

ALGEBRA PROBLEMS AND SOLUTIONS
JANUARY 2003

TONI A. WATSON

PROBLEM 1

- (a) Let H be a group of order 9. Show that the order of the automorphism group of H divides 48 (*Hint*: You may assume, without proving it, that $GL_2(\mathbb{Z}_3)$ has order 48).
- (b) Let G be a group of order $153 = 3^2 \times 17$. Show that the center of G contains a group of order 9.
- (c) Find all groups of order 153.

In this problem, you may not quote results about groups of order p^2q .

Solution:

- (a) Since $|H| = 9$, $H \cong \mathbb{Z}_9$ or $H \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. Since automorphisms map generators to generators, $|Aut(H)|$ is equal to the number of generators of H .

If $H \cong \mathbb{Z}_9$, then $Aut(H) \cong (\mathbb{Z}_9)^\times$ and $|Aut(H)| = \varphi(9) = 3^{2-1}(3-1) = 3(2) = 6$.

If $H \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, then H is a vector space of dimension 2 over \mathbb{Z}_3 , so $Aut(H) \cong GL_2(\mathbb{Z}_3)$. Since the hint tells us that $GL_2(\mathbb{Z}_3)$ has order 48, $|Aut(H)| = 48$. *Note: if $|\mathbb{F}| = q < \infty$, $|GL_n(\mathbb{F})| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$. Since $6|48$ and $48|48$, $|H| = 9$ implies that $|Aut(H)| = 48$.* *

- (b) By Sylow's Theorem, there is a Sylow-3 subgroup of order 9 in G such that $n_3 \equiv 1 \pmod{3}$ and $n_3 | 153 \Rightarrow n_3 | 17$. But since $3 \nmid (17-1)$, it follows that $n_3 = 1$. Sylow's theorem then implies that $P \in Syl_3(G)$ is unique so $P \trianglelefteq G$.

Moreover, Sylow's theorem further implies that there is a Sylow-17 subgroup of order 17 in G such that $n_{17} \equiv 1 \pmod{17}$ and $n_{17} | 153 \Rightarrow n_{17} | 9$. But since $17 > 9$, it follows necessarily that $n_{17} = 1$. Again by Sylow's theorem, $Q \in Syl_{17}(G)$ is unique and $Q \trianglelefteq G$.

Since $\gcd(9, 17) = 1$, $P \cap Q = \{1\}$. Additionally, since $P, Q \trianglelefteq G$, $PQ \leq G$ with $PQ = P \times Q$ and

$$|P \times Q| = |PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{9(17)}{1} = 153 = |G|$$

By Lagrange's Theorem, it follows that $G \cong P \times Q$. Hence, G is necessarily abelian, which implies that the center of G , $Z(G)$ is all of G so $P \leq Z(G)$. ★

(c) From (b), it is known that G is abelian so it is sufficient to apply the Fundamental Theorem of Finitely Generated Abelian Groups. Noting that $|G| = 3^2 \times 17^1$, there are $2 \times 1 = 2$ distinct abelian groups and those groups are

- (1) $\mathbb{Z}_9 \times \mathbb{Z}_{17} \cong \mathbb{Z}_{153}$ and
- (2) $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{17} \cong \mathbb{Z}_3 \times \mathbb{Z}_{51}$

★

PROBLEM 2

Let M be an $m \times n$ matrix (with entries in some field). Show that there exist an invertible $m \times m$ matrix A and an invertible $n \times n$ matrix B such that $AMB = (c_{ij})$ with $c_{ii} = 0$ or 1 for all i and $c_{ij} = 0$ whenever $i \neq j$.

Solution:

Let $V = \mathbb{F}^m$ and $W = \mathbb{F}^n$ be vector spaces over \mathbb{F} . Then there is a basis $\mathcal{B}_1 = \{v_1, \dots, v_m\}$ for V and a basis $\mathcal{B}_2 = \{w_1, \dots, w_n\}$ for W . Additionally, M represents a linear transformation $T \in \text{Hom}(V, W)$. Suppose $R(T)$ is the dimension of T . Then if $R(T) = r$, the Rank Nullity Theorem implies that there is a permutation, σ of \mathcal{B}_1 such that $\{T(v_{\sigma(1)}), \dots, T(v_{\sigma(r)})\}$ forms a basis for $R(T)$ and $\{v_{\sigma(r+1)}, \dots, v_{\sigma(m)}\}$ forms a basis for $\ker(T)$. Since $\text{Im}(T) \subseteq W$, $T(v_{\sigma(i)}) = w_i$ for $i \in \{1, \dots, r\}$. So the basis for $\text{Im}(T)$, $\{T(v_{\sigma(1)}) = w_1, \dots, T(v_{\sigma(r)}) = w_r\}$ can be extended to form \mathcal{B}_2 . We then have bijective transformations $T_V \in \text{Aut}(V)$ and $T_W \in \text{Aut}(W)$ such that the composite transformation $T_V^{-1}TT_W : V \rightarrow W$ gives the matrix

$$C = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

If $T_V^{-1} = A$ and $T_W = B$, then we have $AMB = C = (c_{ij})$ where $c_{ii} = 1$ for $1 \leq i \leq r$ and $c_{ij} = 0$ elsewhere. ★

PROBLEM 3

Let R be a principal ideal domain and let A and B be finitely generated R -modules.

