MA251 Algebra 1 - Week 10

Louis Li

April 5, 2023

1 Week 10

Question 1.

Prove Proposition 5.4.4 and its Corollary 5.4.5 in the notes.

Consider elements $g_1, ..., g_n$ of an abelian group G. It is possible to extend ths assignment $\phi(\mathbf{x}_i) = g_i$ to a group homomorphism $\phi : \mathbb{Z}^n \to G$. We define $\phi((a_1, a_2, ..., a_n)^T) = \sum_{i=1}^{n} a_i g_i$.

(a) Proposition 5.4.4. (i) The function ϕ is a group homomorphism. (ii) The set of elements $\{g_i\}$ are linearly independent if and only if ϕ is injective.

(iii) The set of elements $\{g_i\}$ span G if and only if ϕ is surjective.

(iv) The set of elements $\{g_i\}$ form a free basis of G if and only if ϕ is an isomorphism.

(b) Corollary 5.4.5. Let G be a free abelian group with a free basis $\mathbf{g}_1, ..., \mathbf{g}_n$. Let H be an abelian group and $a_1, .., a_n \in H$. Then there exists a unique group homomorphism $\phi : G \to H$ such that $\phi(g_i) = a_i$ for all i.

Proof.

(a) Since the target group is abelian and the source is free abelian, so if we specify the images of the basis elements we get a unique extension by $\mathbb{Z}$-linearity. Hence ϕ is a group homomorphism.

(b) If the set of elements $\{g_i\}$ are linearly independent, then if

$$\sum_{i=1}^{n} a_i g_i = 0_G,$$

then $a_i = 0_{\mathbb{Z}}$. This means $\ker(\phi) = \{0_{\mathbb{Z}}\}$ and by proposition 5.3.4, ϕ is injective if and only if $\ker(\phi) = \{0_G\}$. Similar for when ϕ is injective.

(c) Suppose the set of elements $\{g_i\}$ span G, then every element $g \in G$ can be expressed as a linear combination of the elements g_i with integer coefficients, i.e., $g = \sum_{i=1}^{n} b_i g_i$ for some integers $b_1, b_2, \ldots, b_n$. Now, let $a = (b_1, b_2, \ldots, b_n)^T \in \mathbb{Z}^n$. Then we have

$$\phi(a) = \phi((b_1, b_2, \ldots, b_n)^T) = \sum_{i=1}^{n} b_i g_i = g.$$

By the definition of ϕ and the fact that g can be expressed as a linear combination of the g_i's. Therefore, ϕ is surjective.

Suppose that ϕ is surjective. We want to show that the set of elements g_i spans G, i.e., every element $g \in G$ can be expressed as a linear combination of the elements g_i with integer coefficients. Let $g \in G$ be arbitrary. Since ϕ is surjective, there exists an element $a \in \mathbb{Z}^n$ such that $\phi(a) = g$. By the definition of ϕ, we have

$$\phi(a) = \phi((a_1, a_2, \ldots, a_n)^T) = \sum_{i=1}^{n} a_i g_i.$$

Therefore, g can be expressed as a linear combination of the elements g_i with integer coefficients, and hence the set of elements g_i spans G.

Therefore, we have shown that the set of elements g_i spans G if and only if ϕ is surjective.

(d) Suppose that the set of elements g_i form a free basis of G. We want to show that ϕ is an isomorphism, i.e., ϕ is both injective and surjective. First, we will show that ϕ is injective. Suppose that $\phi(a) = \phi(b)$ for some $a, b \in \mathbb{Z}^n$. Then, we have

$$\sum_{i=1}^{n} a_i g_i = \phi(a) = \phi(b) = \sum_{i=1}^{n} b_i g_i.$$

Since the set of elements g_i form a free basis of G, it follows that $a_i = b_i$ for all $i = 1, 2, \ldots, n$. Hence, $a = b$, and so ϕ is injective. Next, we will show that ϕ is surjective. Suppose that $g \in G$ is arbitrary. Since the set of elements g_i form a free basis of G, we know that there exist unique integers $a_1, a_2, \ldots, a_n$ such that $g = \sum_{i=1}^{n} a_i g_i$. Therefore, we have

$$\phi((a_1, a_2, \ldots, a_n)^T) = \sum_{i=1}^{n} a_i g_i = g.$$

Hence, ϕ is surjective.

Since ϕ is both injective and surjective, it follows that ϕ is an isomorphism.

Suppose that ϕ is an isomorphism. We want to show that the set of elements g_i form a free basis of G.

