Algebra 1 Final

Jaden Wang

Please do NOT grade Problem 4.

Problem (1)**.** Let $|G : H| = n$.

Case (1). If n is a prime, then it must be the smallest prime dividing $|G|$ by assumption. Then $|H|$ has index the smallest prime and therefore $H \trianglelefteq G$ by Corollary 4.5.

Case (2). Supoose n is not a prime. Then the prime factors of $|H|$ must be strictly larger than n. Consider the action representation $\phi : G \to S_n$ of G acting on cosets G/H by left multiplication. Per Homework 2 Problem 2 we know that $K := \ker \phi$ is the largest normal subgroup contained in H. Therefore, $|G : H| = n$ divides $|G : K|$ divides $|G| = |H|n$. That is, $|G : K| = dn$ where $d||H|$. But since we know that every prime dividing $|H|$ is strictly larger than n, each prime factor of d is also greater than n as well. Moreover, $|\operatorname{im} \phi|$ divides $|S_n| = n!$, so by the definition of factorial, prime factors of $|\operatorname{im} \phi|$ must all be no greater than n. By the first isomorphism theorem, we know that $|G : K| = |\operatorname{im} \phi|$. However, if $d > 1$, then $|G : K|$ would contain prime factors strictly larger than any prime factor in $|\operatorname{im} \phi|$ so they wouldn't equal, a contradiction. It follows that $d = 1$ and therefore $|G : K| = |G : H|$. This implies that $H = K$ and therefore $H \trianglelefteq G$ as K does.

Problem (2)**.** By the class equation,

$$pq - p - q = |X| = |Z| + \sum_{a \in A} [G : G_a]$$

where Z is the set of elements with trivial orbits (*i.e.* fixed points) and A is the set consisting of one representative from each nontrivial orbit. Since $|G| = pq$, $[G : G_a]$ must divide $|G|$ so $[G : G_a] = 1, p, q$ or pq. If $[G : G_a] = 1$, then G fixes a and we are done. If $[G : G_a] = pq$, this violates that the sum is at most $pq - p - q < pq$. We are left of the cases where $[G : G_a] = p$ or q. Then the sum can be written as

$$\sum_{a \in A} [G : G_a] = mp + nq$$

for some $m, n \in \mathbb{N}$ (note when $A = \emptyset$, $m = n = 0$). It follows that

$$pq - p - q = |Z| + mp + nq$$
$$|Z| = pq - (m+1)p - (n+1)q$$

Suppose to the contrary that $|Z| = 0$, then $pq = (m+1)p + (n+1)q$. This implies that $p|(m+1)p + (n+1)q$ and $q|(m+1)p + (n+1)q$ which by the definition of primes implies $p|n+1$ and $q|m+1$. But since $m+1, n+1 > 0$, we must have $m+1 \geq q$ and $n+1 \geq p$, then $(m+1)p + (n+1)q \geq qp + pq = 2pq > pq$, a contradiction. This forces $|Z| > 0$. That is, there is at least one fixed point.

Problem (3)**.** Given $P \in Syl_p(G)$ and $Q \in Syl_p(H)$, since $|Q| = p^k$ for some k and $Q \leq H \leq G$, Q is a p-subgroup of G. Thus by Sylow Theorem, there exists a $g \in G$ s.t. $Q \leq gPg^{-1}$. This establishes that $Q \leq gPg^{-1} \cap H$.

Let $|gPg^{-1}| = p^n$ for some $n \geq k$, and $|H| = p^k m$ where p doesn't divide m. We see that $gPg^{-1} \cap H$ must have order dividing both p^n and $p^k m$ and therefore must divide $p^k = |Q|$, *i.e.* $|gPg^{-1} \cap H| \leq |Q|$. It follows that $Q = gPg^{-1} \cap H$.

