Practice Final Examination Mathematics 100A

Solutions

Several of the solutions to the problems have a great deal more detail than will be expected of the students in the course. It is important to make sure that the idea that you use to solve a problem is explained. Calculations that are left out should also be justified. If you remember a theorem or an exercise you have done then you can apply it (with the assertion of where the fact comes from). If the result is “bogus” however you will almost certainly suffer the consequences.

1. Let $G = \left\{ g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}_3 \text{ and } ad - bc = \mathbb{1} \right\}$.

(a) Prove that $G$ has order 24. Hint: Set $H = \left\{ g = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \mid x \in \mathbb{Z}_3 \right\}$.

Show that $\phi : G/H \rightarrow \{(x, y) \mid (x, y) \neq (0, 0)\}$ given by $\phi(gH) = (a, c)$ for $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is well defined and bijective. (Hint: Show that if $m = \begin{bmatrix} a & b' \\ c & d' \end{bmatrix}$ and $ad' - b'c = 1$ then $g^{-1}m \in H$ so $m \in gH$.)

(b) Prove that $G$ is not isomorphic with $S_4$.

Solution: (a) If $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $u = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ and $uH = gH$ then there exists $x \in \mathbb{Z}_3$ such that $\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & ax + b \\ c & cx + d \end{bmatrix}$.

Thus $a' = a, c' = c$. Hence $\phi$ is well defined. If $m = \begin{bmatrix} a & b' \\ c & d' \end{bmatrix}$ then since $g^{-1} = \begin{bmatrix} d & -b' \\ -c' & a \end{bmatrix}$ we have $g^{-1}m = \begin{bmatrix} da - bc & db' - bd' \\ -ca + ac & -cb' + ad' \end{bmatrix} = \begin{bmatrix} 1 & db' - bd' \\ 0 & 1 \end{bmatrix}$.

Since the determinants of $g$ and $m$ are both 1. This implies that the map is one to one. If $(x, y) \in \mathbb{Z}_3 \times \mathbb{Z}_3$ is not $(0, 0)$ then if $x \neq 0$ then $\begin{bmatrix} x & 0 \\ y & 1 \end{bmatrix} \in G$ if $x = 0$ then $\begin{bmatrix} y^{-1} & 0 \\ 0 & 0 \end{bmatrix} \in G$ so $\phi$ is onto. Thus $|G/H| = \left|\{(x, y) \mid (x, y) \neq (0, 0)\}\right| = 9 - 1 = 8$. $|H| = |\mathbb{Z}_3| = 3$. Thus $|G| = |G/H||H| = 3 \times 8 = 24$.

(b) If $s \in S_4$ and $st = ts$ for all $t \in S_4$ then we show that $s(i) = i$ for all $i = 1, 2, 3, 4$. If $t \in S_4$ then $s(t) = ts$ then $s(i) = st(i) = ts(i)$. Thus $t(s(i)) = s(i)$ for all $t$ such that $t(i) = i$. If $s(i) = k \neq i$ and if $j \neq i$ and $j \neq k$ then $(jk)i = i$ and $(jk)s(i) = (jk)k = j \neq k$. This is a contradiction so we must have $s(i) = i$ for all $i$. The element $u = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is in $G$ since $1 \cdot 1 = 1 = 1$. Since $ug = gu$ for all $g \in G$ the two groups cannot be isomorphic.
2. Let \( n \geq 4 \) consider the group \( H \) generated by all 4-cycles in \( S_n \). Show that \( H = S_n \). Hint: First show that \( H \) is a normal subgroup. Then show that \((1432)(1423)(1243) = (12)\).

Solution: Consider the 4-cycle \((abcd)\) then if \( t \in S_n \) then \( t(abcd)^{-1} = (uvwu) \) with \( u = t(a), v = t(b), w = t(c), x = t(d) \). Thus if \( s \) is a product of 4 cycles then \( t(s)^{-1} \) is also a product of 4 cycles. Thus \( H \) is a normal subgroup. Set \( u = (1432)(1423)(1243) \). Then \( 1 \rightarrow 2 \rightarrow 3 \rightarrow 2, 2 \rightarrow 4 \rightarrow 2 \rightarrow 1, 3 \rightarrow 1 \rightarrow 4 \rightarrow 3 \) so \( u = (12) \). If \( (ab) \) is any transposition. Let \( \{c_3, \ldots, c_n\} \) be the set \( \{i \leq i \leq n, i \neq a, b\} \) and define \( s(1) = a, s(2) = b, s(j) = c_j \) for \( i \geq 3 \). Then \( s(12)s^{-1} = (ab) \). Thus \( H \) contains all transpositions. Since every element of \( S_n \) is a product of transpositions \( \begin{cases} H \end{cases} = S_n \).

