Solutions to Homework for M351 – Algebra I

Examples & Hwk 32:

> If R and S are rings, then the mappings $i_1 : R \to R \oplus S$, $a \mapsto (a, 0)$ and $i_2 : S \to R \oplus S$, $b \mapsto (0, b)$ are ring homomorphisms. Moreover, the mapping $i_D : R \to R \oplus R$, $a \mapsto (a, a)$ is a ring homomorphism.
>
> The mapping $R \to R[i]$, $x \mapsto (x, 0)$ is a ring homomorphism.

Solution: $i_1(a + a') = (a + a', 0) = (a, 0) + (a', 0) = i_1(a) + i_1(a')$. Analogous proof for times instead of plus. So the homomorphism is proved easily. i_1 is 1-1 but, unless S is the ring consisting of 0 only, it is not onto.

Analogous statements hold for i_2 and i_D.

Examples & Hwk 33:

> Given a ring R, is the mapping $x \mapsto -x$, $R \to R$ a ring automorphism?

Solution: The mapping is clearly one-to-one and onto, being its own inverse. But it is in general not a ring homomorphism. It does satisfy $-(a + b) = (-a) + (-b)$, which makes it at least a group automorhism for the additive group; but for the mapping to be a ring homomorphism, it would also be required that $(-a)(-b) = -(ab)$ for all a, b. But $(-a)(-b) = ab$.

So the mapping is a ring automorphism if and only if $-ab = ab$ for all a, b. Sufficient for this condition is $-a = a$ for all a. (In which case the mapping is the identity.) In a ring with 1, this is also necessary, since we can choose $b = 1$.

Examples & Hwk 34:

> The mapping $\mathbb{Z} \to \mathbb{Z}_n$, $x \mapsto \bar{x}_n$ (the congruence class of x modulo n) is a ring homomorphism.

Solution: Homomorphism proofs in class. The homomorphism is not 1-1 ($\bar{0} = \bar{n}$, even though $0 \neq n$), but it is onto.

Examples & Hwk 35:

> The mapping $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$, $A \mapsto \det A$ is a group homomorphism. (Note that $\mathbb{R}^*$ is the group of all invertible real numbers (i.e., all real numbers other than 0), together with multiplication.) Is the mapping $\det : M_n(\mathbb{R}) \to \mathbb{R}$, $A \mapsto \det A$ a ring homomorphism?

Solution: The group homomorphism property is simply $\det(AB) = (\det A)(\det B)$. It is clearly not 1-1 (unless $n = 1$) since different matrices can have the same determinant. But it is onto: To exhibit an invertible matrix with determinant $a \neq 0$, we can take a diagonal matrix with all 1's on the diagonal, except for one diagonal entry, which is to be a. (By choosing which diagonal entry is to be a (and choosing $a \neq 1$), we get a counterexample for 1-1.

det is not a ring homomorphism (unless $n = 1$), because '$\det(A + B) = (\det A) + (\det B)$' is not true. (Take $A = B = I$ as a counterexample.)

In the exceptional case $n = 1$ (1×1 matrices), det is a ring isomorphism and identifies the matrix $[a]$ with the number a.

Examples & Hwk 36:

> Given any interval $[a,b] \subset \mathbb{R}$ (with $b > a$), the mapping $I : C^0[0,1] \to C^0[a,b]$ given by $(I(f))(x) := f(\frac{x-a}{b-a})$ for $a \le x \le b$ is a ring isomorphism.
>
> If $[0,1] \supseteq [a,b]$, then the mapping $J : f \mapsto f|_{[a,b]}$ which restricts the domain of a function f to the smaller domain $[a,b]$ is a ring homomorphism. It is onto, but (unless $[a,b] = [0,1]$) not 1-to-1.

Solution: First note that I is well-defined. For $x \in [a,b]$, it holds $\frac{x-a}{b-a} \in [0,1]$, and therefore $f(\frac{x-a}{b-a})$ makes sense. $I(f) = f \circ h$ with $h(x) = \frac{x-a}{b-a}$, so $I(f)$ is a continuous function, being the composition of continuous functions.

For the homomorphism property, we must show $I(f+g) = I(f) + I(g)$ and $I(f \cdot g) = I(f) \cdot I(g)$, which means $(I(f+g))(x) = (I(f)+I(g))(x)$ for every x, and similarly for the case of the product. Now indeed,

$$(I(f+g))(x) = (f+g)(\frac{x-a}{b-a}) = f(\frac{x-a}{b-a}) + g(\frac{x-a}{b-a}) = (I(f))(x) + (I(g))(x) = (I(f)+I(g))(x)$$

A very analogous calculation applies to 'times'.

The homomorphism property of J is trivial. To show that J is onto, amounts to showing that any continuous function f on $[a,b]$ can be extended to a continuous function g on $[0,1]$. We define $g(x) = f(a)$ if $0 \le x \le a$, $g(x) = f(x)$ if $a \le x \le b$, and $g(x) = f(b)$ if $b \le x \le 1$. Then $J(g) = f$.