Problem (4)**.** (DO NOT GRADE). For any $a \in \mathbb{Z}$, denote $a_m := a \bmod m$ and $a_n := a \bmod n$. Since $\mathbb{Z}_n = \langle 1_n \rangle$ and $\mathbb{Z}_m = \langle 1_m \rangle$ as abelian groups, we can define an abelian group (or $\mathbb{Z}$-module) homomorphism ϕ by mapping generator to generator: $\phi : \mathbb{Z}_n \to \mathbb{Z}_m, 1_n \mapsto 1_m$. Note $\phi(a_n) = a_m$. This is well-defined since $m|n$ and $1_m \cdot n = 1_m \cdot m \cdot k = 0 \cdot k = 0$ satisfies the relation on the generator 1_n. Surjectivity is clear from that the generator 1_m is hit. It remains to check that ϕ respects multiplication: given $a_n, b_n \in \mathbb{Z}_n$, we have

$$\begin{aligned}
\phi(a_n b_n) &= \phi((ab)_n) \\
&= (ab)_m \\
&= a_m b_m \\
&= \phi(a_n)\phi(b_n)
\end{aligned}$$

Hence ϕ is a ring homomorphism.

Given $a_n \in \mathbb{Z}_n^\times$, we know that $\gcd(a, n) = 1$. Since $m|n$, we have $\gcd(a, m) = 1$ so $a_m = \phi(a_n) \in \mathbb{Z}_m^\times$. Thus the restriction $\overline{\phi} : \mathbb{Z}_n^\times \to \mathbb{Z}_m^\times$ of ϕ is well-defined and clearly remains a homomorphism. Let $n = km$ for some $k \in \mathbb{Z}_+$. Consider $\ker \overline{\phi} = \{a_n \in \mathbb{Z}_n^\times : \overline{\phi}(a_n) = a_m = 1_m\} = \{a_n \in \mathbb{Z}_n^\times : a = 1 + \ell m, \ell \in \mathbb{Z}\} = \{a_n : a = 1 + \ell m, 0 \le \ell \le k-1, \gcd(1+\ell m, km) = 1\}$. Since it is clear that $\gcd(1 + \ell m, km) = 1 =$, we finally simplify to

$$\ker \overline{\phi} = \{a_n : a = 1 + \ell m, 0 \le \ell \le k - 1, \gcd(a, k) = 1\}.$$

Problem (5)**.** It doesn't seem like commutativity is required?

First I show an elementary proof. Suppose we have a multiplication $\times$ structure with identity on $\mathbb{Q}/\mathbb{Z}$. Let the identity be $[p/q] \neq [0]$, *i.e.* $q \neq 0$ and $p/q \notin \mathbb{Z}$, as $\mathbb{Q}/\mathbb{Z}$ is not the trivial ring. Then by the axiom of identity, $[p/q] \times [1/2] = [1/2] \neq [0]$. However,

$$\begin{aligned}
[p/q] \times [1/2] &= [p/2q + p/2q] \times [1/2] \\
&= ([p/2q] + [p/2q]) \times [1/2] \\
&= [p/2q] \times [1/2] + [p/2q] \times [1/2] && \text{distributivity} \\
&= [p/2q] \times ([1/2] + [1/2]) && \text{distributivity} \\
&= [p/2q] \times [1] \\
&= [p/2q] \times [0] \\
&= [0],
\end{aligned}$$

a contradiction. Hence no such ring structure exists.

Here I also show a similar proof using the language of tensor products as a bonus.

It suffices to show that no compatible multiplication can be defined on $\mathbb{Q}/\mathbb{Z}$. Suppose that we have an associative and distributive binary operation (demanded by a ring multiplication) $m : \mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ defined on the $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$, with a multiplicative identity $\mathbb{1}$. Then by distributivity laws, m is a $\mathbb{Z}$-bilinear map. By the universal property of tensor products of modules over a commutative ring ($\mathbb{Z}$) (Theorem 10.10 and Corollary 10.12), we have the commutative diagram:

$$\begin{tikzcd}
\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z} \arrow[r, "\iota"] \arrow[dr, "m"'] & \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} \arrow[d, "\phi"] \\
& \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

However, since $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$ (Example 4 under Corollary 10.12), this forces $\iota = 0$ so m is the zero $\mathbb{Z}$-module homomorphism as well. But this violates the axiom for the identity $m(\mathbb{1}, [1/2]) = [1/2] \neq [0]$ (since $1/2 \notin \mathbb{Z}$), a contradiction. Hence no such ring structure exists for the abelian group $\mathbb{Q}/\mathbb{Z}$ so there is no such isomorphic ring either.