Since ϕ is an isomorphism, it follows that ϕ is bijective. Hence, for every $g \in G$, there exists a unique element $a \in \mathbb{Z}^n$ such that $\phi(a) = g$. Let $g \in G$ be arbitrary, and let $a = (a_1, a_2, \ldots, a_n)^T$ be the unique element of $\mathbb{Z}^n$ such that $\phi(a) = g$. Then, we have

$$g = \phi(a) = \sum_{i=1}^{n} a_i g_i.$$

Therefore, the set of elements g_i spans G.

To show that the set of elements g_i form a free basis of G, we need to show that they are linearly independent. Suppose that there exist integers $a_1, a_2, \ldots, a_n$ not all zero such that $\sum_{i=1}^{n} a_i g_i = 0$. Then, we have

$$\phi((a_1, a_2, \ldots, a_n)^T) = \sum_{i=1}^{n} a_i g_i = 0.$$

Since ϕ is injective, it follows that $(a_1, a_2, \ldots, a_n)^T = 0$, which implies that $a_i = 0$ for all $i = 1, 2, \ldots, n$. Hence, the set of elements g_i is linearly independent. Therefore, the set of elements g_i form a free basis of G.

Hence, we have shown that the set of elements g_i form a free basis of G if and only if ϕ is an isomorphism.

For Corollary 5.4.5, To prove that there exists a group homomorphism $\phi : G \to H$ such that $\phi(g_i) = a_i$ for all i, we will define ϕ by extending the linear function $f : \mathbb{Z}^n \to H$ such that $f(\mathbf{e_i}) = a_i$, where $\mathbf{e_i}$ is the standard basis vector in $\mathbb{Z}^n$.

Specifically, we define ϕ as follows: for any $\mathbf{m} \in \mathbb{Z}^n$, we can write $\mathbf{m} = \sum_{i=1}^n m_i\mathbf{e_i}$, and then we set $\phi(\mathbf{m}) = \sum_{i=1}^n m_i a_i$.

To see that ϕ is well-defined, suppose that $\mathbf{m} = \sum_{i=1}^n m_i\mathbf{e_i} = \sum_{i=1}^n m_i'\mathbf{e_i}$. Then $m_i = m_i'$ for all i, since the $\mathbf{e_i}$ form a basis for $\mathbb{Z}^n$. Therefore, we have $\phi(\mathbf{m}) = \sum_{i=1}^n m_i a_i = \sum_{i=1}^n m_i' a_i = \phi(\mathbf{m}')$, and so ϕ is well-defined.

Next, we show that ϕ is a group homomorphism. Let $\mathbf{m}, \mathbf{n} \in \mathbb{Z}^n$. Then we have:

$$\phi(\mathbf{m} + \mathbf{n}) = \sum_{i=1}^n (m_i + n_i)a_i \qquad = \sum_{i=1}^n m_i a_i + \sum_{i=1}^n n_i a_i \; = \phi(\mathbf{m}) + \phi(\mathbf{n}).$$

This shows that ϕ preserves addition.

Finally, we show that ϕ is unique. Suppose there exists another group homomorphism $\psi : G \to H$ such that $\psi(g_i) = a_i$ for all i. Then for any $\mathbf{m} \in \mathbb{Z}^n$, we have:

$$\psi(\mathbf{m}) = \psi\left(\sum_{i=1}^n m_i\mathbf{e_i}\right) \quad = \sum_{i=1}^n m_i\psi(\mathbf{e_i}) \; = \sum_{i=1}^n m_i a_i \quad = \phi(\mathbf{m}).$$

Therefore, ψ and ϕ agree on all elements of G, and so $\psi = \phi$. This shows that ϕ is unique.

In conclusion, we have shown that there exists a unique group homomorphism $\phi : G \to H$ such that $\phi(g_i) = a_i$ for all i.

$\square$

Question 2.

Are the following sets integral bases of $\mathbb{Z}^3$? If not, do they span, are they linearly independent or neither?

(a) $\mathbf{y}_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$,$\mathbf{y}_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$, $\mathbf{y}_3 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$,

(b) $\mathbf{y}_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$,$\mathbf{y}_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$,$\mathbf{y}_3 = \begin{pmatrix} -1 \\ 0 \\ -1 \end{pmatrix}$,

(c) $\mathbf{y}_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$,$\mathbf{y}_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$,$\mathbf{y}_3 = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}$.

Solution.

We can use the old-fashioned way to check their linear independence and span. However, here we are introduced to a new method, it is to find the determinant of the change of basis from the standard integral basis to these new vectors (which is just the matrix with $\mathbf{y}_i$ as the columns). The proposition here is that if a $n \times n$ matrix has a determinant of 1, then its columns form a basis in $\mathbb{R}^n$.

