Math 151

Practice problems for Test 2

Solutions

1. (Note: feel free to show me your examples to make sure they are correct.)

group	order	abelian?	cyclic?
$\mathbb{Z}_5^*$	4	yes	yes
$\mathbb{Z}_6$	6	yes	yes
S_3	6	no	no
$\mathbb{Z}_4 \times \mathbb{Z}_2$	8	yes	no
$\mathbb{Z}$	∞	yes	yes
$GL_2(\mathbb{R})$	∞	no	no
$\{e\}$=trivial	1	yes	yes
D_5	10	no	no
$Mat_{2\times 3}(\mathbb{Z}_2)$	64	yes	no
$\mathbb{R}$	∞	yes	no

$\mathbb{Z}_5^*$ consists of all invertible elements in $\mathbb{Z}_5$, and it is a group under multiplication. $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$, so $|\mathbb{Z}_5^*| = 4$. It is abelian since multiplication of numbers is commutative. It is cyclic because it is generated by 2: $< 2 >= \{1, 2, 4, 3\} = \mathbb{Z}_5^*$.

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} =< 1 >$ is an abelian cyclic group (under addition) of order 6. (In general, $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\} =< 1 >$ is an abelian cyclic group of order n.)

$S_3 = \{(1), (12), (13), (23), (123), (132)\}$ has order 6. It is not abelian because e.g. $(12)(13) = (132)$ and $(13)(12) = (123)$. (In general, S_n, the permutation group on a set of n elements, it has order $n!$ and is non-abelian if $n > 2$.) It is not cyclic if $n > 2$ because every cyclic group is abelian and this one is not.

$\mathbb{Z}_4 \times \mathbb{Z}_2 = \{(x, y) \mid x \in \mathbb{Z}_4,\ y \in \mathbb{Z}_2\}$ is the set of all pairs, and it has order $4 \cdot 2 = 8$. It is abelian since both $\mathbb{Z}_4$ and $\mathbb{Z}_2$ are. It is not cyclic because it has no element of order 8: it is easy to check that the order of each element is ≤ 4.

$\mathbb{Z}$ is an infinite cyclic group consisting of all integer numbers (with addition). It is abelian since addition of numbers is abelian. It is cyclic because it is generated by 1.

$GL_2(\mathbb{R})$ is the group of 2×2 invertible matrices with real entries under multiplication. There are infinitely many such matrices, so its order is infinity. It is not abelian because e.g. $\begin{bmatrix} 0 & 2 \\ 3 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 2 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$. It is not cyclic because every cyclic group is abelian.

$\{e\}$=trivial group has only one element. It is abelian (all elements commute), and cyclic (generated by e). It is a very uninteresting group, but I just wanted to give an example of a group of order 1.

D_5, dihedral group of order $2 \cdot 5 = 10$, is the group of rigid motions of a regular pentagon. Its elements are $e, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b$. It is not abelian (e.g. $ba = a^4b \neq ab$), and hence not cyclic.

$Mat_{2\times 3}(\mathbb{Z}_2)$ is the group of all 2×3 matrices with entries in $\mathbb{Z}_2$ under addition. Its order is 64: each entry can be either 0 or 1, and there are 6 entries, so there are $2^6 = 64$ such matrices. It is abelian since addition in $\mathbb{Z}_2$ is commutative. But it is not cyclic: each non-zero element has order 2 because if you add an entry of a matrix to itself you'll get 0, thus any matrix added to itself gives the zero matrix. Therefore there is no element (matrix) of order 64.

$\mathbb{R}$ is an infinite group of real numbers under addition. It is abelian (addition of numbers is commutative) but not cyclic: every nonzero element generates a cyclic subgroup consisting of its own multiples, thus every cyclic subgroup has a smallest positive element. But $\mathbb{R}$ does not have any.

2. (a) Let $S = \{A \in GL_2(\mathbb{R}) \mid \det(A) > 0\}$. First, S is closed under multiplication since if $A, B \in S$, then $\det(A) > 0$ and $\det(B) > 0$, and then $\det(AB) = \det(A)\det(B) > 0$, so $AB \in S$. Second, S contains the identity matrix, since $\det(I_2) = 1 > 0$. Finally, S is closed under the inverses since if $A \in S$, then $\det(A) > 0$, and then $\det(A^{-1}) = (\det(A))^{-1} > 0$, so $A^{-1} \in S$. Thus the set S is a subgoup.

   (b) The set is not a subgroup because it does not contain the identity matrix, since $\det(I_2) = 1$.

   (c) The set is not a subgroup because it is not closed under the inverses, e.g. for $A = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$, $\det(A) = 4 \in \mathbb{Z}$, so A is in the set, but $A^{-1} = \begin{bmatrix} 0.5 & 0 \\ 0 & 0.5 \end{bmatrix}$ has $\det(A^{-1}) = 0.25 \notin \mathbb{Z}$, so A^{-1} is not in the set.

