

Homework #8

Nikhil Unni

1. Determine the isomorphism type of the factor group $\mathbb{Z}_8 \times \mathbb{Z}_6 \times \mathbb{Z}_4 / \langle 2, 2, 2 \rangle$ and give two proofs – one using elementary analysis of the orders of elements, and one using the First Isomorphism Theorem.

The factor group has 16 elements, since the original group has 192 elements, and the subgroup has 12. So our candidates for the isomorphism type are types from \mathbb{Z}_{16} . I exhaustively generated all the 16 elements of the factor group and their respective order with Python:

```
{(2, 2, 2), (2, 0, 2), (0, 4, 0), (4, 0, 0), (6, 0, 2), (4, 4, 0), (0, 2, 0), (2, 4, 2), (0, 0, 0), (6, 2, 2), (6, 4, 2), (4, 2, 0)} : 1
{(4, 0, 1), (2, 0, 3), (2, 4, 3), (0, 0, 1), (6, 2, 3), (0, 4, 1), (6, 4, 3), (4, 2, 1), (6, 0, 3), (4, 4, 1), (2, 2, 3), (0, 2, 1)} : 4
{(2, 4, 0), (6, 2, 0), (2, 0, 0), (0, 4, 2), (6, 4, 0), (0, 2, 2), (6, 0, 0), (4, 2, 2), (4, 0, 2), (2, 2, 0), (4, 4, 2), (0, 0, 2)} : 2
{(2, 0, 1), (6, 4, 1), (2, 2, 1), (4, 2, 3), (6, 0, 1), (0, 2, 3), (4, 0, 3), (4, 4, 3), (2, 4, 1), (6, 2, 1), (0, 4, 3), (0, 0, 3)} : 4
{(2, 3, 2), (0, 5, 0), (6, 5, 2), (0, 3, 0), (6, 1, 2), (4, 1, 0), (4, 5, 0), (2, 1, 2), (6, 3, 2), (2, 5, 2), (4, 3, 0), (0, 1, 0)} : 2
{(2, 5, 3), (4, 3, 1), (0, 1, 1), (2, 3, 3), (0, 5, 1), (6, 5, 3), (0, 3, 1), (6, 1, 3), (4, 1, 1), (4, 5, 1), (2, 1, 3), (6, 3, 3)} : 4
{(4, 5, 2), (2, 1, 0), (2, 5, 0), (6, 3, 0), (4, 3, 2), (0, 1, 2), (6, 5, 0), (2, 3, 0), (6, 1, 0), (0, 5, 2), (0, 3, 2), (4, 1, 2)} : 2
{(0, 3, 3), (4, 1, 3), (0, 1, 3), (4, 5, 3), (2, 1, 1), (0, 5, 3), (2, 5, 1), (6, 3, 1), (4, 3, 3), (6, 5, 1), (2, 3, 1), (6, 1, 1)} : 4
{(3, 0, 2), (5, 4, 0), (1, 4, 0), (7, 2, 2), (1, 0, 0), (3, 4, 2), (5, 2, 0), (3, 2, 2), (7, 0, 2), (7, 4, 2), (1, 2, 0), (5, 0, 0)} : 4
{(1, 2, 1), (5, 0, 1), (5, 4, 1), (1, 4, 1), (3, 0, 3), (7, 2, 3), (1, 0, 1), (3, 4, 3), (5, 2, 1), (3, 2, 3), (7, 0, 3), (7, 4, 3)} : 2
{(3, 2, 0), (7, 0, 0), (1, 2, 2), (7, 4, 0), (5, 4, 2), (5, 0, 2), (3, 0, 0), (7, 2, 0), (3, 4, 0), (1, 4, 2), (1, 0, 2), (5, 2, 2)} : 4
{(1, 0, 3), (5, 2, 3), (3, 2, 1), (7, 0, 1), (1, 2, 3), (7, 4, 1), (5, 0, 3), (3, 0, 1), (5, 4, 3), (7, 2, 1), (1, 4, 3), (3, 4, 1)} : 2
{(1, 1, 0), (3, 3, 2), (5, 3, 0), (1, 5, 0), (7, 1, 2), (1, 3, 0), (7, 5, 2), (3, 5, 2), (5, 5, 0), (7, 3, 2), (3, 1, 2), (5, 1, 0)} : 4
{(3, 3, 3), (5, 3, 1), (1, 5, 1), (7, 1, 3), (1, 3, 1), (3, 5, 3), (7, 5, 3), (5, 5, 1), (7, 3, 3), (5, 1, 1), (3, 1, 3), (1, 1, 1)} : 2
{(7, 5, 0), (1, 3, 2), (5, 5, 2), (3, 1, 0), (7, 3, 0), (3, 5, 0), (5, 1, 2), (5, 3, 2), (3, 3, 0), (1, 1, 2), (1, 5, 2), (7, 1, 0)} : 4
{(5, 5, 3), (3, 5, 1), (3, 1, 1), (7, 3, 1), (1, 1, 3), (5, 1, 3), (5, 3, 3), (3, 3, 1), (7, 1, 1), (1, 5, 3), (7, 5, 1), (1, 3, 3)} : 2
```

