Math 417 Problem Set 2 Solutions

(*) 12. Find the inverse of the element $A = \begin{pmatrix} 1 & 0 & 3 \\ 0 & 5 & 1 \\ 3 & 1 & 2 \end{pmatrix}$ in $GL_3(\mathbb{Z}_7)$.

We can find the inverse either by using a formula for the entries of the inverse of the 3×3 matrix (which involves the inverse of the determinant of A, computed mod 7), or by solving the (implied) system of linear equations, in the equation $A \cdot A^{-1} = I$ (again, solved mod 7), or we can use the shorthand for esssentially solving this system of equations, via the super-augmented matrix and row reduction. (Below we take the approach of <u>adding</u> a multiple of one row to another to make an entry equal to 0 mod 7, rather than subtracting to make it 0; many different routes work.)

$$(A|I) = \left(\begin{array}{ccc|ccc} 1 & 0 & 3 & 1 & 0 & 0 \\ 0 & 5 & 1 & 0 & 1 & 0 \\ 3 & 1 & 2 & 0 & 0 & 1 \end{array}\right) \to \left(\begin{array}{ccc|ccc} 1 & 0 & 3 & 1 & 0 & 0 \\ 0 & 5 & 1 & 0 & 1 & 0 \\ 7 & 1 & 14 & 4 & 0 & 1 \end{array}\right)$$

$$= \left(\begin{array}{ccc|ccc} 1 & 0 & 3 & 1 & 0 & 0 \\ 0 & 5 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 4 & 0 & 1 \end{array}\right) \to \left(\begin{array}{ccc|ccc} 1 & 0 & 3 & 1 & 0 & 0 \\ 0 & 1 & 0 & 4 & 0 & 1 \\ 0 & 5 & 1 & 0 & 1 & 0 \end{array}\right) \to \left(\begin{array}{ccc|ccc} 1 & 0 & 3 & 1 & 0 & 0 \\ 0 & 1 & 0 & 4 & 0 & 1 \\ 0 & 7 & 1 & 8 & 1 & 2 \end{array}\right)$$

$$= \left(\begin{array}{ccc|ccc} 1 & 0 & 3 & 1 & 0 & 0 \\ 0 & 1 & 0 & 4 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 2 \end{array}\right) \to \left(\begin{array}{ccc|ccc} 1 & 0 & 7 & 5 & 4 & 8 \\ 0 & 1 & 0 & 4 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 2 \end{array}\right) = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 5 & 4 & 1 \\ 0 & 1 & 0 & 4 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 2 \end{array}\right)$$

and so $A^{-1} = \begin{pmatrix} 5 & 4 & 1 \\ 4 & 0 & 1 \\ 1 & 1 & 2 \end{pmatrix}$. And we can check this by direct computation!

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 5 & 1 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 5 & 4 & 1 \\ 4 & 0 & 1 \\ 1 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 8 & 7 & 7 \\ 21 & 1 & 7 \\ 21 & 14 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

(again, the equalities hold modulo 7).

(*) 14. (Gallian, p.57, #34) Prove that if G is a group and $a, b \in G$ then $(ab)^2 = a^2b^2$ if and only if $ab = ba$.

By definition, $(ab)^2 = (ab)(ab) = abab$ and $a^2b^2 = (aa)(bb) = aabb$. If the two are equal, $abab = aabb$, then multiplying by a^{-1} on the left yields

$bab = (a^{-1}a)bab = a^{-1}(abab) = a^{-1}(aabb) = (a^{-1}a)abb = abb.$

Then multiplying by b^{-1} on the right yields

$ba = ba(bb^{-1}) = (bab)b^{-1} = (abb)b^{-1} = (ab)(bb^{-1}) = ab,$

and so $ba = ab$, as desired. On the other hand, if we know that $ba = ab$, then

$aba = a(ba) = a(ab) = aab$, and so

$(ab)^2 = abab = (aba)b = (aab)b = (aa)(bb) = a^2b^2.$

(*) 16. (Gallian, p.69, # 4) Show that if G is a group and $a \in G$, then $|a| = |a^{-1}|$.

