Kayla Orlinsky

Algebra Exam Spring 2010

Problem 1. Let $f(x) = x^6 + 3 \in \mathbb{Q}[x]$. Show that the Galois group of f is S_3.

Solution. First, we note that $f(x)$ is separable since its roots are all distinct.

We now proceed with some computation to determine the number and order of the roots that we need to adjoint to $\mathbb{Q}$ to obtain the splitting field for f.

Now, if $f(x) = 0$ then $x^6 = -3$. Letting $z = Re^{i\theta} \in \mathbb{C}$ we get that

$$(Re^{i\theta})^6 = R^6 e^{i6\theta} = -3 = 3(-1 + 0i)$$

so $R = \sqrt[6]{3}$ and $6\theta = (2k+1)\pi$.

This computation shows that we get

$$\pm\sqrt[6]{3}i \qquad \sqrt[6]{3}\left(\pm\frac{\sqrt{3}}{2} \pm \frac{1}{2}i\right)$$

as roots.

Since

$$(\sqrt[6]{3}i)^4 = 3^{\frac{4}{6}} = 3^{\frac{1}{2}}3^{\frac{1}{6}} = \sqrt[6]{3}\sqrt{3}$$

so we finally get that all the roots of $f(x)$ can be obtained by adjoining $\sqrt[6]{3}i$ to $\mathbb{Q}$.

Namely, if $\alpha = \sqrt[6]{3}i$, then the roots of f are

$$\pm\alpha, \qquad \pm\alpha^4 \pm \alpha$$

Namely, $\mathbb{Q}(\alpha)$ is the splitting field for f.

Since we already noted that f is separable, we get that $|\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$ since the minimal polynomial of α is $x^6 + 3$.

Now, we need only prove that $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ is non-abelian.

However, this is straightforward since we already wrote down the roots of f.

If

$$\begin{aligned} \tau : \mathbb{Q}(\alpha) &\to \mathbb{Q}(\alpha) \\ \alpha &\mapsto -\alpha \end{aligned}$$

and

$$\begin{aligned}\sigma : \mathbb{Q}(\alpha) &\to \mathbb{Q}(\alpha)\\ \alpha &\mapsto \alpha^4 + \alpha\end{aligned}$$

Note that both of these maps exist since f is irreducible and separable so $\mathrm{Gal}(f)$ is transitive (for any two roots of f, there exists an automorphism sending one to the other).

Finally,

$$\tau(\sigma(\alpha)) = \tau(\alpha^4 + \alpha) = \alpha^4 - \alpha$$

and

$$\sigma(\tau(\alpha)) = \sigma(-\alpha) = -\alpha^4 - \alpha$$

so the two maps do not commute.

Therefore, $\mathrm{Gal}(f)$ is non-abelian and since the only non-abelian group of order 6 is S_3 we are done.

✌

Problem 2.

(a) Let G be a group of order pqr, where $p < q < r$ are primes. Show that G contains a normal subgroup of index p.

(b) Determine up to isomorphism all groups of order $3 \cdot 7 \cdot 13$.

Solution.

(a) By Lagrange's theorem, for all $p||G|$, there exists a subgroup N of order p. Now, we will show that if p is the smallest prime dividing $|G|$ and $[G : N] = p$ then N is normal.

> **Claim 1.** If p is the smallest prime dividing $|G|$ and $[G : N] = p$, then N is normal.
>
> *Proof.* Assume not. Then there exists $g \in G$ with $g \notin N$ such that $N \neq gNg^{-1}$. Let $N^g = gNg^{-1}$.
>
> Now, as sets, we have that
> $$|NN^g| = \frac{|N||N^g|}{|N \cap N^g|}.$$
>
> If $G = NN^g$ then $g^{-1} = n_1 g n_2 g^{-1}$ and so $n_1^{-1} n_2^{-1} = g \in N$, an contradiction. Namely, $|G| > |NN^g|$.
>
> However, we finally have that
> $$|NN^g| = \frac{|N||N^g|}{|N \cap N^g|} < |G| = p|N|$$
> and so namely,
> $$\frac{|N^g|}{|N \cap N^g|} < p$$
> Since p is the smallest prime dividing $|G|$, there cannot be any elements of order smaller than p and so namely, $|N^g| = |N \cap N^g|$ and since $N \cap N^g \subset N^g$, we get that $N \cap N^g = N^g$.
>
> Namely, $N = N^g$. This is a contradiction again and so no such g exists. ✌

Therefore, from the claim, N is normal and it exists by Lagrange.

