

DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF MASSACHUSETTS, AMHERST

ADVANCED EXAM — ALGEBRA

AUGUST 27, 2001

Passing Standard: It is sufficient to do FIVE problems correctly, including at least ONE FROM EACH of the four parts.

All rings are commutative with 1, and every ring homomorphism takes 1 to 1.

Part I.

1. Show that there is no simple group of order 36. (Hint: You may quote the Sylow theorems, but otherwise provide all details.)

2. How many homomorphisms are there from the group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ to the dihedral group of order 8? (Hint: you can use the fact that the dihedral group of order 8 has exactly two subgroups isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.)

Part II.

1. (a) Prove that a finite integral domain must be a field.
(b) Determine all prime ideals and maximal ideals of the ring $\mathbf{Z}/n\mathbf{Z}$, for $n > 1$.

2. Determine all ring automorphisms of the polynomial ring $\mathbf{Z}[x]$.

Part III.

1. Determine an integer m such that $(\mathbf{Z}/10\mathbf{Z} \oplus \mathbf{Z}/21\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/9\mathbf{Z}) \simeq \mathbf{Z}/m\mathbf{Z}$ as \mathbf{Z} -modules.

2. Let M be the $n \times n$ matrix over a field K of characteristic zero such that every entry of M is 1.

- (a) Find the characteristic polynomial of M .
 - (b) Determine the Jordan canonical form of M over K .
-

Part IV.

1. Let F_1, F_2 be two intermediate subfields of a Galois extension K/k . Let $H_1 = \text{Gal}(K/F_1)$ and $H_2 = \text{Gal}(K/F_2)$. Show that H_1 and H_2 are conjugate (as subgroups) in $\text{Gal}(K/k)$ if and only if there exists an automorphism $\tau \in \text{Gal}(K/k)$ such that $\tau(F_1) = F_2$.

2. (a) Compute the minimal polynomial of $\sqrt{2} + \sqrt{-2}$ over \mathbf{Q} .
(b) Determine the Galois group of the Galois closure of the extension $\mathbf{Q}(\sqrt{2} + \sqrt{-2})/\mathbf{Q}$.

Note: Although it is NOT essential for this problem, you may find it convenient to use the fact that the resolvent cubic of $x^4 + bx^3 + cx^2 + dx + e$ is $x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2$.

**Solution to Algebra Advanced Exam
August 2001**

Part I, #1: Let G be a group of order 36. The number of Sylow 3-subgroups of G is $\equiv 1 \pmod{3}$ and divides 4. Thus there are 1 or 4 of them. If we get 1 then the Sylow 3-subgroup is normal. If not, denote by S the set of these four Sylow 3-subgroups. Sylow's Theorem says that G acts on S by conjugation, whence we get a permutation representation $\varphi : G \rightarrow \text{Perm}(S) \simeq S_4$. But $\#S_4 = 24$ while $\#G = 36$, so φ is not injective, whence $\ker \varphi$ is a non-trivial normal subgroup of G .

Part I, #2: The dihedral group D_8 has five subgroups T_1, \dots, T_5 of order 2, along with two subgroups $H_1, H_2 \simeq \mathbf{Z}/2 \times \mathbf{Z}/2$. There are three ways to map $\mathbf{Z}/2 \times \mathbf{Z}/2$ onto each T_i , so all together there are 15 homomorphisms with order 2 image. The maps from $\mathbf{Z}/2 \times \mathbf{Z}/2$ to each given H_i is the same as automorphisms of two-dimensional vector spaces over \mathbf{F}_2 , i.e. elements of $GL_2(\mathbf{F}_2)$. This group has six elements. Along with the trivial homomorphism, we get $15 + 2 \times 6 + 1 = 28$ maps.

Part II, #1: (a) Let A be a finite integral domain. Fix any non-zero element $b \in A$, and consider the map $\varphi : A \rightarrow A : x \mapsto bx$. Since A is a domain, $\ker \varphi$ is trivial. That means φ is an injective of finite set, and hence φ is bijective. In particular, there exists $\beta \in A$ such that $b\beta = 1$. Thus every non-zero element of A has an inverse, whence A is a field.

(b) Let \bar{I} be an ideal of $\mathbf{Z}/n\mathbf{Z}$. By the isomorphism theorems, \bar{I} corresponds to an ideal I of the ring \mathbf{Z} containing the ideal $n\mathbf{Z}$. Since \mathbf{Z} is a PID, we can write $I = m\mathbf{Z}$ for some integer m . The condition $I \supset n\mathbf{Z}$ then becomes $m|n$. Furthermore, the isomorphism theorems say that

$$(\mathbf{Z}/n\mathbf{Z})/\bar{I} \simeq \mathbf{Z}/m\mathbf{Z}.$$

Thus

$$\begin{aligned} \bar{I} \text{ is a prime ideal} &\Leftrightarrow \mathbf{Z}/m\mathbf{Z} \text{ is an integral domain} \\ &\Leftrightarrow m \text{ is a prime} \\ &\Leftrightarrow \mathbf{Z}/m\mathbf{Z} \text{ is a (finite) field} \\ &\Leftrightarrow \bar{I} \text{ is a maximal ideal.} \end{aligned}$$

Thus the set of maximal ideals of \mathbf{Z}/n coincides with the set of prime ideals of \mathbf{Z}/n , and is in bijective correspondence with the set of prime divisors of n .