Since there are different such extensions (unless $a = 0$, $b = 1$), we have ample counterexamples for 1-1. For instance if $b < 1$, we can define $g_1(x) := f(b) + x - b$ if $b \le x \le 1$ (and $g_1(x) = g(x)$ for $0 \le x \le b$). Then $g_1 \ne g$ in $C^0[0,1]$, but $J(g_1) = J(g)$. The case $a > 0$ allows an analogous construction.

Examples & Hwk 37:

> Given any ring R and any set X, the set of all functions $f : X \to R$, together with addition and multiplication defined by $(f+g)(x) := f(x) + g(x)$, $(fg)(x) := f(x)g(x)$, is a ring. (Can you prove this?) We sometimes call this ring R^X.
>
> The mapping $\chi : \mathcal{P}(M) \to (\mathbb{Z}_2)^M$, $A \mapsto \chi_A$, where the function χ_A is defined by $\chi_A(x) = 0$ if $x \notin A$ and $\chi_A(x) = 1$ if $x \in A$, is a ring isomorphism. (The main difficulty in proving this statement is to carefully understand what is being said. And the best test of whether you have understood the statement is whether you can reproduce it closed-notes, without rote memorization.)

Solution: I'll skip the rather trivial proof that R^X is a ring. For the ring homomorphism property we have to show, for $A, B \in \mathcal{P}(M)$ (i.e., for $A, B \subseteq M$) that $\chi_{A+B} = \chi_A + \chi_B$ and $\chi_{A \cdot B} = \chi_A \cdot \chi_B$. These are equations of functions defined on M. So we have to show $\chi_{A+B}(x) = \chi_A(x) + \chi_B(x)$ and $\chi_{A \cdot B}(x) = \chi_A(x)\chi_B(x)$ for all $x \in M$.

Proof of $\chi_{A \cdot B}(x) = \chi_A(x)\chi_B(x)$: Since the only values for these functions are 0 and 1 in $\mathbb{Z}_2$, we conclude that $\chi_A(x)\chi_B(x)$ equals 1 if and only if both factors are 1, i.e., iff $x \in A$ and $x \in B$, which is equivalent to $x \in A \cap B = A \cdot B$. This in turn is equivalent to $\chi_{A \cdot B}(x) = 1$. So $\chi_A(x)\chi_B(x) = 1$ iff $\chi_{A \cdot B}(x) = 1$. With only one other value, 0, available ($\chi(x) = 0$ iff $\chi(x) \ne 1$), we conclude $\chi_{A \cdot B} = \chi_A \cdot \chi_B$

Proof of $\chi_{A+B}(x) = \chi_A(x) + \chi_B(x)$: The reasoning is similar: We note that $\chi_A(x) + \chi_B(x)$ is 1 if and only if exactly one of $\chi_A(x)$, $\chi_B(x)$ is 1, i.e., iff x is contained in exactly one of A and B. This is equivalent to $x \in A + B$, by the definition of $A + B$. We conclude again: $\chi_A(x) + \chi_B(x) = 1$ iff $\chi_{A+B}(x) = 1$.

Examples & Hwk 38:

> The map $R \to M_2(R)$, $x \mapsto \left[\begin{array}{cc} x & 0 \\ 0 & x \end{array}\right]$ is a ring homomorphism.

Solution: Call this map I. So $I(x) = \left[\begin{array}{cc} x & 0 \\ 0 & x \end{array}\right]$. Since $I(x+y)$ and $I(x)+I(y)$ are equal, namely they are $\left[\begin{array}{cc} x+y & 0 \\ 0 & x+y \end{array}\right]$, and since also $I(xy) = I(x)I(y)$, namely both sides equal $\left[\begin{array}{cc} xy & 0 \\ 0 & xy \end{array}\right]$, we know that I is a ring homomorphism. It is clearly not onto, because the image does not contain non-diagonal matrices, But it is trivially 1-1.

Examples & Hwk 39:

> The map $\mathbb{C}^* \to GL_2(\mathbb{R})$, $\alpha + i\beta \mapsto \left[\begin{array}{cc} \alpha & -\beta \\ \beta & \alpha \end{array}\right]$ is a group homomorphism.

Solution: Let this map be called I again. It is well-defined since the matrix $I(\alpha + i\beta)$ is indeed invertible (its determinant is $\alpha^2 + \beta^2 \neq 0$), because $\alpha + \beta i \neq 0$. ($0 \notin \mathbb{C}^*$.)

We must show $I((\alpha + i\beta)(\gamma + i\delta)) = I(\alpha + i\beta)I(\gamma + i\delta)$.

$$I((\alpha + i\beta)(\gamma + i\delta)) = I(\alpha\gamma - \beta\delta + i(\alpha\delta + \beta\gamma)) = \left[\begin{array}{cc} \alpha\gamma - \beta\delta & -(\alpha\delta + \beta\gamma) \\ \alpha\delta + \beta\gamma & \alpha\gamma - \beta\delta \end{array}\right]$$

On the other hand,

$$I(\alpha + i\beta)I(\gamma + i\delta) = \left[\begin{array}{cc} \alpha & -\beta \\ \beta & \alpha \end{array}\right] \left[\begin{array}{cc} \gamma & -\delta \\ \delta & \gamma \end{array}\right] = \left[\begin{array}{cc} \alpha\gamma - \beta\delta & -\alpha\delta - \beta\gamma \\ \beta\gamma + \alpha\delta & -\beta\delta + \alpha\gamma \end{array}\right]$$

So both are indeed equal.