(b) $\boxed{\text{Abelian: } \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{13}}$ by the fundamental classification theorem of Abelian Groups.

Now, using the Sylow Theorems, which state that $n_p \equiv 1 \mod p$ and that $n_p|m$ with $|G| = p^k m$.

Thus, $n_7 \equiv 1 \mod 7$ and $n_7 | 3 \cdot 13$. Since $7 \nmid 12$, and $7 \nmid 38$, $n_7 = 1$.

Finally, $n_{13} = 1$ trivially by the same reasoning.

Thus, G contains exactly one normal Sylow subgroup of orders $7, 13$. Note that any Sylow 3-subgroups are isomorphic to $\mathbb{Z}_3, \mathbb{Z}_7, \mathbb{Z}_{13}$ respectively.

Now, we begin the classificiation. Starting with a normal Sylow-subgroup, we will take automorphisms of that Sylow subgroup and see how those act on the product of the remain two Sylow subgroups.

Then we note that from (a), $P_7 P_{13}$ is a normal subgroup of G.

First, if G has a normal Sylow 3-subgroup, then $\mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_3^* \cong \mathbb{Z}_2$. Since there are no order two elements of $\mathbb{Z}_7 \times \mathbb{Z}_{13}$ and so this yields nothing. Namely, there are no non-trivial homomorphisms $\varphi : \mathbb{Z}_7 \times \mathbb{Z}_{13} \to \mathbb{Z}_2$

Second, $\mathrm{Aut}(\mathbb{Z}_7) \cong \mathbb{Z}_6$ has two elements of order 3,

$$\begin{aligned} \alpha_1 : \mathbb{Z}_7 &\to \mathbb{Z}_7 \\ b &\mapsto b^2 \end{aligned} \qquad\qquad \begin{aligned} \alpha_2 : \mathbb{Z}_7 &\to \mathbb{Z}_7 \\ b &\mapsto b^4 \end{aligned}$$

Note that $\alpha_2 = \alpha_1^2$

Thus, we can let

$$\begin{aligned} \psi_1 : \mathbb{Z}_3 \times \mathbb{Z}_{13} &\to \mathbb{Z}_6 \\ (1,0) &\mapsto 2 = \alpha_1 \\ (0,1) &\mapsto 0 = \mathrm{Id} \end{aligned}$$

be a non-trivial homomorphism.

Let

$$\mathbb{Z}_3 \times \mathbb{Z}_{13} = \langle a \rangle \times \langle c \rangle \qquad \mathbb{Z}_7 = \langle b \rangle$$

Then $\psi_1(a,0)(b) = \alpha_1(b) = b^2$ and $\psi_1(0,c)(b) = \mathrm{Id}(b) = b$. Finally, for ψ_1, this gives the relation

$$aba^{-1} = \psi_1(a)(b) = b^2 \implies ab = b^2 a$$

and

$$cbc^{-1} = b \implies cb = bc.$$

Thus, we obtain the presentation

$$\mathbb{Z}_7 \rtimes_{\psi_1} (\mathbb{Z}_3 \times \mathbb{Z}_{13}) \cong \langle a, b, c \,|\, a^3 = b^7 = c^{13} = 1, ac = ca, ab = b^2 a, cb = bc \rangle \cong (\mathbb{Z}_7 \rtimes_{\psi_1} \mathbb{Z}_3) \times \mathbb{Z}_{13}$$

and similarly for ψ_2,

$$\begin{aligned} \psi_2 : \mathbb{Z}_3 \times \mathbb{Z}_{13} &\to \mathbb{Z}_6 \\ (1,0) &\mapsto 4 = \alpha_2 \\ (0,1) &\mapsto 0 = \mathrm{Id} \end{aligned}$$

