

MATH 321 Final Examination Answer Key

(1) Give an example of a fact that you have known long before taking MATH 321 but which you recognized in MATH 321 to be a piece of information about groups.

There are lots of possible answers here. For example, you may have learned that the well-known identities

$$\begin{aligned}\cos(a + b) &= \cos a \cos b - \sin a \sin b \\ \sin(a + b) &= \sin a \cos b + \cos a \sin b\end{aligned}$$

express that the set of rotations is a subgroup of $\text{Isom}(E)$.

(2) Denote the residue class of $a \in \mathbb{Z}$ modulo 18 by \bar{a} , modulo 24 by \tilde{a} . Is the “mapping” $\varphi : \mathbb{Z}_{18} \rightarrow \mathbb{Z}_{24}$, $\bar{a} \mapsto \tilde{a}$ a group homomorphism?

We have $\overline{18} = \bar{0}$ but $18\varphi = \tilde{18} \neq \tilde{0} = 0\varphi$, so φ is not well defined and cannot be a group homomorphism.

(3) Are \mathbb{Z}_9^\times and \mathbb{Z}_{18}^\times isomorphic groups?

In \mathbb{Z}_9^\times , we have $2^1 = 2 \neq 1$, $2^2 = 4 \neq 1$, $2^3 = 8 \neq 1$, $2^4 = 7 \neq 1$, $2^5 = 5 \neq 1$, $2^6 = 1$, so $|\langle 2 \rangle| = o(2) = 6 = \varphi(9) = |\mathbb{Z}_9^\times|$ and $\mathbb{Z}_9^\times = \langle 2 \rangle$ is a cyclic group of order 6.

In \mathbb{Z}_{18}^\times , we have $5^1 = 5 \neq 1$, $5^2 = 7 \neq 1$, $5^3 = -1 \neq 1$, $5^4 = -5 \neq 1$, $5^5 = -7 \neq 1$, $5^6 = 1$, so $|\langle 5 \rangle| = o(5) = 6 = \varphi(18) = |\mathbb{Z}_{18}^\times|$ and $\mathbb{Z}_{18}^\times = \langle 5 \rangle$ is a cyclic group of order 6.

Hence $\mathbb{Z}_9^\times \cong C_6 \cong \mathbb{Z}_{18}^\times$: the groups \mathbb{Z}_9^\times and \mathbb{Z}_{18}^\times are indeed isomorphic.

(4) Can there exist a group G and an element a of G such that $o(a^3) = 20$ and $o(a^5) = 9$? Either give an example of such a pair G, a , or prove that this is impossible.

Suppose that G, a is such a pair. Then $a^{60} = (a^3)^{20} = 1$ and $o(a)$ is finite, and in fact a divisor of 60. As $(o(a), 3) = 1$ or $(o(a), 3) = 3$, from $20 = o(a^3) = \frac{o(a)}{(o(a), 3)}$, we get $o(a) = 20$ or $o(a) = 60$, this yields $9 = o(a^5) = \frac{o(a)}{(o(a), 5)} = \frac{20}{(20, 5)} = 5$ or $9 = o(a^5) = \frac{o(a)}{(o(a), 5)} = \frac{60}{(60, 5)} = 12$, which is impossible. Thus such a pair cannot exist.

(5) Let $F = \langle f \rangle$ be a cyclic group of order 4 and $T = \langle t \rangle$ a cyclic group of order 10. Find all group homomorphisms from F into T .

Let φ be a homomorphism from $F = \langle f \rangle$ into $T = \langle t \rangle$. Then

$$F/\text{Ker } \varphi \cong \text{Im } \varphi \leq T$$

yields

$$|F/\text{Ker } \varphi| = |\text{Im } \varphi| \mid |T|$$

and by Lagrange’s theorem, $|F/\text{Ker } \varphi| = |F : \text{Ker } \varphi|$ is both a divisor of $|F| = 4$ and a divisor of $|T| = 10$, so it is a divisor of $(4, 10) = 2$. Hence $|F/\text{Ker } \varphi| = |\text{Im } \varphi| = 1$ or $|F/\text{Ker } \varphi| = |\text{Im } \varphi| = 2$.