3. Which of the following sets with binary operations as given (the \( a \) operation is for the addition the \( m \) for multiplication) is a ring with the indicated 0? (You must give reasons to get full credit.)

a) \( R = \mathbb{Z} \) and \( a(x, y) = x - y \) and \( m(x, y) = xy \) with \( 0_R = 0, 1_R = 1 \).

b) \( R = \mathbb{Z} \) and \( a(x, y) = x + y + 1 \) and \( m(x, y) = xy + x + y \) with \( 0_R = -1, 1_R = 0 \).

c) \( R = \mathbb{R} \times \mathbb{R} \) and \( a((x_1, x_2), (y_1, y_2)) = (x_1 + y_1, x_2 + y_2), m((x_1, x_2), (y_1, y_2)) = (x_1 y_1 + x_2 y_2, x_1 y_2 + x_2 y_1) \) with \( 0_R = (0, 0) \) and \( 1_R = (1, 0) \).

Solution. a) We must first check whether \( \mathbb{Z} \) under subtraction is a group. We check \( a(x, a(y, z)) = x - a(y, z) = x - (y - z) = x - y + z \). On the other hand \( a(a(x, y), z) = a(x, y + z) = x - (y + z) \). Thus if \( z \neq 0 \) we have \( a(x, a(y, z)) \neq a(a(x, y), z) \) so \( \mathbb{Z} \) is not a group with respect to the binary operation \( a \). So the system in a) is NOT a ring.

b) We first check that with the operation \( a, \mathbb{Z} \) is a group.

\[
a((x, y), z) = x + a(y, z) + 1 = x + (y + z + 1) + 1 = x + y + z + 2.
\]

\[
a(a(x, y), z) = a(x, y) + z + 1 = (x + y + 1) + z + 1 = x + y + z + 2.
\]

Thus the operation \( a \) is associative. Also \( a(-1, x) = -1 + x + 1 = x, a(x, -1) = x + -1 + 1 = x \) so \(-1 \) is an identity for \( a \). If \( x \in \mathbb{Z} \) consider \( a(x, -x - 2) = x + (-x - 2) + 1 = -1 \). So if \( y = -x - 2 \) then \( a(x, y) = -1 \) the identity for \( a \). Since \( a(x, y) = x + y + 1 \) the group with operation \( a \) is abelian. We now look at \( m \). \( m(m(x, y), z) = m(x, y)z + m(x, y) + z = (xy + x + y)z + (xy + x + y) + z = xyz + xz + yz + xy + x + y + z \) and \( m(x, m(y, z)) = xym(y, z) + x + m(y, z) = x(yz + y + z) + x + y + z + z = xyz + xy + xz + yz + x + y + z \). So the associative rule for \( m \) is satisfied. We note that \( m(x, y) = m(y, x) \) so we need only check one of the distributive rules we have \( m(x, a(y, z)) = xa(y, z) + x + a(y, z) = x(y + z + 1) + x + y + z + 1 = xy + xz + 2x + y + z + 1 \). Also, \( a(m(x, y), m(x, z)) = m(x, y) + m(x, z) + 1 = (xy + x + y) + (xz + x + z) + 1 = xy + xz + 2x + y + z + 1 \). As for the multiplicative identity we note that \( n(0, y) = y \) and \( n(x, 0) = x \). So it IS a ring.

c) We have seen that \( \mathbb{R} \times \mathbb{R} \) is an abelian group under the operation \( a \) in this case. We check that \( m \) is associative.

\[
m(x_1, x_2, m(y_1, y_2), (z_1, z_2)) = m(m(x_1, x_2), (y_1, y_2), (z_1, z_2))
\]
On the other hand we have

\[ m(m((x_1, x_2), (y_1, y_2)), (z_1, z_2)) = m((x_1y_1 + x_2y_2, x_1y_2 + x_2y_1), (z_1, z_2)) \]

\[ = ((x_1y_1 + x_2y_2)z_1 + (x_1y_2 + x_2y_1)z_2, (x_1y_1 + x_2y_2)z_2 + (x_1y_2 + x_2y_1)z_1) \]

\[ = (x_1y_1z_1 + x_1y_2z_2 + x_2y_1z_1 + x_2y_2z_2, x_1y_1z_2 + x_1y_2z_1 + x_2y_1z_2 + x_2y_2z_1). \]