There are at least two ways to approach this (and probably more?). If $|a| < \infty$, then setting $n = |a|$ for notational simplicity, we know that $a^n = e$, so $(a^{-1})^n = a^{-1} \cdots a^{-1} = (a \cdots a)^{-1} = (a^n)^{-1} = e^{-1} = e$ (where this 'used' that $(ab)^{-1} = b^{-1}a^{-1}$ and induction), and so we know that $|a^{-1}| \leq n$ (by definition) or $|a^{-1}|$ divides n (from results from class), depending on your viewpoint. In particular, we have $|a^{-1}| < \infty$, as well.

But then , since $(a^{-1})^{-1} = a$ and we know that $m = |a^{-1}| < \infty$ (introducing the notation again for simplicity), the same argument above shows that $n = |a| = |(a^{-1})^{-1}| \leq m$ (or n divides m, if you take that viewpoint). So we have established that $m \leq n$ and $n \leq m$ (or $m|n$ and $n|m$, with $m, n \geq 1$), which (both) imply that $n = m$. So $m = |a^{-1}| = |a| = n$, as desired.

For completeness, we should mention that if $|a| = \infty$ then we must also have $|a^{-1}| = \infty$, since otherwise $|a^{-1}| = m < \infty$, and then our argument above implies that $|a| = |(a^{-1})^{-1}|$ must be finite as well (and $|a| \leq m$), a contradiction! So $|a^{-1}| = \infty$, and in particular $|a^{-1}| = |a|$. So whether $|a|$ is finite or infinite, we always have $|a| = |a^{-1}|$.

A selection of further solutions

10. Use the Euclidean algorithm to find the inverses of the elements 2, 3, and 7 in the group $G = (\mathbb{Z}_{137}^*, \cdot, 1)$.

$137 = 68 \cdot 2 + 1$, and so $1 = 1 \cdot 137 + (-68) \cdot 2$, so $1 \equiv_{137} (-68)(2) \equiv_{137} (69)(2)$, and so $2^{-1} = 69$ in $\mathbb{Z}_{137}$.

$137 = (45)(3)+2$, so $2 = (1)(137)+(-45)(3)$, and $3 = (1)(2)+1$, so $1 = (1)(3)+(-1)(2)$. Then $1 = (1)(3) + (-1)[(1)(137) + (-45)(3)] = (-1)(137) + (46)(3)$, so $1 \equiv_{137} (46)(3)$, and so $3^{-1} = 46$ in $\mathbb{Z}_{137}$.

$137 = (19)(7) + 4$, so $4 = (1)(137) + (-19)(7)$. Then $7 = (1)(4) + 3$, so $3 = (1)(7) + (-1)(4)$. Then $4 = (1)(3) + 1$, so $1 = (1)(4) + (-1)(3)$. Unwinding this,
$1 = (1)(4) + (-1)(3) = (1)(4) + (-1)[(1)(7) + (-1)(4)] = (-1)(7) + (2)(4)$, and so $1 = (-1)(7) + (2)(4) = (-1)(7) + (2)[(137) + (-19)(7)] = (2)(137) + (-39)(7)$. So $1 \equiv_{137} (-39)(7) \equiv_{137} (98)(7)$, and so $7^{-1} = 98$ in $\mathbb{Z}_{137}$.

[Check! $(7)(98) = 686 = (5)(137) + 1 \equiv_{137} 1$.]

13. (Gallian, p.57, #42) Suppose that $F_1 = F(\theta)$ and $F_2 = F(\psi)$ (to adopt Gallian's notation) are reflections in lines of slope θ and ψ, with $\theta \neq \psi$, and $F_1 \circ F_2 = F_2 \circ F_1$. Show that then $F_1 \circ F_2 = R(\pi)$ is rotation by angle π.

[Your results from Problem #1 might help!]

From Problem #1 we know that $F_1 \circ F_2 = F(\theta) \circ F(\psi) = R(2\theta - 2\psi)$, and (so) $F_2 \circ F_1 = F(\psi) \circ F(\theta) = R(2\psi - 2\theta)$. If these two rotations are equal, then their rotation angles must be equal, up to a multiple of 2π. (That is, their difference is a multiple of 2π.) If we interpret the question as saying that θ and ψ are between 0 and 2π and unequal, then $0 < |(2\theta - 2\psi) - (2\psi - 2\theta)| < 4\pi$, so $|(2\theta - 2\psi) - (2\psi - 2\theta)| = |4(\theta - \psi)| = 2\pi$, and $2\theta - 2\psi = \pm\pi$. So $F_1 \circ F_2 = R(\pm\pi)$ is rotation by π (which is equal to rotation by $-\pi$).