In the first case $|F/\text{Ker } \varphi| = |\text{Im } \varphi| = 1$, we have $F = \text{Ker } \varphi$, so φ must be the function for which $a\varphi = 1 \in T$ for all $a \in F$. This φ is really a homomorphism since $(ab)\varphi = 1 = 1 \cdot 1 = a\varphi \cdot b\varphi$ for all $a, b \in F$.

In the second case $|F/\text{Ker } \varphi| = |\text{Im } \varphi| = 2$, the kernel $\text{Ker } \varphi$ must be the unique subgroup of the cyclic group $F = \langle f \rangle$ of index 2, and we know that this subgroup is $\langle f^2 \rangle = \{1, f^2\}$. Also $\text{Im } \varphi$ must be the unique subgroup of the cyclic group $T = \langle t \rangle$ that has order 2, and we know that this subgroup is $\langle t^{10/2} \rangle = \langle t^5 \rangle = \{1, t^5\}$. It follows that φ maps 1 and f^2 to $1 \in T$, and maps f to t^5 , $f^3 = f^2 \cdot f$ to $f^2\varphi \cdot f\varphi = 1 \cdot t^5 = t^5$. Hence φ must be the function

$$\begin{aligned} f^0 = 1 &\mapsto 1 = t^0 = t^{5 \cdot 0} \\ f^1 = f &\mapsto t^5 = t^{5 \cdot 1} \\ f^2 = f^2 &\mapsto 1 = t^{10} = t^{5 \cdot 2} \\ f^3 = f^3 &\mapsto t^5 = t^{15} = t^{5 \cdot 3}. \end{aligned}$$

This φ is really a homomorphism since $(f^m f^n)\varphi = f^{m+n}\varphi = t^{5(m+n)} = t^{5m+5n} = t^{5m}t^{5n} = (f^m)\varphi(f^n)\varphi$ for all $m, n \in \mathbb{Z}$.

Thus there are exactly two homomorphisms from F into T . These are the function $f^m \mapsto 1$ and the function $f^m \mapsto t^{5m}$.

(6) If $a, b, c \in \mathbb{Z}_{11}$ and $G := \{g \in \text{GL}(2, \mathbb{Z}_{11}) : \det g \in \{4, 5, a, b, c\}\}$ is a group, what are a, b and c ?

Since G is a group, the identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is in G , so $1 = \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \{4, 5, a, b, c\}$ and one of a, b, c is equal to 1, say $a = 1$. Then we get $G \supseteq \text{SL}(2, \mathbb{Z}_{11}) = \text{Ker } \det$, where $\det : \text{GL}(2, \mathbb{Z}_{11}) \rightarrow \mathbb{Z}_{11}^\times$ is the surjective determinant homomorphism. We know that any subgroup of $\text{GL}(2, \mathbb{Z}_{11})$ containing $\text{Ker } \det$ is the preimage, under \det , of a suitable subgroup H of \mathbb{Z}_{11}^\times , so it has the form $\{g \in \text{GL}(2, \mathbb{Z}_{11}) : \det g \in H\}$ for some subgroup H of \mathbb{Z}_{11}^\times . Hence $\{4, 5, a, b, c\} = \{4, 5, 1, b, c\}$ must be a subgroup of \mathbb{Z}_{11}^\times , it must be closed under multiplication: $4 \cdot 5 = 9$ and $4 \cdot 9 = 3$ must be in it, so b, c are 9, 3.

(7) Let G be a group, H a commutative group, $\varphi : G \rightarrow H$ a homomorphism onto H . Let N be a subgroup of G that contains $\text{Ker } \varphi$. Show that N is a normal subgroup of G .

Since H is abelian and $G/\text{Ker } \varphi \cong \text{Im } \varphi = H$, the factor group $G/\text{Ker } \varphi$ is also abelian, so every subgroup of $G/\text{Ker } \varphi$ is normal in $G/\text{Ker } \varphi$. In particular, $N/\text{Ker } \varphi \trianglelefteq G/\text{Ker } \varphi$. The theorem that describes the correspondence between subgroups of G and the subgroups of $G/\text{Ker } \varphi$ yields now $N \trianglelefteq G$.

(8) Let H be a subgroup of a group G . Suppose $g \in G$ and $o(g) = n \in \mathbb{N}$. If $g^m \in H$ and if m and n are relatively prime, prove that $g \in H$.