3. First notice that $\mathbb{R}$, $\mathbb{R}^*$, $\mathbb{R}^+$, and $GL_2(\mathbb{R})$ have infinite order, while $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_8$, $\mathbb{Z}_8 \times \mathbb{Z}_2$, and $\mathbb{Z}_{16}$ have order 16. So we only have to check the first 4 groups, and the last 4 groups, separately.

   Among the first 4 groups, $\mathbb{R}$ and $\mathbb{R}^+$ are isomorphic: let $f : \mathbb{R} \to \mathbb{R}^+$ be defined by $f(x) = e^x$. Then $f(x+y) = e^{x+y} = e^x e^y = f(x)f(y)$. f is one-to-one because if $f(x) = f(y)$ then $e^x = e^y$, then $\ln e^x = \ln e^y$ which implies $x = y$. Finally, f is onto because for any positive real z, let $x = \ln z$, then $f(x) = f(\ln z) = e^{\ln z} = z$. (See example 3.4.2 on p.136.)

   Groups $\mathbb{R}$ and $\mathbb{R}^*$ are not isomorphic because the first group has no element of order 2, and the second group has an element of order 2, namely $-1 : (-1)^2 = 1$. $\mathbb{R}^+$ and $\mathbb{R}^*$ are not isomorphic for the same reason. (See example 3.4.4 on p.137.)

   Finally, $GL_2(\mathbb{R})$ is not isomophic to any of the above because $GL_2(\mathbb{R})$ has an element of order 4 (e.g. see exercise 1(b) on page 119), but the other groups do not.

   Among the last 4 groups, $\mathbb{Z}_2 \times \mathbb{Z}_8$ and $\mathbb{Z}_8 \times \mathbb{Z}_2$ are isomorphic: define $f : \mathbb{Z}_2 \times \mathbb{Z}_8 \to \mathbb{Z}_8 \times \mathbb{Z}_2$ by $f((x,y)) = (y,x)$. Obviously this is a 1-1 correspondence, and it is a homomorphism because $f((x,y)+(z,w)) = f((x+z, y+w)) = (y+w, x+z) = (y,x)+(w,z) = f((x,y)) + f((z,w))$.

   All other pairs are not isomorphic: $\mathbb{Z}_4 \times \mathbb{Z}_4$ only has elements of order ≤ 4; $\mathbb{Z}_2 \times \mathbb{Z}_8$ and $\mathbb{Z}_8 \times \mathbb{Z}_2$ have elements of order 8 but no elements of order 16; $\mathbb{Z}_{16}$ has elements of order 16.

4. Let's denote this subset of G by H. We want to show that H is a subgroup.

   Closed under multiplication: if $a, b \in H$, then $a^2 = b^2 = e$. Then $(ab)^2 = a^2 b^2 = e \cdot e = e$, so $ab \in H$.
   Identity: $o(e) = 1 \leq 2$, so $e \in H$.
   Closed under inverses: if $a \in H$, then $a^2 = e$. Then $(a^{-1})^2 = (a^2)^{-1} = e^{-1} = e$, so $a^{-1} \in H$.

5. Let's denote the given matrix by A. We have to compute powers of A until we get the identity matrix. The smallest positive k such that $A^k = I$ is then the order of A, and the cyclic subgroup generated by A is $\{I, A, A^2, \ldots, A^{k-1}\}$. Notice that entries of our matrices are elements of $\mathbb{Z}_3$, so each time we multiply matrices, we have to reduce each entry of the product modulo 3. Then
   $< \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} >= \left\{ I_2, \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix} \right\}$.
   Therefore the order of A is 6.

6. (a) Generators of $\mathbb{Z}_{24}$ are numbers (more precisely, classes of numbers) between 0 and 24 that are relatively prime to 24. There are 8 of them: 1, 5, 7, 11, 13, 17, 19, 23.

(b) $H = \{0, 6, 12, 18\}$ is a cyclic subgroup. Generators: 6 and 18. 0 and 12 are not generators because the order of 0 is 1, and the order of 12 is 2.
$K = \{0, 4, 8, 12, 16, 20\}$ is a cyclic subgroup. Generators: 4 and 20.
$H \cap K = \{0, 12\}$ is a cyclic subgroup. Generator: 12.
$H \cup K = \{0, 4, 6, 8, 12, 16, 18, 20\}$ is not a subgroup: it is not closed under addition, e.g., $4 + 6 = 10 \notin H \cup K$.
$H + K = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\}$ is a cyclic subgroup. Generators: 2, 10, 14, 22.

7. (a) $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 3x$ is a homomorphism: $f(x + y) = 3(x + y) = 3x + 3y = f(x) + f(y)$. $\mathrm{Ker}(f) = \{0\}$. Image $= 3\mathbb{Z}$, the set of all multiples of 3. It is one-to-one because $3x = 3y$ implies $x = y$. It is not onto because e.g. 1 is not in the image. It is not an isomorphism because it is not onto.