- (a) Show that if $0 \neq a \in A$ and $0 \neq b \in B$ are not torsion elements (that is, there are no $0 \neq r \in R$ with $ra = 0$ and similarly for b), then $a \otimes b \neq 0$ in $A \otimes_R B$.
- (b) Give an example where $a \neq 0$ is a nontorsion element, $b \neq 0$ is a torsion element and $a \otimes b = 0$.

Solution:

- (a) Since A and B are finitely generated, there exists a basis $\mathcal{B}_A = \{e_1, \dots, e_n\}$ for A and a basis $\mathcal{B}_B = \{f_1, \dots, f_m\}$ for B such that $a = \sum^n r_i e_i$ and $b = \sum^m s_k f_k$ where $r_i, s_k \in R$ for each i and k . Then

$$\begin{aligned} a \otimes b &= \sum_{i=1}^n r_i e_i \otimes \sum_{k=1}^m s_k f_k \\ &= \sum_{i=1}^n r_i e_i \otimes s_1 f_1 + \dots + \sum_{i=1}^n r_i e_i \otimes s_m f_m \\ &= \text{etc} \\ &= \sum_{i=1}^n \sum_{k=1}^m r_i s_k (e_i \otimes f_k) \end{aligned}$$

Since a and b are nontorsion, each basis element is nontorsion and since the basis elements are nonzero $r_i s_k (e_i \otimes f_k) = 0$ if and only if $r_i s_k = 0$. Since a and b are both nonzero, there must be at least one $i \in \{1, \dots, n\}$ and $k \in \{1, \dots, m\}$ such that $r_i s_k \neq 0$. So $a \otimes b \neq 0$.

- (b) Let $R = A = \mathbb{Z}$ and $B = \mathbb{Z}/2\mathbb{Z}$. Then

$$2 \otimes 1 = 2 \cdot 1 \otimes 1 = 1 \otimes 2 \cdot 1 = 1 \otimes 0 = 0$$

(Recall: $a \otimes 0 = a \otimes (0 + 0) = a \otimes 0 + a \otimes 0 \implies a \otimes 0 = 0$).



PROBLEM 4

Let R be a commutative ring with 1. Let $x, y \in R$ be nonzero. Assume that x is not a zero divisor in R and that y is not in the ideal xR . Consider the R -module homomorphisms

$$\begin{aligned} f : R &\rightarrow R \oplus R, & f(r) &= (xr, yr) \\ g : R \oplus R &\rightarrow R, & g(a, b) &= ay - bx. \end{aligned}$$

- (a) Show that $\text{Im} f = \ker g$ if and only if the congruence class of y , namely $y + xR$, is not a zero divisor in the ring R/xR .
- (b) Show that there is an R -module homomorphism $h : R \rightarrow R \oplus R$ such that gh is the identity map of R if and only if the ideal $xR + yR$ generated by x and y equals R .

Solution:

- (a) Since $gf(r) = g(xr, yr) = xry - yrx = 0$ for each $r \in R$ (recall R is commutative), $\text{Im}f \subseteq \ker g$ trivially. So the goal is to show the result for $\ker g \subseteq \text{Im}f$.

First suppose that $\ker g \subseteq \text{Im}f$. Then if $(a, b) \in \ker g$,

$$\begin{aligned} ay - bx = 0 &\implies ay = bx \\ &\implies ay \in \langle x \rangle. \end{aligned}$$

by hypothesis, $(a, b) = (xr, yr)$ for some $r \in R$ so $a = xr \implies a \in \langle x \rangle$. So y is not a zero divisor in R/xR .

Conversely, suppose y is not a zero divisor in R/xR and let $(a, b) \in \ker g$. Then

$$\begin{aligned} ay - bx = 0 &\implies ay = bx \\ &\implies ay \in \langle x \rangle \\ &\implies a \in \langle x \rangle \\ a = sx &\quad \text{for some } s \in R \end{aligned}$$

$$\begin{aligned} &\implies sxy - bx = 0 \\ &\implies (sy - b)x = 0 \\ &\implies sy = b \quad \text{since } x \text{ is nonzero} \\ &\implies (a, b) = (sx, sy) \implies \ker g \subseteq \text{Im}f \end{aligned}$$

- (b) First suppose that there exists such an h . Then since h is a homomorphism, $h(1) = (1, 1)$ so $gh(1) = 1 \implies g(1, 1) = y - x = 1$ so $1 \in \langle x \rangle + \langle y \rangle \implies \langle x \rangle + \langle y \rangle = R$.