So we know we can eliminate \mathbb{Z}_{16} because it has an order 16 element, $\mathbb{Z}_8 \times \mathbb{Z}_2$ because it has an order 8 element, $\mathbb{Z}_4 \times \mathbb{Z}_4$ because it doesn't have enough order 2 elements, and $(\mathbb{Z}_2)^4$ because it doesn't have any order

4 elements. So we know it must be $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

We can prove the isomorphism with the First Isomorphism Theorem. We know that our subgroup is Normal, because it is the subgroup of an abelian group. Let $\phi : \mathbb{Z}_8 \times \mathbb{Z}_6 \times \mathbb{Z}_4 \rightarrow \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ such that $(a, b, c) \mapsto (a - c(\text{mod } 4), b(\text{mod } 2), c(\text{mod } 2))$. It's a valid homomorphism because modulo arithmetic yields the same value if you apply the modulo before or after the arithmetic. So by the First Isomorphism Theorem, because the kernel of ϕ is our identity, H in the quotient group, the quotient group is isomorphic to our isomorphism type.

2. Let $R = M_n(\mathbb{R})$ denote the ring of $n \times n$ matrices with real entries. Determine (with proof) whether each of the following is a subring of R .

For the following problems, I'm going to just have a checklist of things to prove S is a subring of R :

- The additive identities are the same ($0_r = 0_s$)
- Closed under additive addition/inverses ($a - b \in S$)
- Closed under multiplication (associativity will come for "free") ($ab \in S$)
- Has multiplicative identity (1_s)

The first two bullets ensure that the subring is a valid group, which we've already proved. The bottom two ensure that it's a valid subring (of unity). S is only a subring iff the third bullet is true, just by the definition of a subring, and we want only subrings of unity, and this is only true iff the fourth bullet is true.

(a) $T = \{A \in R : \text{trace}(A) \in \mathbb{Q}\}$

- Let the additive identity of trace be the zero matrix 0_N , which is just $n \times n$ zeroes. Then, for any element $t \in T$, $\text{trace}(t + 0_N) = \text{trace}(t)$, since the addition of the zeroes to the diagonal of the matrix does not change the sum of the diagonals. ($m + 0n = m$). And since t was a valid member of T , $m \in \mathbb{Q}$.
- For some $a, b \in T$, we can show that $a - b \in T$. $\text{trace}(a - b)$ can be calculated by just subtracting the traces of a and b . This becomes : $\text{trace}(a - b) = \text{trace}(a) - \text{trace}(b)$, and since \mathbb{Q} is closed under subtraction, $a - b$ is a valid element in T .
- For some $a, b \in T$, we can show that $ab \in T$. Since all the elements along the diagonal of ab are dot products of rows and columns of a and b , and since \mathbb{Q} is closed under multiplication/addition/subtraction, all of the elements along the diagonal are in \mathbb{Q} , and all the sum of those elements are in \mathbb{Q} as well.

