using complete sentences. No calculators, notes, cellphones, smartwatches, or other outside assistance allowed.

Part 1: Groups

Choose *two* of the following problems.

(1) (a) Show that there exists a nonabelian group of order 27.

Proof. We will construct a nonabelian semidirect product of $\mathbb{Z}/9$ by $\mathbb{Z}/3$, which has order $9 \cdot 3 = 27$. To this end, first note that the map ϕ of multiplication by $[4]$ in $\mathbb{Z}/9$ is group automorphism that has order 3 in $\mathrm{Aut}(\mathbb{Z}/9)$. Indeed, we have

$$\phi^3([n]) = [4]^3[n] = [64][n] = [1][n] = [n]$$

in $\mathbb{Z}/9$, so ϕ^3 is the identity in $\mathrm{Aut}(\mathbb{Z}/9)$, and ϕ is not the identity itself since $\phi([1]) = [4]$. Thus, by the UMP of cyclic groups, there is a homomorphism $\psi : \mathbb{Z}/3 \to \mathrm{Aut}(\mathbb{Z}/9)$ given by $\psi([1]) = \phi$. Then the group $\mathbb{Z}/9 \rtimes_\psi \mathbb{Z}/3$ is a nonabelian group of order 27. □

(b) Give, with justification, a presentation for the group you found in part (a).

Proof. We claim that $\langle x, y \mid x^9 = y^3 = e, yx = x^4y\rangle$ is a presentation for the group $G = \mathbb{Z}/9 \rtimes_\psi \mathbb{Z}/3$. Let H be the group with presentation $\langle x, y \mid x^9 = y^3 = e, yx = x^4y\rangle$. Note that G is generated by the elements $g := ([1], [0])$ and $h := ([0], [1])$, since we can write an arbitrary element $([i], [j])$ as $([i], [0])([0], [j]) = g^i h^j$ (here we are abusing notation by using multiplicative notation in terms of g and h). Note also that the relations $g^9 = e$, $h^3 = e$ hold in G, as well as

$$hg = (\psi([1]), [1]) = ([4], [1]) = g^4h.$$

It follows from the UMP for presentations that there is a unique homomorphism $\alpha : H \to G$ given by $\alpha(x) = g$, $\alpha(y) = h$. Since $g, h \in \mathrm{im}(\alpha)$, we have $G = \langle g, h\rangle \subseteq \mathrm{im}(\alpha) \subseteq G$, so α is surjective. Then by using the relations $x^9 = y^3 = e$ in H, we can rewrite any element as products of x^i and y^j with $0 \leq i < 9$, $0 \leq j < 3$. Then using the relation $yx = x^4y$, we can rewrite any element as a product with a power of x on the left and a power of y on the right, and again using the relations $x^9 = y^3 = e$, in the form x^iy^j with $0 \leq i < 9$, $0 \leq j < 3$. This shows that $|H| \leq 27$. It follows that α must also be injective, hence an isomorphism. This justifies the presentation claimed. □

(2) Prove that no group of order $224 = 2^5 \cdot 7$ is simple.

Proof. By the Sylow Theorem, we have that the number of Sylow 2-subgroups is congruent to 1 modulo 2 and divides 7, hence is either 1 or 7.

If there is only one, then it is normal, and in particular a nontrivial proper normal subgroup, so G is not simple.

Consider the case that there are seven Sylow 2-subgroups. Then G acts on the set of these seven Sylow 2-subgroups by conjugation. By the Sylow Theorem, this action is transitive, and in particular nontrivial. Consider the permutation representation $\rho : G \to S_7$ associated to this action (where we have identified $\mathrm{Perm}(\mathrm{Syl}_2(G))$ with S_7). We claim that the kernel of ρ is a nontrivial proper normal subgroup. Since ρ corresponds to a nontrivial action, it is a nontrivial homomorphism, so $\ker(\rho)$ is a proper subgroup of G. To see that $\ker(\rho)$ is nontrivial, suppose for a contradiction that ρ is injective. Then $G \cong \mathrm{im}(\rho) \leq S_7$, so $|G|$ divides $|S_7| = 7!$ by Lagrange. But $|G| = 2^5 \cdot 7$ and $7! = 7 \cdot 5 \cdot 3^2 \cdot 2^4$, so this is not true, and thus ρ is not injective. It follows that the kernel of ρ is a nontrivial proper normal subgroup, so G is not simple in this case either. □

(3) Prove that $\mathbb{Q}/\mathbb{Z}$ is not a finitely generated group.