15. Give an <u>example</u> of a group G and $a, b \in G$ so that $(ab)^4 = a^4b^4$, but $ab \neq ba$.

[Hint: Problem #13 might help? Slightly bigger challenge: try the same thing with the 4's replaced by 3's !]

The cheapest way to arrange this is to (first) try making $(ab)^4 = e = a^4 = b^4$, that is, find elements a and b with order (dividing) 4 whose product ab also has order (dividing) 4, and then check to see if $ab = ba$. Problem #13 suggests a way to do this: try $a = F(\theta)$ and $b = F(\psi)$ with ab <u>not</u> equal to $R(\pi)$ (which, we can note, has order 2), but (rather) having order 4. Note that in this case $a^2 = b^2 = e = R(0)$, and so $a^4 = b^4 = e^2 = e$, and so $a^4b^4 = e = (ab)^4$. And to get what we want, we set $\theta - \psi = \pi/4$, so $ab = R(2(\pi/4)) = R(\pi/2)$, which does have order 4. Specifically, we can choose $F_1 = R(\pi/4)$ and $F_2 = R(0)$. And we can choose any group G that contains these reflections, like the symmetries of a circle, or the symmetries of a square.

Other examples can (with some experimentation!) be constructed in other non-abelian groups. For example, in $G = \mathbb{Z}_5 \times \mathbb{Z}_5^*$, with the multiplication $(a, b) * (c, d) = (a+bc, bd)$ (mod 5), we can work out that

$(a, b)^4 = [(a, b)^2]^2 = [(a, b)(a, b)]^2 = (a + ba, bb)^2 = (a + ba, bb)(a + ba, bb) = (a + ba + (bb)(a + ba), b^4) = (a(1 + b + b^2 + b^3), b^4)$. But in $\mathbb{Z}_5^*$, $1^4 = 2^4 = 3^4 = 4^4 \equiv_5 1$ (they are 1, 16, 81, and 256), and $1 + 1^1 + 1^2 + 1^3 = 4 = -1$, $1 + 2 + 2^2 + 2^3 = 15 = 0$, $1 + 3 + 3^3 + 3^3 = 40 = 0$, and $1 + 4 + 4^2 + 4^3 = 85 = 0$. So $(a, b)^4 = (0, 1) = e$ so long as $b \neq 1$.

So, for example, $(1, 2)^4 = (2, 2)^4 = (0, 1) = e$, so $(1, 2)^4(2, 2)^4 = ee = e$, while $(1, 2)(2, 2) = (1 + 2 \cdot 2, 2 \cdot 2) = (0, 4)$, so setting $a = (1, 2)$ and $b = (2, 2)$ we have $(ab)^4 = (0, 4)^4 = e = (1, 2)^4(2, 2)^4 = a^4b^4$, but $ab = (0, 4)$ and $ba = (2, 2)(1, 2) = (4, 4)$, so $ab \neq ba$.

An example involving $(ab)^3 = a^3b^3$ can be built along the same lines, the key fact above was that in $\mathbb{Z}_5^*$ every element satisfied $x^4 = 1$ (and this tended to make $1+x+x^2+x^3 = (x^4 - 1)(x - 1)^{-1}$ equal 0 (except when $x = 1$)). We can search for other $\mathbb{Z}_n^*$ where something similar happens, since in $\mathbb{Z}_n \times \mathbb{Z}_n^*$ we similarly have $(a, b)^3 = (a(1+b+b^2), b^3)$. So we would like to find elements $x = b, d$, and bd (none equal to 1) in a $\mathbb{Z}_n^*$ so that $x^3 = 1$ and (so) $1+x+x^2 = 0$. The delicate point is that we can't make this happen for <u>every</u> x in a $\mathbb{Z}_n^*$, it turns out. But on the other hand, by changing the first coordinate we can let $b = d$ (since then $(bd)^3 = (b^2)^3 = (b^3)^2 = 1^2 = 1$). So, for example, in $\mathbb{Z}_7^*$ we have $2^3 = 1$, and so $a = (1, 2)$, $b = (2, 2)$, and $ab = (1, 2)(2, 2) = (5, 4)$ all have cube equal to $(0, 1) = (0, 1)(0, 1)$, and so $(ab)^3 = a^3b^3$, but $ba = (2, 2)(1, 2) = (4, 4) \neq (5, 4) = ab$.