Thus \( m \) is associative. We note that \( m((x_1, x_2), (y_1, y_2)) = m((y_1, y_2), (x_1, x_2)). \)

So we need only check one distributive rule.

\[ m((x_1, x_2), a((y_1, y_2), (z_1, z_2))) = m((x_1, x_2), (y_1 + z_1, y_2 + z_2)) = \]

\[ (x_1(y_1 + z_1) + x_2(y_2 + z_2), x_1(y_2 + z_2) + x_2(y_1 + z_1)) = \]

\[ (x_1y_1 + x_1z_1 + x_2y_2 + x_2z_2, x_1y_2 + x_1z_2 + x_2y_1 + x_2z_1). \]

We have

\[ a(m((x_1, x_2), (y_1, y_2)), m((x_1, x_2), (z_1, z_2)) = \]

\[ a((x_1y_1 + x_2y_2, x_1y_2 + x_2y_1), (x_1z_1 + x_2z_2, x_1z_2 + x_2z_1) \]

\[ = (x_1y_1 + x_2y_2 + x_1z_1 + x_2z_2, x_1y_2 + x_2y_1 + x_1z_2 + x_2z_1). \]

So the distributive rule is satisfied. Finally, \( m((1, 0), (x, y)) = (x, y), m((x, y), (1, 0)) = (x, y) \). This IS a ring.

4. Let \( G \) be a commutative group and let \( H \) denote the set of elements of finite order in \( G \).

a) Show that \( H \) is a subgroup of \( G \).

b) Consider the matrices \( A = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}, B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \) in the group \( GL(2, \mathbb{R}) \) calculate the orders of \( A \) and \( B \) and deduce that the elements are of finite order. Show that \( AB \) does not have finite order. Why doesn’t this contradict part a)?

Solution: a) We must show that if \( a, b \in H \) then \( a^{-1} \) and \( ab \) are in \( H \). If \( a^n = e \) then multiplying both sides of the equation by \( a^{-n} \) we see that \( e = a^{-n} \). So \( a^{-1} \in H \). If \( a^n = e \) and \( b^m = e \) then \( (ab)^{nm} = a^{nm}b^{mn} = (a^n)(b^m)^n = e^ne^n = e \) so \( ab \in H \). Thus \( H \) is a subgroup.

b) \( A^2 = \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix}, A^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \) so \( A \) has order 3. \( B^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \) so \( B \) has order 2. \( AB = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = C \). So \( C^2 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, C^3 = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \).

We note that if \( C^k = \begin{bmatrix} a_k & b_k \\ c_k & d_k \end{bmatrix} \) then \( a_{k+1} = c_k \) and \( c_{k+1} = a_k + c_k \). This implies that \( c_{k+2} = a_{k+1} + c_{k+1} = c_k + c_{k+1} \). In other words the numbers \( c_k \) are defined by \( c_1 = 1, c_2 = 1 \) and \( c_{n+2} = c_n + c_{n+1} \). In particular we see that
if \( n \geq 2 \), \( c_{n+1} > c_n \) so \( C \) has infinite order. (The sequence \( c_k \) is usually called the Fibonacci sequence. This sequence has remarkable properties.) This is no contradiction since the group of of \( 2 \times 2 \) invertible matrices over \( \mathbb{R} \) is not abelian.

5. Assume that \( G \) is a group whose order is 10 show that \( G \) is isomorphic to either \( \mathbb{Z}_{10} \) or \( D_5 \) (the dihedral group with 10 elements).