Proof 1. To obtain a contradiction, suppose that $\mathbb{Q}/\mathbb{Z}$ is finitely generated. Let

$$\left\{\frac{a_1}{b_1}+\mathbb{Z}, \frac{a_2}{b_2}+\mathbb{Z}, \ldots, \frac{a_t}{b_t}+\mathbb{Z}\right\}$$

be a generating set. Consider $\frac{1}{2b_1\cdots b_t}+\mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. We must then have

$$\frac{1}{2b_1\cdots b_t}+\mathbb{Z} = \sum_i n_i \frac{a_i}{b_i}+\mathbb{Z}$$

for some $n_1, \ldots, n_t \in \mathbb{Z}$. This means

$$\frac{1}{2b_1\cdots b_t} = n_0 + \sum_i n_i \frac{a_i}{b_i}$$

for some $n_0, n_1, \ldots, n_t \in \mathbb{Z}$, so we have

$$1 = 2b_1\cdots b_t + \sum_i 2n_i a_i c_i$$

where $c_i = b_1\cdots b_t/b_i \in \mathbb{Z}$. Note that this is an equation of integers. But this yields a contradiction, as the left-hand side is odd and the right-hand side is even. We conclude that no finite generating set exists; i.e., this is not a finitely generated group. □

Proof 2. To obtain a contraction, suppose that $\mathbb{Q}/\mathbb{Z}$ is finitely generated. Since this is a quotient of an abelian group, it is abelian, so it is a finitely generated abelian group. Then by the structure theorem for finitely generated abelian groups, we have an isomorphism

$$\mathbb{Q}/\mathbb{Z} \cong \mathbb{Z}^r \times \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t.$$

Note first that $r = 0$; if $r > 0$, then these is an element of infinite order in the RHS, but any element $\frac{a}{b}+\mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ has finite order (since $b\left(\frac{a}{b}+\mathbb{Z}\right) = a+\mathbb{Z} = 0+\mathbb{Z}$). But if $r = 0$, then the RHS is a finite group, and $\mathbb{Q}/\mathbb{Z}$ is infinite (e.g., $\frac{1}{n}+\mathbb{Z}$ are distinct). This gives the desired contraction. □

Part 2: Rings

Choose *two* of the following problems.

(4) Let R be a ring. Let I and J be ideals of R, and recall that $I + J = \{a + b \mid a \in I,\, b \in J\}$.

(a) Show that if $I = (S)$ and $J = (T)$ for some subsets $S, T \subseteq R$, then $I + J = (S \cup T)$.

Proof 1. By definition (S) is the smallest ideal containing S.
To show that $I + J \subseteq (S \cup T)$, note that $(S \cup T)$ is an ideal containing S and T, and hence containing $(S) = I$ and $(T) = J$. Then if $a \in I$ and $b \in J$, since $a, b \in (S \cup T)$ and $(S \cup T)$ is an ideal, $a + b \in (S \cup T)$.
To show that $(S \cup T) \subseteq I + J$, recall that $I + J$ is an ideal, and $S \subseteq I \subseteq I + J$ and $T \subseteq J \subseteq I + J$ imply $S \cup T \subseteq I + J$, so $(S \cup T) \subseteq I + J$. □

Proof 2. We have the concrete description $(S) = \{\sum r_i s_i r_i' \mid s_i \in S, r_i, r_i' \in R\}$.
To show that $I + J \subseteq (S \cup T)$, given $a \in I = (S)$ we can write $a = \sum r_i s_i r_i'$ for some $s_i \in S, r_i, r_i' \in R$ and $b \in J = (T)$ we can write $b = \sum q_i t_i q_i'$ for some $t_i \in T, q_i, q_i' \in R$. Then $a + b = \sum r_i s_i r_i' + \sum q_i t_i q_i'$ gives an expression of $a + b$ as a sum of elements of the form $x_i y_i x_i'$ with $y_i \in S \cup T$ and $x_i, x_i' \in R$. This shows that $I + J \subseteq (S \cup T)$.
To show that $(S \cup T) \subseteq I + J$, an element of $z \in S \cup T$ can be written as a sum of elements of the form $x_i y_i x_i'$ with $y_i \in S \cup T$ and $x_i, x_i' \in R$. Collecting the indices with $y_i \in S$ into one sum a and the indices with $y_i \in T$ into another sum b, we have $a \in (S) = I$ and $b \in (T) = J$, and $z = a + b \in I + J$. □

(b) Let $\pi : R \to R/I$ be the quotient homomorphism. Show that $\dfrac{R/I}{\pi(J)} \cong \dfrac{R}{I + J}$.