Now, we note that

$$\begin{aligned}\varphi : \mathbb{Z}_3 \times \mathbb{Z}_{13} &\to \mathbb{Z}_3 \times \mathbb{Z}_{13}\\ (1,0) &\mapsto (2,0)\\ (0,1) &\mapsto (0,1)\end{aligned}$$

is an automorphism of $\mathbb{Z}_3 \times \mathbb{Z}_{13}$ and since $\psi_2 = \psi_1 \circ \varphi$, we have that ψ_1 and ψ_2 generate isomorphic semi-direct products.

Third, $\mathrm{Aut}(\mathbb{Z}_{13}) \cong \mathbb{Z}_{12}$ which has 2 elements of order 3 and no elements of order 7 call them β_1, β_2 with $\beta_1(c) = c^3$ and $\beta_2(c) = c^9$.

Let $\psi_3 : \mathbb{Z}_3 \times \mathbb{Z}_7 \to \mathbb{Z}_{12}$ be the map where $\psi_3(a)(c) = \beta_1(c) = c^3$ and $\psi_3(b)(c) = c$

Similarly, $\psi_4(a)(c) = c^9$ and $\psi_4(b)(c) = c$. As from the previous case, letting $\varphi(1,0) = (2,0)$ and $\varphi(0,1) = (0,1)$, we get hat $\psi_4 = \psi_3 \circ \varphi$ and so again, the semi-direct products will be isomorphic.

This gives one presentation:

$$\mathbb{Z}_{13} \rtimes_{\psi_3} (\mathbb{Z}_3 \times \mathbb{Z}_7) \cong \langle a, b, c \,|\, a^3 = b^7 = c^{13} = 1, ab = ba, ac = c^3 a, bc = cb \rangle \cong (\mathbb{Z}_{13} \rtimes_{\psi_3} \mathbb{Z}_3) \times \mathbb{Z}_7$$

.

Fourth $P_7 P_{13} \cong \mathbb{Z}_7 \times \mathbb{Z}_{13}$ is also a normal subgroup. $\mathrm{Aut}(\mathbb{Z}_7 \times \mathbb{Z}_{13}) \cong \mathbb{Z}_6 \times \mathbb{Z}_{12}$.

Thus, we have

$$\begin{aligned}\psi_5 : \mathbb{Z}_3 &\to \mathbb{Z}_6 \times \mathbb{Z}_{12}\\ 1 &\mapsto (2,0) = (\alpha_1, \mathrm{Id})\\ \psi_6 : \mathbb{Z}_3 &\to \mathbb{Z}_6 \times \mathbb{Z}_{12}\\ 1 &\mapsto (4,0) = (\alpha_2, \mathrm{Id})\\ \psi_7 : \mathbb{Z}_3 &\to \mathbb{Z}_6 \times \mathbb{Z}_{12}\\ 1 &\mapsto (0,4) = (\mathrm{Id}, \beta_1)\\ \psi_8 : \mathbb{Z}_3 &\to \mathbb{Z}_6 \times \mathbb{Z}_{12}\\ 1 &\mapsto (0,8) = (\mathrm{Id}, \beta_2)\\ \psi_9 : \mathbb{Z}_3 &\to \mathbb{Z}_6 \times \mathbb{Z}_{12}\\ 1 &\mapsto (2,4) = (\alpha_1, \beta_1)\\ \psi_{10} : \mathbb{Z}_3 &\to \mathbb{Z}_6 \times \mathbb{Z}_{12}\\ 1 &\mapsto (2,8) = (\alpha_1, \beta_2)\\ \psi_{11} : \mathbb{Z}_3 &\to \mathbb{Z}_6 \times \mathbb{Z}_{12}\\ 1 &\mapsto (4,4) = (\alpha_2, \beta_1)\\ \psi_{12} : \mathbb{Z}_3 &\to \mathbb{Z}_6 \times \mathbb{Z}_{12}\\ 1 &\mapsto (4,8) = (\alpha_2, \beta_2)\end{aligned}$$