Problem (8)**.** Since G is finitely generated, we can apply the structure theorem for $\mathbb{Z}$-modules. In particular, we wish to diagonalize the presentation represented by the relation matrix via the Smith Normal Form.

$$\begin{aligned} \begin{pmatrix} 1 & -1 & 3 \\ 2 & 1 & 0 \end{pmatrix} &\xrightarrow{R_2 - 2R_1} \begin{pmatrix} 1 & -1 & 3 \\ 0 & 3 & -6 \end{pmatrix} \\ &\xrightarrow{C_2 + C_1, C_3 - 3C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & -6 \end{pmatrix} \\ &\xrightarrow{C_3 + 2C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} \end{aligned}$$

Thus we obtain a new set of generators x', y', z' with the relations $x' = 0, 3y' = 0, 0z' = 0$. Therefore, $\operatorname{Ann}_{\mathbb{Z}}(\langle x' \rangle) = \mathbb{Z}$, $\operatorname{Ann}_{\mathbb{Z}}(\langle y' \rangle) = \langle 3 \rangle$, and $\operatorname{Ann}_{\mathbb{Z}}(\langle z' \rangle) = 0$ since z' has no relation. This implies that

$$\begin{aligned} G &\cong \mathbb{Z}/\operatorname{Ann}_{\mathbb{Z}}(\langle x' \rangle) \oplus \mathbb{Z}/\operatorname{Ann}_{\mathbb{Z}}(\langle y' \rangle) \oplus \mathbb{Z}/\operatorname{Ann}_{\mathbb{Z}}(\langle z' \rangle) \\ &= \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/\langle 3 \rangle \oplus \mathbb{Z}/0 \\ &\cong \mathbb{Z} \oplus \mathbb{Z}_3 \end{aligned}$$

Problem (9)**.** The number of possible JCF (up to permutation of Jordan blocks) over $\mathbb{C}$ is the same as the number of possible RCF over $\mathbb{C}$. First we see that the minimal polynomial $m(x)$ must be divisible by $x(x^2-1)(x^2+1) = x(x+1)(x-1)(x+i)(x-i)$. Then Cayley-Hamilton yields the following possible invariant factors over $\mathbb{C}$:

(1) $x(x^2+1) | x(x^2-1)(x^2+1) = m(x)$.

(2) $x^2+1 | x^2(x^2-1)(x^2+1) = m(x)$.

(3) $x | x(x^2-1)(x^2+1)^2 = m(x)$.

(4) $x^2(x^2-1)(x^2+1)^2 = m(x)$.

Therefore the number is 4.

Problem (11)**.** By Eisenstein $p = 5$, we see that $5|20$ but 25 does not divide 20 so $x^{15} + 20$ is irreducible.

$$\begin{aligned} x^{15} + 20 &= 0 \\ x^{15} &= -20 \\ x &= -\sqrt[15]{20}e^{(2k\pi i)/15} \end{aligned}$$

Let $\gamma := \sqrt[15]{20}$ and $\zeta = e^{2\pi i/15}$. Clearly ζ, γ generate all the roots.

Since $-\gamma$ is a root of $x^{15} + 20$ which is irreducible, $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 15$. Since ζ is a primitive 15th roots of unit, by Corollary 13.42, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8$. Since $\gcd(15, 8) = 1$, by Lagrange $[\mathbb{Q}(\gamma, \zeta) : \mathbb{Q}] = 15 \cdot 8 = 120$. Since any field that $x^{15} + 20$ splits must contain γ, ζ, and $\mathbb{Q}(\gamma, \zeta)$ is the smallest field containing γ, ζ by definition, we conclude that it is the splitting field of $x^{15} + 20$ with degree 120.