(b) $f : \mathbb{Z} \to \mathbb{Z}_4$, $f(x) = [x]_4$ is a homomorphism: $f(x + y) = [x + y]_4 = [x]_4 + [y]_4 = f(x) + f(y)$. $\mathrm{Ker}(f) = 4\mathbb{Z}$, the set of all multiples of 4. Image $= \mathbb{Z}_4$. It is not one-to-one because e.g. $f(0) = [0]_4$ and $f(4) = [4]_4 = [0]_4$. It is onto: every element of $\mathbb{Z}_4$ is in the image since $[x]_4 = f(x)$. It is not an isomorphism because it is not one-to-one.

(c) $f : \mathbb{Z} \to \mathbb{Z}_6$, $f(x) = [2x]_6$ is a homomorphism: $f(x + y) = [2(x + y)]_6 = [2x + 2y]_6 = [2x]_6 + [2y]_6 = f(x) + f(y)$. $\mathrm{Ker}(f) = 3\mathbb{Z}$, the set of all multiples of 3. Image $= 2\mathbb{Z}_6 = \{0, 2, 4\}$. It is not one-to-one because e.g. $f(0) = [0]_6$ and $f(3) = [6]_6 = [0]_6$. It is not onto because e.g. $[1]_6$ is not in the image. It is not an isomorphism e.g. because it is not one-to-one.

(d) $f : \mathbb{Z}_2 \to \mathbb{Z}$, $f([x]_2) = x$ is not a homomorphism because it is not a well-defined function: $[0]_2 = [2]_2$, but $f([0]_2) = 0$, $f([2]_2) = 2$, and $0 \neq 2$.

(e) $f : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$, $f([x]_{10}) = [3x]_{10}$ is a homomorphism. First, we will show that this function is well-defined: if $[x]_{10} = [y]_{10}$, then $f([x]_{10}) = [3x]_{10} = [3y]_{10} = f([y]_{10})$. It preserves the operation since $f([x]_{10} + [y]_{10}) = f([x + y]_{10}) = [3x + 3y]_{10} = [3x]_{10} + [3y]_{10} = f([x]_{10}) + f([y]_{10})$. It is one-to-one: if $f([x]_{10}) = f([y]_{10})$, then $[3x]_{10} = [3y]_{10}$. Multiplying both sides by 7, we get $[21x]_{10} = [21y]_{10}$. Since $[21]_{10} = [1]_{10}$, we have $[x]_{10} = [y]_{10}$. It is onto since for any $[y]_{10}$, $f([7y]_{10}) = [21y]_{10} = [y]_{10}$. It is an isomorphism since it is a bijection and preserves the operation.

(f) $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $f((x, y)) = x + y$ is a homomorphism. The kernel consists of all pairs (x, y) for which $x + y = 0$, or $y = -x$. Therefore $\mathrm{Ker}(f) = \{(x, -x)\}$. Image $= \mathbb{R}$: given $z \in \mathbb{R}$, $z = f((z, 0))$ is in the image. It is not one-to-one because e.g. $f((1, 0)) = 1$ and $f((2, 1)) = 1$. It is onto as shown above.It is not an isomorphism because it is not one-to-one.

(g) $f : \mathbb{R}^* \times \mathbb{R}^* \to GL_2(\mathbb{R})$, $f((x, y)) = \begin{bmatrix} 2x - y & y - x \\ 2x - 2y & 2y - x \end{bmatrix}$ is a homomorphism:

$$f((x, y))f((z, w)) = \begin{bmatrix} 2x - y & y - x \\ 2x - 2y & 2y - x \end{bmatrix} \begin{bmatrix} 2z - w & w - z \\ 2z - 2w & 2w - z \end{bmatrix}$$
$$= \begin{bmatrix} (2x - y)(2z - w) + (y - x)(2z - 2w) & (2x - y)(w - z) + (y - x)(2w - z) \\ (2x - 2y)(2z - w) + (2y - x)(2z - 2w) & (2x - 2y)(w - z) + (2y - x)(2w - z) \end{bmatrix}$$
$$= \begin{bmatrix} 2xz - yw & yw - xz \\ 2xz - 2yw & 2yw - xz \end{bmatrix} = f((xz, yw)) = f((x, y)(z, w)).$$

The kernel of f consists of all pairs for which $2x - y = 2y - x = 1$ and $2x - 2y = y - x = 0$. Solving this system gives $x = y = 1$.

The image of f consists of all matrices of the form $\begin{bmatrix} 2x - y & y - x \\ 2x - 2y & 2y - x \end{bmatrix}$. It is OK to leave this matrix as is. However, I decided to give a slightly more explicit desctiption: let $a = 2x - y$ and $b = y - x$, then the other two entries can be expressed in terms of a and b, and Image $= \left\{ \begin{bmatrix} a & b \\ -2b & a + 3b \end{bmatrix} \mid \text{this matrix must be invertible: } a^2 + 3ab + 4b \neq 0 \right\}$.

f is one-to-one since the kernel is trivial, and it is not onto because e.g. $\begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$ is not in the image. It is not an isomorphism because it is not onto.