Examples & Hwk 40:

> Take the group consisting of the six rational functions $I, F_0, F_1, F_\infty, M, W$ discussed in Ex&Hwk. 8, and the group S_3 discussed in Ex.&Hwk. 7. Write down the group tables and show that these two groups are isomorphic, by explicitly exhibiting a group isomorphism.

Solution: Let's repeat the group table for the group of six functions from Hwk 8:

$\circ$	I	F_0	F_1	F_∞	M	W
I	I	F_0	F_1	F_∞	M	W
F_0	F_0	I	W	M	F_∞	F_1
F_1	F_1	M	I	W	F_0	F_∞
F_∞	F_∞	W	M	I	F_1	F_0
M	M	F_1	F_∞	F_0	W	I
W	W	F_∞	F_0	F_1	I	M

In writing down the group table for the permutation group S_3, we have the choice in which order to put the elements into the columns. We want to do it in such a way that the isomorphism becomes visible. We denote the identical permutation (123) by i. We'll assign names f_0, f_1, f_∞, m and w to the remaining permutations, hoping to construct the group isomorphism as $I \mapsto i$, $F_0 \mapsto f_0$, $F_1 \mapsto f_1$, $F_\infty \mapsto f_\infty$, $M \mapsto m$, $W \mapsto w$.

There are three permutations that are their own inverses, namely (213), (321) and (132). They should be matched with the functions F_0, F_1, F_∞, which are also their own inverses in their group. Which do we match with which? We try one such match, tentatively. *(It seems daunting, because there are six ways to match these, so we may be worried how often we have to try to be successful; but it turns out that any choice we make at this point will lead to a success. So there will actually be more than one isomorphism between these two groups.)*

So I'll call $(213) =: f_0$, $(321) =: f_1$ and $(132) =: f_\infty$, hoping to let the (yet to be constructed) group isomorphism match the capital letters with the corresponding lowercase letters. Since $F_0 \circ F_1 = W$, we let $(213) \circ (321) = (312) =: w$; that leaves $(231) =: m$. Now we must write up the group table for these permutations. If the whole group table for S_3, written in this notation is just the lowercase version of the group table for the rational functions, then we have an isomorphism.

Indeed, we get the table

	(123)	(213)	(321)	(132)	(231)	(312)
$\circ$	$= i$	$= f_0$	$= f_1$	$= f_\infty$	$= m$	$= w$
i	i	f_0	f_1	f_∞	m	w
f_0	f_0	i	w	m	f_∞	f_1
f_1	f_1	m	i	w	f_0	f_∞
f_∞	f_∞	w	m	i	f_1	f_0
m	m	f_1	f_∞	f_0	w	i
w	w	f_∞	f_0	f_1	i	m

and have therefore constructed an isomorphism. As mentioned, there are other solutions.

Note: In complex variables, these six rational functions are constructed as exactly those bijective mappings of the set $\mathbb{C} \cup \{\infty\}$ onto itself that permute the points 0, 1, and ∞. The mappings F_0, F_1 and F_∞ are the ones that leave 0, 1 and ∞ (respectively) **F***ixed, hence the notation. M and W are fantasy names for the other two functions. So in practice, this group of six rational functions was specifically concocted to be isomorphic to S_3. This background would of course give a much more inspired proof for the isomorphism property; the proof pursued here, in its ugliness, has no other justification than being a didactically motivated workout.*

Examples & Hwk 41:

> Continuing with the group RF of all rational functions f of the form $f(z) = (az+b)/(cz+d)$, with composition, from Ex&Hwk 8, take the mapping $P : GL_2(\mathbb{R}) \to RF$, $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto f_{abcd}$, where $f_{abcd}(z) := (az+b)/(cz+d)$. This map is a group homomorphism. Is it 1-to-1? In order to answer whether it is onto, you may need to make the statement more precise: do we mean *real* or *complex* rational functions?

Solution: The last paragraph in the solution to hwk 8, namely that the composition rule corresponds exactly to matrix multiplication, amounts exactly to the statement that P is a group homomorphism.

P is NOT one-to-one. The matrices A and kA (with k any nonzero number) are mapped to the same function. If we mean by RF the set of those rational functions $z \mapsto (az+b)/(cz+d)$ (subject to $ad-bc \neq 0$) with *real* coefficients a, b, c, d, then of course P is onto. If we allow for such functions also with complex coefficients, then P, as defined on $GL_2(\mathbb{R})$ rather than $GL_2(\mathbb{C})$, is not onto.