Conversely, suppose $\langle x \rangle + \langle y \rangle = R$. Then for any $r \in R$, $r = ax + by$. Define $h : R \rightarrow R \oplus R$ by $h : r = ax + by \mapsto (b, -a)$. Then

$$gh(r) = g(b, -a) = by + ax = r$$

So there exists an h such that $gh = id$.



PROBLEM 5

- (a) Show that the polynomial $f(X) = X^4 + 1$ is irreducible in $\mathbb{Q}[X]$.
 (b) The roots of $f(X)$ are the primitive 8th roots of unity. Show that the splitting field F of $f(X)$ has Galois group (over \mathbb{Q}) isomorphic to $(\mathbb{Z}/8\mathbb{Z})^\times$ (= the multiplicative group mod 8). (You may not deduce this from general results about Galois groups of the fields generated

by roots of unity. Your solution should explain how you use the result in part (a).)

- (c) Show that there are exactly three fields with $L \subset F$ and $[L : \mathbb{Q}] = 2$.

Solution:

(a)

Solution 1:

$$\begin{aligned} f(X) = 0 &\implies 0 = X^4 + 1 \\ &= (X^2 - i)(X^2 + i) \\ &= (X - \sqrt{i})(X + \sqrt{i})(X - i\sqrt{i})(X + i\sqrt{i}) \end{aligned}$$

Since none of the α such that $f(\alpha) = 0$ are elements of \mathbb{Q} , $f(X)$ is irreducible over \mathbb{Q} .

Solution 2: There is a natural pairing between $f(X)$ and $f(X+1)$ so if $f(X+1)$ is irreducible, then $f(X)$ is irreducible.

$$\begin{aligned} f(X+1) &= (X+1)^4 + 1 \\ &= X^4 + 4X^3 + 6X^2 + 4X + 2 \end{aligned}$$

By Eisenstein's Criterion (with $p = 2$), $f(X+1)$, hence $f(X)$ is irreducible.

- (b) Let $K = \mathbb{Q}(\zeta)$ be the splitting field over \mathbb{Q} . Since $f(X)$ is irreducible, $f(X)$ is the minimal polynomial for ζ over \mathbb{Q} so $\deg_{\mathbb{Q}} f(X) = |\Gamma(K/\mathbb{Q})| = 4$. So $\Gamma(K/\mathbb{Q}) \cong \mathbb{F}_4$ or $\mathbb{F}_2 \oplus \mathbb{F}_2$.

In (a), the conjugates of $\zeta = \sqrt{i}$ were found to be $\zeta, \zeta^3 = i\sqrt{i}, \zeta^5 = -\sqrt{i}$ and $\zeta^7 = -i\sqrt{i}$.

Note that $\sigma \in \Gamma(K/\mathbb{Q})$ is an automorphism determined by the generator of K/\mathbb{Q} . In particular, if $c = \sigma(\zeta)$, then

$$c^4 = (\sigma(\zeta))^4 = \sigma(\zeta^4) = \sigma(-1) = -1.$$

So c is one of the four conjugates of ζ . That is, the four automorphisms of $\Gamma(K/\mathbb{Q})$ are

$$\begin{aligned} \sigma_1 : \zeta &\mapsto \zeta \\ \sigma_2 : \zeta &\mapsto \zeta^3 \\ \sigma_3 : \zeta &\mapsto \zeta^5 \\ \sigma_4 : \zeta &\mapsto \zeta^7 \end{aligned}$$

Since $|\sigma_2| = |\sigma_3| = |\sigma_4| = 2$, $\Gamma(K/\mathbb{Q}) \cong \mathbb{F}_2 \oplus \mathbb{F}_2$.

Recall that

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \mid (a, n) = 1\} = \{1, 3, 5, 7\} = \langle 3, 5 \rangle$$

has order 4 and is not cyclic (otherwise there would exist an $a \in \mathbb{Z}$ such that $3^a = 5 \pmod{8}$). So $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathbb{F}_2 \oplus \mathbb{F}_2$.

Hence $(\mathbb{Z}/n\mathbb{Z})^\times \cong \Gamma(K/\mathbb{Q})$

- (c) By the fundamental theorem of Galois Theory, there exists a bijective correspondence between intermediate fields and Galois subgroups. In particular, the number of subgroups of $\Gamma(K/\mathbb{Q})$ of index 2 is equal to the number of intermediate fields with $[L : \mathbb{Q}] = 2$.

The three nontrivial automorphisms (found in (b)) each generate a subgroup of order 2. These subgroups have index 2 so there must be three intermediate fields. ★