(a) The change of basis matrix is

$$A = \begin{pmatrix} 1 & 0 & -1 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix},$$

which has determinant 0. Therefore it is not a integral base of $\mathbb{Z}^3$. Therefore, we check if they are linearly independent first. Suppose

$$\alpha_1\mathbf{y}_1 + \alpha_2\mathbf{y}_2 + \alpha_3\mathbf{y}_3 = 0.$$

Solving the coefficients, we have

$$\alpha_1 = \alpha_2 = \alpha_3,$$

for all $\alpha_i \in \mathbb{R}$.

Thus, they are not linearly independent.

Let's check its span right now. If they span $\mathbb{Z}^3$, then they would span $\mathbb{Q}^3$ and we know that 3 vectors span $\mathbb{Q}^3$ if and only if they are a basis. Hence, it cannot span. Counterexample will be: consider $\mathbf{v} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, we see that there are no α_i such that

$$\alpha_1\mathbf{y}_1 + \alpha_2\mathbf{y}_2 + \alpha_3\mathbf{y}_3 = 0.$$

Hence, it cannot span $\mathbb{Z}^3$.

(b) The change of basis is

$$B = \begin{pmatrix} 1 & 0 & -1 \\ -1 & 1 & 0 \\ 0 & -1 & -1 \end{pmatrix},$$

which has determinant -2. Therefore it is not a integral base of $\mathbb{Z}^3$. Therefore, we check if they are linearly independent first. Suppose

$$\alpha_1\mathbf{y}_1 + \alpha_2\mathbf{y}_2 + \alpha_3\mathbf{y}_3 = 0.$$

Solving the coefficients, we have

$$\alpha_1 = \alpha_2 = \alpha_3 = 0.$$

(or since its determinant is non-zero, then it must be linearly independent)

Therefore, they are linearly independent. We can immediately conclude that it does not span $\mathbb{Z}^3$ since if it spans $\mathbb{Z}^3$, then it must be a basis, which contradicts our proposition.

(c) The change of basis is

$$C = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 1 \\ 0 & -1 & -1 \end{pmatrix},$$

which has determinant 1. Therefore, it is an integral base of $\mathbb{Z}^3$ and hence the vectors are linearly independent and span $\mathbb{Z}^3$.

$\square$

Question 3.

Find all subgroups of the groups $\mathbb{Z}/15$ and $\mathbb{Z}/2 \oplus \mathbb{Z}/4$. Express each subgroup as a direct sum of cyclic groups.

Solution.

For the group $\mathbb{Z}/15$, we note that $\mathbb{Z}/15 \cong \mathbb{Z}/3 \oplus \mathbb{Z}/5$. By Lagrange's Theorem, a subgroup H must have order 1,3,5 or 15.

(a) When $|H| = 1$, it is a unique trivial subgroup in this case.

(b) When $|H| = 3$, each subgroup of order 3 is isomorphic to $\mathbb{Z}/3$, which has two elements of order 3: 1 and 2. The only elements of order 3 in $\mathbb{Z}/3 \oplus \mathbb{Z}/5$ are $(1, 0)$ and $(2, 0)$. This gives a unique subgroup $H \cong \mathbb{Z}/3$.

(c) When $|H| = 5$, each subgroup of order 5 is isomorphic to $\mathbb{Z}/5$, which has four elements of order 5: 1,2,3 and 4. The only elements of order 5 in $\mathbb{Z}/3 \oplus \mathbb{Z}/5$ are $(0, n)$, where $n = 1, 2, 3, 4$. This gives a unique subgroup $H \cong \mathbb{Z}/5$.

(d) When $|H| = 15$, we must have $H = \mathbb{Z}/15$, a unique subgroup.

We following the same process with $\mathbb{Z}/2 \oplus \mathbb{Z}/4$. By Lagrange's Theorem, we must have order 1,2,4 and 8.

(a) When $|H| = 1$, it is a unique trivial subgroup in this case.

(b) When $H \cong \mathbb{Z}/2$, H is uniquely determined by its element of order 2. The only elements of order 2 in $\mathbb{Z}/2 \oplus \mathbb{Z}/4$ are $(1, 0), (0, 2)$ and $(1, 2)$. This gives 3 subgroups.

(c) When $H \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$, we have just seen that there are only three of them in the group, this gives a unique subgroup.