Part II, #2: Let φ be such an automorphism. Ring automorphisms take 1 to 1, so φ fixes \mathbf{Z} . Also, $\varphi(x) \in \mathbf{Z}[x]$ and $\varphi^{-1}(x) \in \mathbf{Z}[x]$ as well, so $\deg(\varphi^{-1} \circ \varphi) = (\deg \varphi^{-1}) \times (\deg \varphi)$. But $x = \varphi^{-1}(\varphi(x))$, so both $\varphi(x)$ and $\varphi^{-1}(x)$ are linear. Write $\varphi(x) = ax + b$ and $\varphi^{-1}(x) = cx + d$ for some $a, b, c, d \in \mathbf{Z}$. Then $x = \varphi^{-1}(\varphi(x)) = (c(ax + d) + d)$, whence $\varphi(x) = \pm x \pm b$ for some $b \in \mathbf{Z}$.

Part III, #1: Using the distributive law for tensor products, we get

$$\begin{aligned} &(\mathbf{Z}/10\mathbf{Z} \oplus \mathbf{Z}/21\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/9\mathbf{Z}) \\ &\simeq \mathbf{Z}/10\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/10\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/9\mathbf{Z} \oplus \mathbf{Z}/21\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/21\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/9\mathbf{Z} \end{aligned}$$

Since $\mathbf{Z}/m\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/\gcd(m, n)\mathbf{Z}$, this becomes

$$\begin{aligned} & \mathbf{Z}/\gcd(10, 4)\mathbf{Z} \oplus \mathbf{Z}/\gcd(10, 9)\mathbf{Z} \oplus \mathbf{Z}/\gcd(21, 4)\mathbf{Z} \oplus \mathbf{Z}/\gcd(21, 9)\mathbf{Z} \\ & \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z} \\ & \simeq \mathbf{Z}/6\mathbf{Z}. \end{aligned}$$

Part III, #2: The row space of M is 1-dimensional, so $\dim \ker(M) = n - 1$. In particular, x^{n-1} exactly divides $\text{char}(M)$. On the other hand, if we denote by \vec{e} the column vector all of whose entries are 1, then $M\vec{e} = n\vec{e}$ since K has characteristic zero. Thus $x^{n-1}(x - n)$ divides $\text{char}(M)$. Compare degree and we see that in fact $\text{char}(M) = x^{n-1}(x - n)$. Finally, since the dimension of the eigenspace for 0 (resp. n) is $n - 1$ (resp. 1), the Jordan form of M is

$$\begin{pmatrix} n & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix}.$$

Part IV, #1: Fix $\tau \in \text{Gal}(K/k)$. Pick $h \in H_2$. Then $\tau^{-1}H_2\tau = H_1 \Leftrightarrow \tau^{-1}h\tau \in H_1 \Leftrightarrow \tau^{-1}h\tau x = x$ for all $x \in F_1 \Leftrightarrow h(\tau x) = \tau x$ for all $x \in F_1 \Leftrightarrow \tau x \in K^{H_2} = F_2$ for all $x \in F_1 \Leftrightarrow y \in K^{H_2} = F_2$ for all $y \in \tau(F_1) \Leftrightarrow \tau(F_1) \subset F_2$. A similar calculation gives $\tau^{-1}(F_2) \subset F_1$, whence $F_1 = \tau^{-1}\tau(F_1) \subset F_1$, so we have equality all the way through. In particular, $\tau^{-1}H_2\tau = H_1 \Leftrightarrow \tau(F_2) = F_1$.

Part IV, #2: (a) Set $b = \sqrt{2} + \sqrt{-2}$. Then $b^2 = 4\sqrt{-1}$, whence b is a root of $f(x) = x^4 + 16$. It is easy to check that f is irreducible over \mathbf{Z} , and hence over \mathbf{Z} by Gauss' Lemma. Thus $\mathbf{Q}(b) \simeq \mathbf{Q}[x]/f$ has degree 4 over \mathbf{Q} . The roots of f are 4-th roots of -16 , so any two roots differ by a multiple of a 4-th root of unity. But we saw that $4\sqrt{-1} = b^2 \in \mathbf{Q}(b)$, thus $\mathbf{Q}(b)$ contains all roots of f . Since $\mathbf{Q}(b)$ has characteristic zero, that means $\mathbf{Q}(b)/\mathbf{Q}$ is already Galois. In other words, $\mathbf{Q}(b)/\mathbf{Q}$ is its own Galois closure. Thus $\text{Gal}(\mathbf{Q}(b)/\mathbf{Q})$ has order 4. This leaves us with two choices: $\mathbf{Z}/4$ or $\mathbf{Z}/2 \times \mathbf{Z}/2$. To pin down the Galois group, note that $b = \sqrt{2} + \sqrt{-2}$, whence $b^3 = b\sqrt{-1} = \sqrt{-2} - \sqrt{2}$. Thus $b + b^3 = \sqrt{-2} \in \mathbf{Q}(b)$. Thus $\mathbf{Q}(b)$ contains more than one quadratic subfield, whence $\text{Gal}(\mathbf{Q}(b)/\mathbf{Q}) \simeq \mathbf{Z}/2 \times \mathbf{Z}/2$.

Alternative solution, for those who know about resolvent cubics: The resolvent cubic of f above is $x^3 - 64x = x(x - 8)(x + 8)$, which completely factors over \mathbf{Q} . Since f is irreducible over \mathbf{Q} , it follows that $\text{Gal}(f) \simeq \mathbf{Z}/2 \times \mathbf{Z}/2$. In particular, if we denote by N the Galois closure of $\mathbf{Q}(b)/\mathbf{Q}$, then $4 = \#\text{Gal}(f) = [N : \mathbf{Q}] \geq [\mathbf{Q}(b) : \mathbf{Q}] = 4$, whence $\mathbf{Q}(b)/\mathbf{Q}$ is its own Galois closure, and $\text{Gal}(\mathbf{Q}(b)/\mathbf{Q}) \simeq \mathbf{Z}/2 \times \mathbf{Z}/2$.