Where $\alpha_1 : \mathbb{Z}_6 \to \mathbb{Z}_6$ is defined by $\alpha_1(1) = 2$, $\alpha_2(1) = 4$, $\beta_1 : \mathbb{Z}_{13} \to \mathbb{Z}_{13}$ is defined by $\beta_1(1) = 3$, and $\beta_2(1) = 9$.

Since $\alpha_1^2 = \alpha_2$, and $\beta_1^2 = \beta_2$, it is clear to see that each of these homomorphisms pairs up with another one via $\varphi : \mathbb{Z}_3 \to \mathbb{Z}_3$ defined by $\varphi(1) = 2$. For example, $\psi_6 = \psi_5 \circ \varphi$.

Now, let $\mathbb{Z}_3 = \langle a\rangle$, $\mathbb{Z}_7 = \langle b\rangle$ and $\mathbb{Z}_{13} = \langle c\rangle$ as before. We note that the ψ_5 and ψ_6 which generate isomorphic semi-direct products will generate the same group as ψ_2 from the second part. This is because, a will commute with c and $aba^{-1} = \psi_5(a)(b) = \alpha_1(b) = b^2$.

Similarly, ψ_7 and ψ_8 generate the same group as ψ_3 from the third part.

Finally, this will yield two sets of non-ismorphic groups. First, one defined by ψ_9, with relations $aba^{-1} = \psi_9(a)(b) = \alpha_1(b) = b^2$ and $aca^{-1} = \psi_9(a)(c) = c^3$, which gives

$$(\mathbb{Z}_7 \times \mathbb{Z}_{13}) \rtimes_{\psi_9} \mathbb{Z}_3 \cong \langle a, b, c \,|\, a^3 = b^7 = c^{13} = 1, bc = cb, ab = b^2a, ac = c^3a\rangle.$$

And the other non-isomophic group has relations defined by $aba^{-1} = \psi_{10}(a)(b) = b^2$ and $aca^{-1} = \psi_{10}(a)(c) = c^9$, which gives

$$(\mathbb{Z}_7 \times \mathbb{Z}_{13}) \rtimes_{\psi_{10}} \mathbb{Z}_3 \cong \langle a, b, c \,|\, a^3 = b^7 = c^{13} = 1, bc = cb, ab = b^2a, ac = c^9a\rangle.$$

Note: that to verify that ψ_9 and ψ_{10} do indeed generate non-isomorphic groups we turn to a stronger theorem of Taunt in *Remarks on the Isomorphism Problem in Theories of Construction of Finite Groups.*

The theorem states that:

If $|N|$ and $|H|$ are comprime, then

$$N \rtimes_{\psi_1} H \cong N \rtimes_{\psi_2} H$$

if and only if there exists $\alpha \in \mathrm{Aut}(N)$ and $\beta \in \mathrm{Aut}(H)$ such that

$$(\psi_1 \circ \beta)(h) = \alpha \circ \psi_2(h) \circ \alpha^{-1} \in \mathrm{Aut}(N)$$

for all $h \in H$.

In this case, because $\mathrm{Aut}(N) \cong \mathbb{Z}_6 \times \mathbb{Z}_{12}$ which is abelian. Namely, $\alpha \circ \psi_2(h) \circ \alpha^{-1} = \psi_2(h)$.

Therefore, we have that two homomorphisms generate isomorphic semi-direct products, if and only if they differ by an isomorphism of $\mathbb{Z}_3$. Since there are only two isomoprhisms of $\mathbb{Z}_3$, it is easy to verify that ψ_9 and ψ_{10} do not generate isomorphic semi-direct products.

Fifth We can also define a normal subgroup P_3P_{13} since both P_3 and P_{13} normal in G and intersect trivially, $P_3P_{13} \cong \mathbb{Z}_3 \times \mathbb{Z}_{13}$ is normal in G.