Solution: If \( a \in G \) and \( a \) is not the identity then since the order of \( a \) must be a divisor of 10 the order of \( a \) is 2, 5 or 10. If the order of \( a \) is 10 for some \( a \in G \) then \( G \) is cyclic of order 10. We must therefore show that if every element of \( G \) has order 1, 2 or 5 then \( G \) is isomorphic with \( D_5 \). If every element other than the identity has order 2 then we have seen that \( G \) must be abelian. Under this assumption if \( a \in G \) and \( a \neq e \) then \( H = \{e, a\} \) is a subgroup of order 2. Thus \( G/H \) is a group of order 5 hence cyclic. This implies that if \( x \notin H \) then \( x^5 \in H \) which implies \( x \) has order 5 (since it can’t have order 10). Thus there must be an element of order 5 we denote in \( c \). Set \( H = \langle c \rangle \). Let \( d \in G \) be such that \( d \notin H \). If \( d \) also has order 5 we will derive a contradiction. We note that \( d^k \notin H \) for \( k = 1, 2, 3, 4 \). This can be seen as follows if \( d^k = c^r \) for \( 1 \leq k \leq l \) then \( d^k \) is also of order 5 hence there exists \( r \) such that \( (d^k)^r = d \). So \( d = (c^r)^r \in H \). Hence \( \langle c \rangle \cup \langle d \rangle \) consists of 9 elements. There must be another element \( x \notin \langle c \rangle \cup \langle d \rangle \). The order of \( x \) must be 2 or 5. If it is 5 we have \( x^5 \notin \langle c \rangle \cup \langle d \rangle \) for \( k = 1, 2, 3, 4 \) by the argument we have just used. This is not possible since \( G \) has order 10. Thus \( x \) must have order 2. Now \( cd \) cannot be a power of \( d \) since then \( c \) would be equal to a power of \( d \) and it can’t be a power of \( c \) for the same reason. Thus \( cd = x \) (the only other element). Similarly, \( d^{-1}c = x \). Thus \( cdd^{-1}c = x^2 \) so \( c^2 = e \). This is the desired contradiction. We conclude that if \( d \notin H \) then \( d^2 = e \). Fix \( d \notin H \). Then \( dc \notin H \) so \( dcdc = e \). Thus \( dcd = c^{-1} \). Which shows that \( G \) is isomorphic with \( D_5 \).

6. Let \( G \) be a group and let \( H \) be a cyclic subgroup of \( G \) that is normal in \( G \) show that every subgroup of \( H \) is normal in \( G \).

Solution: Let \( H = \langle c \rangle \) with \( c \in G \). Since \( H \) is normal in \( G \) we see that if for the moment we fix \( x \in G \) then \( xcxc^{-1} = c^k \) for some \( k \) depending on \( x \). If \( U \) is a subgroup of \( H \) then \( U = \langle c^l \rangle \) for some \( l \) since we have proved that a subgroup of a cyclic group is cyclic. Now \( x^dxc^{-1} = (xcx^{-1})^l = (c^k)^l = (c^l)^k \). Thus \( x^dxc^{-1} \subset U \). Since \( x \) was arbitrarily chosen in \( G \), \( U \) is normal in \( G \).

7. Let \( R \) be a commutative ring and \( S \) be the set of \( 2 \times 2 \) matrices with entries in \( R \) under matrix multiplication. Show that \( S \) is a ring. Show that

\[
S^* = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in R \text{ and } ad - bc \in R^* \right\}.
\]

Solution. We have shown that \( S \) is a ring even if \( R \) is not commutative. If \( ad - bc \in R^* \) then let \( \alpha = (ad - bc)^{-1} \). Then (imitating Cramer’s rule) we have

\[
\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \frac{d}{\alpha} & \frac{-b}{\alpha} \\ \frac{c}{\alpha} & \frac{-d}{\alpha} \end{bmatrix} = \begin{bmatrix} \frac{ad}{\alpha} + \frac{-bd}{\alpha} & \frac{ac}{\alpha} + \frac{-bd}{\alpha} \\ \frac{ac}{\alpha} + \frac{-cd}{\alpha} & \frac{ad}{\alpha} + \frac{-cd}{\alpha} \end{bmatrix} =
\]

4
We now show that if \[
\begin{pmatrix}
\frac{ad-bc}{a} & 0 \\
0 & \frac{-bc+ad}{a}
\end{pmatrix}
\in S^* \text{ then } ad-bc \in R^*. \]
We set \( \det \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = ad-bc. \) 

Then exists a homomorphism of \( a, b \) again. If \( G \) for \( \alpha \in x \) then there exists an onto group homomorphism from \( \eta \) onto \( G \) such that \( \eta(g) = \phi(gH) \) is an onto homomorphism of \( G \) to \( C_2 \). Write \( C_2 = \{e, a\} \). Let \( \eta \) be an onto homomorphisms of \( G \) to \( C_2 \) and let \( U \) be the kernel of \( \eta \). If \( x \in G \) is such that \( \eta(x) = a \) then show that the map \( \alpha : C_2 \times U \to G \) given by \( \alpha(e, u) = u \) and \( \alpha(a, u) = xu \) defines a group homomorphism.