There are integers a, b with $am + bn = 1$, so $g = g^1 = g^{am+bn} = g^{am}g^{bn} = (g^m)^a(g^n)^b = (g^m)^a 1^b = (g^m)^a$. As H is closed under multiplication and taking inverses, and as $g^m \in H$, its (positive or negative) power $(g^m)^a$ also belongs to H , i.e., $g = (g^m)^a \in H$.

(9) Let G be a group, $N \leq G$, $A \subseteq G$. If $N \trianglelefteq G$, does $AN = NA$ have to hold true?

Let $x \in AN$. There are $a \in A$, $n \in N$ with $x = an$. From $N \trianglelefteq G$, we get $ana^{-1} \in N$ and so $x = an = ana^{-1}a = ana^{-1} \cdot a \in Na \subseteq NA$, so $x \in NA$. This proves $AN \subseteq NA$.

Let $y \in NA$. There are $n \in N$, $a \in A$ with $y = na$. From $N \trianglelefteq G$, we get $a^{-1}na \in N$ and so $y = na = aa^{-1}na = a \cdot a^{-1}na \in aN \subseteq AN$, so $y \in AN$. This proves $NA \subseteq AN$.

Hence $AN = NA$.

(10) Give an example of a field different from \mathbb{Q} , \mathbb{R} , \mathbb{C} , \mathbb{Z}_p (p prime).

For example, the field $\mathbb{Q}(i) := \{a + bi \in \mathbb{C} : a, b \in \mathbb{Q}\}$ of fractions of $\mathbb{Z}[i]$ or the field $\{f/g : f, g \in \mathbb{Z}[x], g \neq 0\}$ of rational functions over \mathbb{Z} are different from \mathbb{Q} , \mathbb{R} , \mathbb{C} , \mathbb{Z}_p . There are many other examples.

(11) Characterize all rings in which the identity $x^2 - y^2 = (x + y)(x - y)$ is valid.

In any ring R , we have $(x + y)(x - y) = x(x - y) + y(x - y) = xx - xy + yx - yy = x^2 - y^2 + (yx - xy)$, so the above identity holds in R if and only if $yx - xy = 0$ for all $x, y \in R$, i.e., if and only if $xy = yx$ for all $x, y \in R$, so if and only if R is a commutative ring.

(12) Let A be an ideal of R . Is it true that $\text{Mat}_2(R)/\text{Mat}_2(A) \cong \text{Mat}_2(R/A)$?

For $r \in R$, let's denote by \bar{r} the coset $r + A \in R/A$ of A determined by r . Consider the mapping

$$\varphi : \text{Mat}_2(R) \longrightarrow \text{Mat}_2(R/A), \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}.$$

Since $\overline{\bar{r} + \bar{s}} = \overline{r + s}$ and $\overline{\bar{r} \cdot \bar{s}} = \overline{r \cdot s}$ for any $r, s \in R$, we have

$$\begin{aligned} \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right] \varphi &= \begin{pmatrix} a + e & b + f \\ c + g & d + h \end{pmatrix} \varphi = \begin{pmatrix} \overline{a + e} & \overline{b + f} \\ \overline{c + g} & \overline{d + h} \end{pmatrix} \\ &= \begin{pmatrix} \bar{a} + \bar{e} & \bar{b} + \bar{f} \\ \bar{c} + \bar{g} & \bar{d} + \bar{h} \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} + \begin{pmatrix} \bar{e} & \bar{f} \\ \bar{g} & \bar{h} \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \varphi + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \varphi \end{aligned}$$

and

$$\begin{aligned} \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right] \varphi &= \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} \varphi = \begin{pmatrix} \overline{ae + bg} & \overline{af + bh} \\ \overline{ce + dg} & \overline{cf + dh} \end{pmatrix} \\ &= \begin{pmatrix} \bar{a} \cdot \bar{e} + \bar{b} \cdot \bar{g} & \bar{a} \cdot \bar{f} + \bar{b} \cdot \bar{h} \\ \bar{c} \cdot \bar{e} + \bar{d} \cdot \bar{g} & \bar{c} \cdot \bar{f} + \bar{d} \cdot \bar{h} \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \begin{pmatrix} \bar{e} & \bar{f} \\ \bar{g} & \bar{h} \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \varphi \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} \varphi \end{aligned}$$

for every $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in \text{Mat}_2(R)$, so φ is a ring homomorphism.