However, $\mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_{13}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{12}$ has no elements of order 7.

Similarly, $\mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_7) \cong \mathbb{Z}_2 \times \mathbb{Z}_6$ has no elements of order 13.

As we have now ruled out all possible normal subgroups of G, we can conclude that we have found all of the isomorphism classes. Listed out, the four non-abelian groups and one abelian group are

Groups of order $3 \cdot 7 \cdot 13$:

$$\mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{13}$$

$$\mathbb{Z}_7 \rtimes_{\psi_1} \mathbb{Z}_3 \times \mathbb{Z}_{13} \cong \langle a, b, c \,|\, a^3 = b^7 = c^{13} = 1, ac = ca, ab = b^2 a, cb = bc \rangle$$

$$\mathbb{Z}_{13} \rtimes_{\psi_3} \mathbb{Z}_3 \times \mathbb{Z}_7 \cong \langle a, b, c \,|\, a^3 = b^7 = c^{13} = 1, ab = ba, ac = c^3 a, bc = cb \rangle$$

$$(\mathbb{Z}_7 \times \mathbb{Z}_{13}) \rtimes_{\psi_9} \mathbb{Z}_3 \cong \langle a, b, c \,|\, a^3 = b^7 = c^{13} = 1, bc = cb, ab = b^2 a, ac = c^3 a \rangle$$

$$(\mathbb{Z}_7 \times \mathbb{Z}_{13}) \rtimes_{\psi_{10}} \mathbb{Z}_3 \cong \langle a, b, c \,|\, a^3 = b^7 = c^{13} = 1, bc = cb, ab = b^2 a, ac = c^9 a \rangle$$

✌

Problem 3. Let R be a commutative Noetherian ring, and let I, J and K be ideals of R. We say I is irreducible if $I = J \cap K \implies I = J$ or $I = K$.

(a) Show that every ideal of R is a finite intersection of irreducible ideals.

(b) Show that every irreducible ideal is primary. (An ideal I of R is primary if $R/I \neq 0$, and every zero-divisor in R/I is nilpotent.)

Solution.

(a) Assume not. Let I be an ideal of R which is not a finite intersection of irreducibles.

Then, there exists ideals J_1 and J_2 such that $I = J_1 \cap K_1$ with $I \subsetneq J_1$ and $I \subsetneq K_1$. Note that if J_1 and K_1 do not exist, then $I = J_1 \cap K$ implies $I = J_1$ or $I = K_1$ and so I is itself irreducible, a contradiction.

Now, because I is not a finite intersection of irreducibles, it must be that either J_1 or K_1 is also not a finite intersection of irreducibles. (If both were such an intersection, then I would be as well).

WLOG, take J_1 to be not a finite intersection of irreducibles. However, by the same argument as before, we can write $J_1 = J_2 \cap K_2$ with $J_1 \subsetneq J_2$ and $J_1 \subsetneq K_2$.

Namely, we obtain an ascending chain

$$I \subsetneq J_1 \subsetneq J_2 \subsetneq \cdots$$

which must terminate because R is Noetherian.

However, if the chain terminates at J_n, so $J_m = J_n$, then this implies that there do not exist any ideals J and K such that $J_n \subsetneq J \cap K$ and $J_n \subsetneq J$ and $J_n \subsetneq K$. Else, we could call $J_{n+1} = J$.

Thus, J_n is irreducible, which is a contradiction.

(b) Let I be an irrediucible proper ideal of R. Then $R/I \neq 0$.

Let $0 \neq a \in R/I$ be a zero divisor. Then there exists $0 \neq b \in R/I$ such that $ab = 0 \in R/I$ so namely, $ab \in I$ with $a \notin I$ and $b \notin I$.

Now, we note that this implies that $b \in \text{Ann}(a) \subset \text{Ann}(a^2) \subset \text{Ann}(a^3) \subset \cdots$ since if $ab = 0$ then $a^k b = a^{k-1} 0 = 0$.