Solution. a) This has been shown several times but we will give the argument again. If \( a, b \in G \) then \( ab = (ab)^{-1} = b^{-1}a^{-1} = ba. \)

b) We prove this by induction on \( |G| \). If \( |G| \leq 1 \) then \( 1 = 2^0 \) so true. Assume for \( 1 \leq |G| \leq m \) we now prove that it is true for \( |G| \leq m+1. \) Let \( a \neq e \) be in \( G \). Then \( H = \{e, a\} \) is a subgroup. Since \( G \) is abelian we see that \( G/H \) is a group and every element \( x \) of \( G/H \) satisfies \( x^2 = e. \) \( |G/H| = |G|/2 < |G| \).

Hence the inductive hypothesis says that \( |G/H| = 2^n \) for some \( n \) and thus we must have \( |G| = 2^n+1. \)

c) Let \( G \) order \( 2^n. \) We prove by induction on \( n \) that if \( n \geq 1 \) then there exists a homomorphism of \( G \) onto \( C_2. \) If \( n = 1 \) then \( G \) is cyclic of order \( 2 \) hence isomorphic with \( C_2. \) Assume for \( 1 \leq n \leq k \) if \( n = k + 1 \) let \( a \in G \) with

\[
\begin{pmatrix}
\frac{ad-bc}{a} & 0 \\
0 & \frac{-bc+ad}{a}\end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}.
\]
\( a \neq e \). Then \( H = \{ e, a \} \) is a normal subgroup of \( G \). \( G/H \) has order \( 2^k \) so there exists \( \phi : G/H \to C_2 \) an onto homomorphism. Let \( p : G \to G/H \) be defined by \( p(g) = gH \). Then \( p \) is a group homomorphism that is onto. Hence if we put \( \eta(g) = \phi(p(g)) \) then \( \eta \) is an onto homomorphism of \( G \) to \( C_2 \). This completes the induction.

We therefore know that there exists a homomorphism of \( G \) onto \( C_2 \) if \( |G| = 2^n \) and \( n \geq 1 \). We will now prove the assertion in c) by induction on \( n \). If \( n = 1 \) then \( G \) is isomorphic with \( C_2 \) (we have already observed and used this fact). Assume for \( 1 \leq n \leq k \). If \( n = k+1 \) then let \( \eta : G \to C_2 \) be a homomorphism of \( G \) onto \( C_2 \). We write \( C_2 = \{ e, a \} \). Let \( U = \ker \eta \). Then the isomorphism theorem implies \( |G/U| = 2 \) so \( |U| = 2^k \). Choose \( x \in G \) so that \( \eta(x) = a \). Define \( \alpha : C_2 \times U \to G \) by \( \alpha(e,u) = u \) and \( \alpha(a,u) = xu \). Then \( \alpha \) is a group homomorphism. Indeed, \( \alpha((e,u)(e,w)) = \alpha((e,uw)) = uw = \alpha(e,u)\alpha(e,w) \). \( \alpha((a,u)(e,w)) = \alpha(a,uw) = xuw = \alpha(e,u)\alpha(a,w) \). Finally, \( \alpha((a,u),(a,w)) = \alpha(e,uw) = uw = xxuw = xuxw = \alpha(a,u)\alpha(a,w) \). So \( \alpha \) is a group homomorphism. If \( \alpha(y,u) = \alpha(z,w) \) then \( y = \eta(\alpha(y,u)) = \eta(\alpha(z,w)) = z \). Hence \( y = z \). Since \( \alpha(y,e)\alpha(y,u) = u \) and \( \alpha(z,e)\alpha(z,w) = w \) we see that \( u = w \). Thus \( \alpha \) is one to one. Since \( |C_2 \times U| = 2 \times 2^k = |G| \), \( \alpha \) is onto. Hence \( G \) is isomorphic with \( C_2 \times U \).

The inductive hypothesis implies that \( U \) is isomorphic with \( C_2 \times C_2 \times \cdots \times C_2 \) (\( k \)-copies). Thus \( G \) is isomorphic with \( C_2 \times C_2 \times \cdots \times C_2 \) (\( k+1 \)-copies).