(d) When $H \cong \mathbb{Z}/4$, in this case H is uniquely determined by one of its two elements of order 4. The only elements of order 4 in $\mathbb{Z}/2 \oplus \mathbb{Z}/4$ are $(0, 1), (1, 1), (0, 3)$ and $(1, 3)$. This gives 2 subgroups.

(e) When $|H| = 8$, we must have $H = \mathbb{Z}/2 \oplus \mathbb{Z}/4$, a unique subgroup.

$\square$

Question 4.

How many elements of order 2 are there in

(a) $\mathbb{Z}/7$;

(b) $\mathbb{Z}/23452$;

(c) $\mathbb{Z}/4 \oplus \mathbb{Z}/4$;

(d) $\mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/4$.

Solution.

(a) By Lagrange's Theorem, there cannot be such any elements since they would generate a cyclic subgroup of order 2 which is not a factor of 7.

(b) There is 1 element. The choice of group is an arbitrary large even order. Claim that there is exactly one element in every cyclic group of even order m. The elements are residue classes modulo m and the only solution to $2h = m$ for $h \in 1, ..., m$ is $\frac{m}{2}$ (We exclude $h = 0$ since that has order 1).

(c) There are 3 elements. We know that $\mathbb{Z}/4$ has one element of order 2, namely (a, b). Therefore we want to find such a and b such that $2(a, b) = (0, 0)$, that means $2a = 0$ and $2b = 0$. Therefore, we have $(2, 2), (0, 2), (2, 0)$.

(d) There are 8 elements of order 2 such that $2g = 0$ and one of those will be the identity, so there are 7 elements. They are

$$(1, 0, 0), (0, 1, 0), (1, 1, 0), (1, 0, 2), (0, 1, 2), (1, 1, 2), (0, 0, 2).$$

□

Question 5.

Calculate the Smith Normal Form of the following matrices.

$$A_1 = \begin{pmatrix} -3 & 3 & 0 \\ -3 & 3 & 6 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & -2 \\ 3 & 4 \\ 2 & -4 \end{pmatrix}.$$

Solution.

(a) For A_1, $\gcd(-3, 3, 0, 6) = 3$. Since 3 occurs in A_1, we need to move it to the (1,1)th entry using column operations. We use UC2,

$$A_1 = \begin{pmatrix} -3 & 3 & 0 \\ -3 & 3 & 6 \end{pmatrix} \xrightarrow{\mathbf{c}_1 = \mathbf{c}_2 + \mathbf{c}_1} \begin{pmatrix} 0 & 3 & 0 \\ 0 & 3 & 6 \end{pmatrix} \xrightarrow{\mathbf{c}_2 \leftrightarrow \mathbf{c}_1} \begin{pmatrix} 3 & 0 & 0 \\ 3 & 0 & 6 \end{pmatrix}.$$

Now 3 is in the (1,1)th entry, we need to use row operations and column operations to clear everything else in $\mathbf{r}_1$ and $\mathbf{c}_1$. Hence,

$$A_1 = \begin{pmatrix} 3 & 0 & 0 \\ 3 & 0 & 6 \end{pmatrix} \xrightarrow{\mathbf{r}_2 = \mathbf{r}_2 - \mathbf{r}_1} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \end{pmatrix}.$$

In order to get Smith Normal Form, we need to make sure $d_1 | d_2$, hence we use UC2 again,

$$A_1 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \end{pmatrix} \xrightarrow{\mathbf{c}_2 = \mathbf{c}_3 \leftrightarrow \mathbf{c}_2} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}.$$

Therefore, we get the Smith Normal Form of A_1.

(b) For A_2, $\gcd(1, -2, 3, 4, 2, -4) = 1$. Since 1 is already in the (1,1)th entry, we can use it to clear everything out in $\mathbf{r}_1$ and $\mathbf{c}_1$:

$$A_2 = \begin{pmatrix} 1 & -2 \\ 3 & 4 \\ 2 & -4 \end{pmatrix} \xrightarrow{\mathbf{r}_3 = 2\mathbf{r}_1 - \mathbf{r}_3} \begin{pmatrix} 1 & -2 \\ 3 & 4 \\ 0 & 0 \end{pmatrix} \xrightarrow{\mathbf{c}_2 = 2\mathbf{c}_1 + \mathbf{c}_2} \begin{pmatrix} 1 & 0 \\ 3 & 10 \\ 0 & 0 \end{pmatrix} \xrightarrow{\mathbf{r}_2 = \mathbf{r}_2 - 3\mathbf{r}_1} \begin{pmatrix} 1 & 0 \\ 0 & 10 \\ 0 & 0 \end{pmatrix}.$$

Hence, this is the Smith Normal form of A_2.

□