Now, because R is Noetherian and quotients of Noetherian rings are also Noetherian, we have that R/I is Noetherian. Namely, the chain

$$\text{Ann}(a) \subset \text{Ann}(a^2) \subset \text{Ann}(a^3) \subset \cdots$$

must terminate.

Say the chain terminates at $\text{Ann}(a^n)$ so $\text{Ann}(a^m) = \text{Ann}(a^n)$ for all $m \geq n$.

Now, let $b \in \text{Ann}(a)$ and $x \in (b) \cap (a^n)$. Then $x = rb = sa^n$. However, then $0 = rba = sa^{n+1}$ and so $s \in \text{Ann}(a^{n+1}) = \text{Ann}(a^n)$ and so $x = sa^n = 0$.

Thus, $(b) \cap (a^n) = (0) = I$. However, I is irreducible so either $I = (b)$ or $I = (a^n)$. Since $b \notin I$ by assumption, it must be that $I = (a^n)$ and so namely, $a^n = 0 \in R/I$.

Thus, every zero-divisior is nilpotent.

✌

Problem 4. Let A be a finite-dimensional algebra over a field K, such that for every $a \in A$, $a^7 = a$. Show that A is a direct product (sum?) of fields. Which fields can arise?

Solution. First, we note that $K \subset A$ and so the fact that $a^7 = a$ for all $a \in A$ forces $k^7 = k$ for all $k \in K$.

Namely, $K \cong \mathbb{F}_7$.

Now, because A is a finite dimensional vector space, it is Artinian (because all ideals are finite-dimensional subspaces of A so infinite chains cannot exist).

Now, let $a \in J(A)$ the Jacobson radical of A. Then $a^6 \in J(A)$ because $J(A)$ is an ideal of A.

However, $J(A)$ is quasi-invertible so there exists $b \in A$ such that

$$b(1 - a^6) = 1.$$

However, this implies that

$$b(1 - a^6)a = a \implies b(a - a^7) = a \implies a = 0$$

so $J(A) = (0)$.

Therefore, by Artin-Wedderburn, A can be written as a finite direct sum of matrix algebras over division rings. Namely,

$$A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_l}(D_l) \qquad D_l \text{ division rings over } K.$$

Now, because D_i is a division ring over K, it must be a field extension of K. However, since A has the property that $a^7 = a$ for all $a \in A$, each $d \in D_i$ satisfies this property as well so $D_i = K$ for all i.

Now, because there exist non-zero nilpotent elements in any matrix ring, it must be that $n_i = 1$ for all i.

Namely,

$$A \cong \bigoplus_{i=1}^{l} K.$$

✌

Problem 5. Let G and H be finitely generated abelian groups such that $G \otimes_{\mathbb{Z}} H = 0$. Show that G and H are finite and have relatively prime orders.

Solution. By the fundamental theorem of finitely generated abelian groups, we can write

$$G \cong \mathbb{Z}^s \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$$
$$H \cong \mathbb{Z}^t \oplus \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_l}$$

Now, because tensor product distributes across direct sums, we have that

$$\begin{aligned} G \otimes_{\mathbb{Z}} H &= (\mathbb{Z}^s \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}) \otimes_{\mathbb{Z}} (\mathbb{Z}^t \oplus \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_l}) \\ &= (\mathbb{Z}^s \otimes_{\mathbb{Z}} \mathbb{Z}^t) \bigoplus_{i=1}^{k} (\mathbb{Z}_{n_i} \times_{\mathbb{Z}} \mathbb{Z}^t) \bigoplus_{j=1}^{l} (\mathbb{Z}^s \otimes_{\mathbb{Z}} \mathbb{Z}_{n_j}) \bigoplus_{i,j} (\mathbb{Z}_{n_i} \otimes_{\mathbb{Z}} \mathbb{Z}_{m_j}) \\ &= 0 \end{aligned}$$

Since this is only possible if each individual tensor product is zero, we immediately see that $s = t = 0$. Therefore, we need only show that $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m = 0$ implies that n and m are coprime. In fact, we will show something far stronger:

Claim 2. $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m \cong \mathbb{Z}_d$ with $d = \gcd(m, n)$.

