

Math 49 (3)

Final

Write all of your work in your bluebooks. You may write the problems in any order you like, but do not put work for more than one problem on the same page of your bluebook. When you are done, number the pages of your bluebook(s) and make a table of contents on the cover of the first one indicating which problems you worked and which pages I can find them on.

You may cite results proved in class, unless the problem itself amounts to such a result—in which case you should provide a proof.

Problem 1. let $p \in \mathbb{Z}$ be a positive prime.

a) Use unique factorization in \mathbb{Z} to show that \sqrt{p} is irrational.

Solution. Suppose that $\sqrt{p} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$. We would then have one integer with two equal formulations $pb^2 = a^2$. However p occurs an odd number of times in the prime factorization of pb^2 and an even number in a^2 . This contradicts unique factorization in \mathbb{Z} . \square

b) Use the Eisenstein criterion to show that \sqrt{p} is irrational.

Solution. If \sqrt{p} is rational, then it is a rational root of $f(x) = x^2 - p$ so $f(x)$ would be divisible by $x - \sqrt{p}$ and thus not be irreducible as an element of $\mathbb{Q}[x]$. However, p divides all the terms but the highest order term of $f(x)$ and p^2 does not divide the constant term of $f(x)$. So the Eisenstein criterion tells us that $f(x)$ is irreducible in $\mathbb{Q}[x]$. Thus \sqrt{p} cannot be rational. \square

Problem 2.

a) Explain why $[k] \in \mathbb{Z}_n$ is a unit if and only if k and n are relatively prime.

Solution. k and n are relatively prime if and only if there are integers s and t so that $ks + nt = 1$. there are integers s and t so that $ks + nt = 1$ if and only if $[k][s] = [1]$ in \mathbb{Z}_n . \square

b) Illustrate by using the Euclidean algorithm to find an inverse for $[8] \in \mathbb{Z}_{13}$.

Solution. Successive divisions yield,

$$\begin{aligned}13 &= 8 + 5 \\8 &= 5 + 3 \\5 &= 3 + 2 \\3 &= 2 + 1.\end{aligned}$$

Back-substitution gives,

$$\begin{aligned}1 &= 3 - 2 \\&= 3 - (5 - 3) = 2 \times 3 - 5 \\&= 2 \times (8 - 5) - 5 = 2 \times 8 - 3 \times 5 \\&= 2 \times 8 - 3 \times (13 - 8) \\&= 5 \times 8 - 3 \times 13.\end{aligned}$$

From this we see that $[8][5] = [1]$ so $[8]^{-1} = [5]$. □

Problem 3.

a) Show that $x^3 + x^2 - 1 \in \mathbb{Z}_3[x]$ is irreducible.

Solution. Let $p(x) := x^3 + x^2 - 1$ since the degree of $p(x)$ is 3, if it were to factor, it would have a linear term and thus a root. However, $\mathbb{Z}_3 = \{-1, 0, 1\}$ and $p(1) = 1$ while $p(0) = p(-1) = -1$, so $p(x)$ has no roots. □

b) Explain why $\mathbb{Z}_3[x]/(x^3 + x^2 - 1)$ is a field.

Solution. Generally speaking, whenever $p(x) \in k[x]$ is irreducible and k is a field, then so is $k[x]/(p(x))$. The reason for this is that if $[q(x)] \in k[x]/(p(x))$ is nonzero, then $p(x) \nmid q(x)$, so $p(x)$ and $q(x)$ are relatively prime, since $p(x)$ is irreducible. It follows that there are $s(x), t(x) \in k[x]$ so that $s(x)p(x) + t(x)q(x) = 1$. □

c) Illustrate by finding an inverse to the element $[x - 1]$.

Solution. Again, we use the Euclidean algorithm. First we carry out the repeated division, but this time it stops at the first stage:

$$x^3 + x^2 - 1 = (x - 1) \times (x^2 - x - 1) + 1.$$

So we see that $[x - 1]^{-1} = [-x^2 + x + 1]$. □

Problem 4. In this problem, you may use the results of problem 3 without proof. Let U be the group of units in $\mathbb{Z}_3[x]/(x^3 + x^2 - 1)$.

a) What is the order of U ?