Proof 1. Consider the quotient homomorphism $\tau : R \to R/(I + J)$. Note that $I \subseteq I + J = \ker(\tau)$, so the UMP of quotient rings yields a homomorphism $\overline{\tau} : R/I \to R/(I + J)$ given by the rule $\overline{\tau}(r + I) = r + I + J$. Since τ is surjective, $\overline{\tau}$ is as well.
We claim that $\ker(\overline{\tau}) = \pi(J)$. Indeed,

$$\overline{\tau}(r + I) = 0_{R/(I+J)} \Leftrightarrow r + I + J = 0 + I + J \Leftrightarrow r \in I + J \Leftrightarrow r = a + b$$

for some $a \in I, b \in J$, whence $r + I = (a + b) + I = b + I \in \pi(J)$. Conversely, if $r + I \in \pi(J)$, then $r + I = b + I$ for some $b \in J$, and then $r = a + b$ for some $a \in I, b \in J$ and $\overline{\tau}(r + I) = 0_{R/(I+J)}$. This justifies the claim.
Thus, by the First Isomorphism Theorem, $R/(I + J) \cong (R/I)/\pi(J)$. □

Proof 2. Note that

$$\pi(J) = \{b + I \in R/I \mid b \in J\} = \{a + b + I \in R/I \mid a \in I, b \in J\} = \frac{I + J}{I}.$$

Then applying the Cancelling Isomorphism Theorem to $R \supseteq I + J \supseteq I$, we get an isomorphism

$$\frac{R}{I + J} \cong \frac{R/I}{(I + J)/I} \cong \frac{R/I}{\pi(J)}.$$

□

(5) (a) Prove that a finite integral domain must be a field.

Proof 1. Let R be a finite domain, and consider any nonzero element $x \in R$. Since R is finite, there are only finitely many elements of the form x^n with $n \geqslant 0$. In particular, there exist $n > m$ such that $x^n = x^m$. Thus by the cancellation rule, we have

$$x^m \cdot x^{n-m} = x^m \implies x^{n-m} = 1.$$

Note that $a = n - m > 0$ and $x^a = 1$. In particular, x is a unit, with inverse x^{a-1}. We conclude that R is a field. □

Proof 2. Let R be a finite domain, and consider any nonzero element $x \in R$. Consider the function $T_x : R \to R$ given by $T_x(r) = xr$. Note that T_x is injective, since $T_x(r) = T_x(s)$ implies $xr = xs$ implies $r = s$ since R is a domain and x is nonzero. Since R is finite, T_x is then surjective. In particular, there exists $y \in R$ such that $1 = T_x(y) = xy$, and thus x is a unit with inverse y. We conclude that R is a field. □

(b) Prove[1] that if R is a commutative ring and $P \subseteq R$ is a prime ideal such that P has finite index as a subgroup of $(R, +)$, then P is a maximal ideal.

Proof. By assumption the cardinality of R/P, which is the index $[(R, +) : (P, +)]$, is finite. Since P is prime, R/P is a domain. By part (a), R/P is a field. Thus P is maximal. □

[1] Hint: Consider the quotient ring R/P.

(6) Consider the polynomial $f(x) = x^2 + x + [1]_5$ in $\mathbb{Z}/5[x]$. Show that $R = \dfrac{\mathbb{Z}/5[x]}{(f)}$ is a field, and determine the number of elements of R.

Proof. We claim that f is an irreducible element of $\mathbb{Z}/5[x]$. Since $\mathbb{Z}/5[x]$ is a field, any nontrivial factorization of f must be as a product of polynomials of degree one, and any polynomial of degree one over a field has a root, so it suffices to show that f has no root in $\mathbb{Z}/5$. To check this, we can just evaluate at every element of $\mathbb{Z}/5[x]$: we have

$$f([0]) = [1],\ f([1]) = [3],\ f([2]) = [2],\ f([3]) = [3],\ f([4]) = [1].$$

Now, since $\mathbb{Z}/5[x]$ is a PID, every irreducible element generates a maximal ideal. Thus (f) is maximal so $R = \mathbb{Z}/5[x]/(f)$ is a field.

To compute the number of element of R we recall that, as a consequence of the division algorithm, every element $g + (f) \in R$ has a unique representative r such that $\deg(r) < 2$ or $r = 0$. There are $5^2 = 25$ such polynomials, so $|R| = 25$. □