Proof. To do this, we let $f : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_d$ defined by $f(a, b) = (a \mod d, b \mod d)$ which is well defined because $d = \gcd(m, n)$.

Now, by the universal property of tensor products, because $\mathbb{Z}_d$ is abelian, there exists a map $\varphi : \mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m \to \mathbb{Z}_d$ such that $f = \varphi \circ i$ where $i : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m$ defined by $i(a, b) = a \otimes b$.

Now, if $f(a, b) = (0, 0)$ then $d|a$ and $d|b$. Therefore,

$$\frac{n}{d}(a \otimes b) = n\frac{a}{d} \otimes b = 0 \qquad a/d \text{ has order dividing } n$$

and similarly,

$$(a \otimes b)\frac{m}{d} = a \otimes \frac{b}{d}m = 0$$

Therefore, the order of $a \otimes b$ divides n/d and m/d. However, $d = \gcd(m, n)$ so n/d and m/d are coprime so $a \otimes b$ has order 1 and is trivial.

Thus, $\ker(f) \subset= \ker(\varphi \circ i) \subset \ker(i)$. However, clearly $\ker(i) \subset \ker(\varphi \circ i)$ so $\ker(f) = \ker(i)$ and therefore, $\ker(\varphi) = (0)$.

> Finally, f is certainly surjective since $d|n$ and $d|m$ so φ must be surjective as well.
>
> Therefore, φ is an isomorphism. ✌

Finally, from the claim, $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m = 0$ forces $\gcd(n, m) = 1$ and so n_i and m_j are coprime for all i, j. Namely, $|G|$ and $|H|$ are coprime.

✌

Problem 6. Let S and T be diagonalizable endomorphisms of a finite dimensional complex vector space. If S and T commute show that they are polynomials in each other.

Solution. First, we note that it is necessary that either S or T has distinct eigenvalues.

For example, $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ are both diagonalizable matrices, and so represent diagonalizable endomorphisms from $\mathbb{R}^2 \to \mathbb{R}^2$. Furthermore, $IA = A = AI$ so both matrices commute.

However, $A^n = A$ for all n and so if I is a polynomial in A it is of the form $I = aA + bI$ which implies that $I = \frac{a}{1-b}A$ which is a contradiction.

Now, assume WLOG, that S has distinct eigenvalues.

Then the minimal polynomial of S is the characteristic polynomial of degree n by Cayley.

Now, let M be the space of all matrices which commute with S.

It is immediate that M is a subspace of $M_n(\mathbb{C})$ since it is closed under addition and scalar multiplication. Namely, if S commutes with A and B, then

$$S(aA + bB) = SaA + SbB = aAS + bBS = (aA + bB)S.$$

Now, we note that S commutes with itself so $S^n \in M$ for all $n \in \mathbb{N}$.

Claim 3. M has dimension n and $\{I, S, S^2, ..., S^{n-1}\}$ is a basis for M.

Proof. First, because S has minimal polynomial of degree n, this set is certainly linearly independent in $M_n(\mathbb{C})$ and so it is in M as well.

Therefore, $\deg(M) \geq n$.

Now, let T commute with S. Let x be an eigenvector of S with eigenvalue λ.

Then
$$S(Tx) = TSx = T\lambda x = \lambda Tx$$
so Tx is also an eigenvector of S with eigenvalue λ.

However, the eigenvalues of S are all distinct, so the eigenvectors of S associated to λ generate a 1-dimensional subspace. Namely, there exists γ so $Tx = \gamma x$.

Therefore, the eigenvectors of S are the same as those of T.

Namely, S and T are simultaneously diagonalizable so there exists a P invertible such that $PSP^{-1} = D_1$ and $PTP^{-1} = D_2$.