Solution. We know that $\mathbb{Z}_3[x]/(x^3 + x^2 - 1)$ is a field, so all of the nonzero elements are units. Furthermore, the order of this field is $3^3 = 27$ so $|U| = 26$. □

b) What is the order of $[x] \in U$?

Solution. Since $|U| = 26$, the order of $[x]$ must be a divisor of 26. Since $[x^2] \neq [1]$, we know the order will be 13 or 26. Thus it suffices to calculate $[x]^{13} = [x^{13}]$. This we do by long division, obtaining

$$x^{13} = (x^{10} - x^9 + x^8 - x^6 - x^5 + x^4 + x^3 + x^2 + 1)(x^3 + x^2 - 1) + 1$$

so we see that $[x]^{13} = [1]$ and so the order of $[x]$ is 13. □

Problem 5. In the following problem we take \mathbb{k} to be a field $S \subseteq M_n(\mathbb{k})$ to be the subset of upper triangular $n \times n$ matrices (zero below the diagonal) and I to be the subset of strictly upper triangular matrices (zero on and below the diagonal). If this level of generality is too much, you may take $\mathbb{k} = \mathbb{R}$ and $n = 2$ for substantial partial credit.

a) Show that S is a subring of $M_n(\mathbb{k})$.

Solution. To see that S is a subring of $M_n(\mathbb{k})$, we need to see that S is closed under addition and multiplication and that 0 is in S . Closure under addition and $0 \in S$ are both immediate. To see that S is closed under multiplication, consider $A = [a_{ij}]$ and $B = [b_{ij}]$ in S . We have $a_{ij} = b_{ij} = 0$ whenever $i > j$. Choose $i > j$ we then have $[AB]_{ij} = \sum_k a_{ik}b_{kj} = 0$ because for every k , we either have $i > k$ or $k > j$. This shows that S is closed under multiplication. □

b) Show that I is a two-sided ideal in S .

Solution. Consider $A = [a_{ij}]$ in S and $B = [b_{ij}] \in I$. We have $a_{ij} = 0$ whenever $i > j$ and $b_{ij} = 0$ whenever $i \geq j$. Again I is clearly a subgroup of $(S, +)$. So we need to show that AB and BA are in I . Choose $i \geq j$. We then have $[AB]_{ij} = \sum_k a_{ik}b_{kj} = 0$ because for every k we either have $i > k$ or $k \geq j$. Similarly, we have $[BA]_{ij} = \sum_k b_{ik}a_{kj} = 0$ because for every k we either have $i \geq k$ or $k > j$. (Alternatively, one can identify I as the kernel of the homomorphism f given in the solution to the next part.) \square

c) Use the first isomorphism theorem to identify S/I as isomorphic to another subring of $M_n(\mathbb{k})$.

Solution. Let R be the subring of $M_n(\mathbb{k})$ consisting of diagonal matrices. Let $f: S \rightarrow R$ be the map which takes each upper triangular matrix to the diagonal matrix with the same diagonal entries. That is to say, we have

$$[f(A)]_{ij} = \begin{cases} a_{ii} & , \text{ if } i = j \\ 0 & \text{ otherwise.} \end{cases}$$

$f(A + B) = f(A) + f(B)$ is immediate. Furthermore, if $a_{ij} = b_{ij} = 0$ for all $i > j$ and $A = [a_{ij}]$ and $B = [b_{ij}]$ then we have $[AB]_{ii} = \sum_k a_{ik}b_{ki} = a_{ii}b_{ii}$ since all the other terms are zero. This shows that $F(AB) = f(A)f(B)$, so f is a homomorphism of rings. It is clear that the kernel of f is I and that f is surjective. The first isomorphism theorem then gives that $S/I \approx R$. \square

Problem 6. Let G be a group and $\mathcal{Z} = \mathcal{Z}(G)$ be its center.

a) Give a careful explanation of why \mathcal{Z} is a normal subgroup of G .

Solution. An element $c \in G$ is in the center exactly when $cg = gc$ for every $g \in G$. Equivalently $gcg^{-1} = c$. Thus we see that $g\mathcal{Z}g^{-1} = \mathcal{Z}$ —that is to say \mathcal{Z} is normal. \square

b) Prove that G/\mathcal{Z} cannot be a nontrivial cyclic group.