Any element of $\text{Mat}_2(R/A)$ has the form $\begin{pmatrix} a+A & b+A \\ c+A & d+A \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \varphi \in \text{Im } \varphi$, so $\text{Im } \varphi = \text{Mat}_2(R/A)$.

We have

$$\begin{aligned} \text{Ker } \varphi &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_2(R) : \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_2(R) : \bar{a} = \bar{0}, \bar{b} = \bar{0}, \bar{c} = \bar{0}, \bar{d} = \bar{0} \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_2(R) : a \in A, b \in A, c \in A, d \in A \right\} \\ &= \text{Mat}_2(A). \end{aligned}$$

Therefore the formula $\text{Mat}_2(R)/\text{Ker } \varphi \cong \text{Im } \varphi$ yields $\text{Mat}_2(R)/\text{Mat}_2(A) \cong \text{Mat}_2(R/A)$.

(13) Let D be a principal ideal domain, a, b relatively prime elements of D . Is D/abD isomorphic to $D/aD \oplus D/bD$?

Let's denote the coset $x + aD$ by \bar{x} , and the coset $x + bD$ by \tilde{x} and consider the function $\varphi : D \rightarrow D/aD \oplus D/bD$ given by $x\varphi = (\bar{x}, \tilde{x})$ for all $x \in D$. Since

$$(x+y)\varphi = (\overline{x+y}, \widetilde{x+y}) = (\bar{x} + \bar{y}, \tilde{x} + \tilde{y}) = (\bar{x}, \tilde{x}) + (\bar{y}, \tilde{y}) = x\varphi + y\varphi$$

and

$$(xy)\varphi = (\overline{xy}, \widetilde{xy}) = (\bar{x} \cdot \bar{y}, \tilde{x} \cdot \tilde{y}) = (\bar{x}, \tilde{x})(\bar{y}, \tilde{y}) = x\varphi \cdot y\varphi$$

for all $x, y \in D$, this function φ is a homomorphism. Thus $D/\text{Ker } \varphi \cong \text{Im } \varphi$.

We have

$$\begin{aligned} \text{Ker } \varphi &= \{x \in D : (\bar{x}, \tilde{x}) = (\bar{0}, \tilde{0})\} \\ &= \{x \in D : \bar{x} = \bar{0}, \tilde{x} = \tilde{0}\} \\ &= \{x \in D : x \in aD, x \in bD\} \\ &= aD \cap bD. \end{aligned}$$

Now, if $x \in aD \cap bD$, then there are elements d, e in D with $x = ad = be$; here $a \mid be$ and since D is a principal ideal domain and a is relatively prime to b , we get $a \mid e$. So $af = e$ for some $f \in D$ and $x = be = b(af) = abf \in abD$. This proves $aD \cap bD \subseteq abD$. On the other hand, if $y \in abD$, then $y = abd$ for some $d \in D$, so $y = a(db) \in aD$ and $y = b(ad) \in bD$, so $y \in aD \cap bD$. This proves $abD \subseteq aD \cap bD$. Hence $\text{Ker } \varphi = aD \cap bD = abD$.

Next we examine $\text{Im } \varphi$. Since D is a principal ideal domain and a, b are relatively prime, there are $a', b' \in D$ such that $aa' + bb' = 1$. Any element

of $D/aD \oplus D/bD$ has the form (\bar{r}, \tilde{s}) for some $r, s \in D$. If we define $x := saa' + rbb'$, we find

$$\begin{aligned}
 x\varphi &= (\bar{x}, \tilde{x}) \\
 &= (\overline{saa' + rbb'}, \widetilde{saa' + rbb'}) \\
 &= (\overline{rbb'}, \widetilde{saa'}) \\
 &= (\overline{r(1 - aa')}, \widetilde{s(1 - bb')}) \\
 &= (\overline{r - ara'}, \widetilde{s - bsb'}) \\
 &= (\bar{r}, \tilde{s}).
 \end{aligned}$$

So every element (\bar{r}, \tilde{s}) is the image of a suitable $x \in D$ under φ . Hence $\text{Im } \varphi = D/aD \oplus D/bD$.

We obtain $D/abD = D/\text{Ker } \varphi \cong \text{Im } \varphi = D/aD \oplus D/bD$.