Thus,

$$\begin{aligned} M &= \{A \in M_n(\mathbb{C}) \mid AS = SA\} \\ &= \{P^{-1}DP \in M_n(\mathbb{C}) \mid DD_1 = D_1D\} \\ &\cong M' \subset \{D \in M_n(\mathbb{C}) \mid D \text{ diagonal } \} \end{aligned}$$

so namely, $\dim(M) \leq n$.

Since M has dimension n and $\{I, S, S^2, ..., S^{n-1}\}$ is linearly independent in M, then it forms a basis for M. ✌

Finally, from the claim, $T \in M$ and so T is a linear combination of basis elements and so T is a polynomial in S.

Similarly for S being a polynomial in T. ✌

Problem 7. What are the prime ideals of $\mathbb{Z}[x]$? What are the maximal ideals? Carefully explain your answers.

Solution. $\boxed{\text{Prime}}$ Clearly, $(0), (p), (f(x)), (p, f(x))$ are all prime whenever $f(x)$ is irreducible in $\mathbb{Z}[x]$ which is a UFD.

This is because

$$\mathbb{Z}[x]/(p) \cong \mathbb{Z}_p[x] \qquad \text{PID because } \mathbb{Z}_p \text{ is a field}$$

so namely, $\mathbb{Z}[x]$ is a domain.

Similarly, if $f(x)$ is irreducible, then $\mathbb{Z}[x]/(f(x))$ is a domain. This is because if $g(x)$ is a zero divisor in $\mathbb{Z}[x]/(f(x))$, then there exists $h_1(x) \notin (f(x))$ and $h_2(x) \notin (f(x))$ such that $g(x)h_1(x) = f(x)h_2(x)$. However, $f(x)$ irreducible in $\mathbb{Z}[x]$ which is a UFD implies that $f(x)$ is prime. So this implies that $f(x)|g(x)$ or $f(x)|h_1(x)$. Since $f(x) \nmid h_1(x)$ by the assumption that $h_1(x) \notin (f(x))$, it must be that $g(x) \in (f(x))$ and so $g(x) = 0 \in \mathbb{Z}[x]/(f(x))$.

Finally, $(p, f(x))$ is prime for similar reasons as the first two.

Now, assume that P is a non-zero prime ideal of $\mathbb{Z}[x]$. If $f(x) \in P$ is irreducible and constant, then $f = p$ for a prime p, else $\mathbb{Z}[x]/P$ will not be a domain. Therefore, if every $f \in P$ is constant, then $P = (p)$ for some prime p.

Next, let $f(x) \in P$ be non-constant and irreducible. Note that such an f must exist, else $f(x) = g(x)h(x)$ and so because P is prime, either $g(x) \in P$ or $h(x) \in P$. In either case, because f can have only a finite number of irreducible factors, we can proceed until P contains an irreducible element.

Now, we note that if $P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ since if $ab \in P \cap \mathbb{Z}$ then either $a \in P$ or $b \in P$ and certainly a or b is in $\mathbb{Z}$.

Therefore, $P \cap \mathbb{Z} = (0)$ or $P \cap \mathbb{Z} = (p)$ for p prime.

If P does not contain p, then $P/(p) \cong P$ and $\mathbb{Z}[x]/(p) \cong \mathbb{Z}_p[x]$ which is a PID. Therefore, $P/(p) = (h(x)) \cong P$ and so because f is irreducible and $f \in P$ $P = (f(x))$.

If P does contain p, then by the exact same reasoning, $P/(p) = (f(x))$ and so $P = (f(x), p)$ since every $h \in P$ is of the form $fk_1 + pk_2$.

Therefore, the above list are the only possible prime ideals of $\mathbb{Z}[x]$.

$\boxed{\text{Maximal}}$ Now, if M is a maximal ideal of $\mathbb{Z}[x]$, then M is prime and $\mathbb{Z}[x]/M$ is a field. Since the only prime ideal in our above list which satisfies this criteria is $(f(x), p)$, we have that the maximal ideals are of the form $(f(x), p)$ for f irreducible and p prime. ✌