Solution. This is a result we proved in class, but of course, just citing that result is not sufficient. We suppose that G/\mathcal{Z} is cyclic and we will show that $\mathcal{Z} = G$. Let $a\mathcal{Z}$ be a generator for G/\mathcal{Z} . We will show that every element of G can be written as $a^i c$ for some integer i and some $c \in \mathcal{Z}$. Given $g \in G$ $g\mathcal{Z} = a^i \mathcal{Z}$ for some i , because $a\mathcal{Z}$ generates G/\mathcal{Z} . Thus $g = a^i c$ for $c \in \mathcal{Z}$ as desired. Now if $g_1, g_2 \in G$ are arbitrary, choose integers i_1, i_2 and $c_1, c_2 \in \mathcal{Z}$ so that $g_1 = a^{i_1} c_1$ and $g_2 = a^{i_2} c_2$. It then follows that $g_1 g_2 = a^{i_1+i_2} c_1 c_2 = g_2 g_1$. That is to say G is commutative, so $G = \mathcal{Z}$ as desired. \square

Problem 7. Let p and q be distinct primes and suppose that G is a group of order pq . Suppose that a and b are elements of G with orders $|a| = p$ and $|b| = q$.

a) Prove that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Solution. Every nontrivial element of $\langle a \rangle$ has order p while every nontrivial element of $\langle b \rangle$ has order q , thus there can be no nontrivial elements in common to both groups. \square

b) Suppose further that both $\langle a \rangle$ and $\langle b \rangle$ are normal subgroups of G . Prove that G is abelian.

Solution. Since $A = \langle a \rangle$ and $B = \langle b \rangle$ are normal and $A \cap B = \{e\}$, we know that the map $A \times B \rightarrow G$ which carries (a, b) to ab is an injective homomorphism. However, since $|A \times B| = pq = |G|$, this homomorphism is in fact an isomorphism. So $G \approx A \times B$. But $A \times B$ is abelian since both A and B are. \square

c) Give an example to show that when $\langle a \rangle$ and $\langle b \rangle$ are not both normal, G may not be abelian.

Solution. In S_3 , we have $|(01)| = 2$ and $|(123)| = 3$ while $|S_3| = 2 \times 3$ and S_3 is not abelian. \square

Problem 8. Recall that S_n denotes the symmetric group of order $n!$. For each of the following statements, determine whether it is true or false. In either case prove your assertion with a proof or an example.

a) There is a surjective homomorphism $S_4 \rightarrow S_3$.

Solution. There is such a thing. We will demonstrate its existence, by producing a normal subgroup $H \triangleleft S_4$ with $|H| = 4$ and G/H nonabelian. Since $|S_4/H| = 4!/4 = 6$, and since every nonabelian group of order 6 is isomorphic to S_3 , this will be the composite $S_4 \rightarrow S_4/H \rightarrow S_3$ of the quotient epimorphism and the isomorphism will give the desired epimorphism $S_4 \rightarrow S_3$. We will take $H := \{e, (12)(34), (13)(24), (14)(23)\}$. It is straightforward to check that H is a subgroup by showing its closure in a multiplication table. H is normal, because it is a union of conjugacy classes, since a conjugacy class is all elements sharing a particular cycle structure, and H consists of the identity together with the products of pairs of disjoint transpositions. Finally G/H is nonabelian, since H does not contain the commutator subgroup. In particular $(12)(123)(12)^{-1}(123)^{-1} = (132)(132) = (123) \notin H$. \square

b) There is a surjective homomorphism $S_5 \rightarrow S_4$.

Solution. If there were such a homomorphism, its kernel would be a normal subgroup of S_5 with order 5, by the first isomorphism theorem and Lagrange's theorem. Since the only normal subgroup of S_5 is A_5 , this cannot happen. \square

Problem 9 (Only do this if you have finished all the other problems, and you still have time left over.) Throughout this exam, while your answers have all been justified with clear explanations, you will have cited some results from class. If you have finished and there is still time left, identify one or more of those results, state it (or them), and provide a proof (or proofs).