- Let our unity be the identity matrix, I_N . Then, for any $t \in T$, $I_N t = t I_N$, and $\text{trace}(I_N) = n \in \mathbb{Q}$, so it is a valid element.
- (b) $D = \{A \in R : \det(A) \in \mathbb{Q}\}$
- $\det(0_N) = 0 \in \mathbb{Q}$, so the zero matrix is a valid element in D .
 - For some $a, b \in D$, we can show $a - b \in D$. Algorithmically, in the calculation of $a - b$ as well as $\det(a - b)$, the only operations we use are multiplication, addition, and subtraction (fact pulled from Linear Algebra). And since \mathbb{Q} is closed under all of these operations, $\det(a - b)$ must be in \mathbb{Q} .
 - The same is for any $ab : a, b \in D$. Since the multiplication of matrices involves no division, its product has only rational entries, and then its determinant must be a rational number as well.
 - Let the unity be the identity matrix, I_N . Then, $\det(I_N) = 1 \in \mathbb{Q}$.
- (c) $L = \{A \in R : A \text{ is lower triangular}\}$
- Trivially, the zero matrix, 0_N is lower triangular, since everything is 0, so it's a valid element.
 - For any $a, b \in L$, $a - b \in L$, because in both, every element above the diagonal is 0. And so all of the resulting elements above the diagonal in $a - b$ are just $0 - 0 = 0$, making it a valid lower triangular matrix as well.
 - From past homework, and from linear algebra, we know that lower triangular matrices are closed under multiplication. If you think of any element above the diagonal, like $(ab)[1][2]$, anywhere where the first row of a is nonzero, that position in the second column of b is zero, so the entire dot product just evaluates to 0 for those elements.
 - The identity matrix, I_N is lower triangular by definition, so it's a valid element as well.
3. Let $R = \mathbb{Z}[x]$, the ring of polynomials with coefficients in \mathbb{Z} .
- (a) Let $S = \{p(x) \in R : \text{every term of } p(x) \text{ has even degree}\} = \{a_0 + a_2x^2 + \dots a_{2k}x^{2k} : k \in \mathbb{Z}, k \geq 0, \text{ and } a_i \in \mathbb{Z}\}$. Prove that S is a subring of R .

Using the same checklist from earlier:

- The additive identity 0 has an even degree of 0, so it's a valid element in S .
- For any $a, b \in S$, $a - b$ can only have elements with degree from either a or b , which both only have elements of even degree, so $a - b$ therefore must only have elements of even degree. Also, all the elements have integer coefficients since the integers are closed under addition/subtraction.

- For any $a, b \in S$, ab can only have elements of even degree. Either: An elements degree is from a or b , in which case it must be even, as shown above. Or it has a degree of the sum of two elements from a and b respectively. And since evenness is closed under addition, all the elements of this type must be of even degree as well. So all of the elements in ab must be of an even degree. And all the coefficients are still $\in \mathbb{Z}$ since integers are closed under multiplication/addition.
 - The polynomial unity, 1, also has an even degree of 0.
- (b) Let $\phi : R \rightarrow \mathbb{Z} \times \mathbb{Z}$ be defined by $p(x) \rightarrow (p(0), p(1))$. Show that ϕ is a ring homomorphism, and find $\ker \phi = \phi^{-1}[(0, 0)]$.

First we can show that it is a valid homomorphism. Since $p(x)$ is a continuous real-valued function, and $(f+g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$, for some functions $f, g : \mathbb{R} \rightarrow \mathbb{R}$, we know that $(p_1 + p_2)(x) = p_1(x) + p_2(x)$ and $(p_1 p_2)(x) = p_1(x)p_2(x)$. So for some $a, b \in R$:

$$\begin{aligned}\phi(a + b) &= ((a + b)(0), (a + b)(1)) \\ &= (a(0) + b(0), a(1) + b(1)) = (a(0), a(1)) + (b(0), b(1)) \\ &= \phi(a) + \phi(b)\end{aligned}$$

Similarly:

$$\begin{aligned}\phi(ab) &= ((ab)(0), (ab)(1)) \\ &= (a(0)b(0), a(1)b(1)) = (a(0), a(1))(b(0), b(1)) \\ &= \phi(a)\phi(b)\end{aligned}$$

Then $\ker \phi$ is just the set of polynomials where $p(0) = 0$ and $p(1) = 0$. The set where $p(0) = 0$ are the set containing only monomials of power greater than 0 (cannot have any constant terms). And the set where $p(1) = 0$ are the set of polynomials where the coefficients sum to 0.

$$\ker \phi = \{p(x) \in R : \text{power of } p(x) > 0\} \cap \{p(x) \in R : \text{the coefficients of } p(x) \text{ sum to } 0\}$$