MA503: Homework 7

Exercise 7.1. [10pts] Find the Smith normal form of the matrix

$$\begin{bmatrix} 1 & 2 & 1 \\ 3 & 4 & 0 \\ 2 & 1 & -1 \end{bmatrix}$$

Show all steps!

Solution: (1) Subtract the row #1 multiplied by 3 from the row #2 to get

$$\begin{bmatrix} 1 & 2 & 1 \\ 0 & -2 & -3 \\ 2 & 1 & -1 \end{bmatrix}$$

(2) Subtract the row #1 multiplied by 2 from the row #3 to get

$$\begin{bmatrix} 1 & 2 & 1 \\ 0 & -2 & -3 \\ 0 & -3 & -3 \end{bmatrix}$$

(3) Subtract the column #1 from the columns #2 and #3 to get

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -2 & -3 \\ 0 & -3 & -3 \end{bmatrix}$$

(4) Subtract the row #3 from the row #2 to get

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -3 & -3 \end{bmatrix}$$

(5) Add the row #2 multiplied by 3 to the row #3 to get

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -3 \end{bmatrix}$$

(6) Multiply the row #3 by -1 to get

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$

□

Exercise 7.2. [10pts] Consider the set $\mathbf{Hom}(\mathbb{Z}^n, \mathbb{Z}_2)$ of homomorphisms from $\mathbb{Z}^n$ to $\mathbb{Z}_2$ has 2^n elements. Fix the standard free basis $\{e_1, \ldots, e_n\}$ for $\mathbb{Z}^n$.

(a) Consider any homomorphism $\varphi : \mathbb{Z}^n \to \mathbb{Z}_2$. Let $b_i = \varphi(e_i)$ for $i = 1, \ldots, n$. Let $v = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$. Show that $\varphi(v)$ is uniquely defined by $b_1, \ldots, b_n$, i.e., find a formula for $\varphi(v)$.

(b) Prove that for any $b_1, \ldots, b_n \in \{0, 1\}$ there exists a homomorphism φ satisfying $b_i = \varphi(e_i)$ for every $i = 1, \ldots, n$.

(c) Conclusion. There are 2^n choices of $b_1, \ldots, b_n \in \{0, 1\}$. Each choice defines a unique homomorphism. Hence, there are 2^n homomorphisms.

Solution: Fix any homomorphism $\varphi : \mathbb{Z}^n \to \mathbb{Z}_2$. Then every $v = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$ can be uniquely expressed as a linear combination of the basis vectors

$$(\alpha_1, \ldots, \alpha_n) = \alpha_1 e_1 + \ldots + \alpha_n e_n$$

and by definition of a homomorphism we have

$$\begin{aligned}\varphi(v) &= \varphi(\alpha_1 e_1 + \ldots + \alpha_n e_n)\\ &= \varphi(\alpha_1 e_1) + \ldots + \varphi(\alpha_n e_n)\\ &= \alpha_1\varphi(e_1) + \ldots + \alpha_1\varphi(e_n)\\ &= \alpha_1 b_1 + \ldots + \alpha_1 b_n.\end{aligned}$$

So, the formula for $\varphi(v)$ is uniquely defined by the values of $b_1, \ldots, b_n$. That proves (a).

Now we prove the converse statement. Fix $b_1, \ldots, b_n \in \{0, 1\}$. Define a map $\varphi : \mathbb{Z}^n \to \mathbb{Z}_2$ as follows:

$$(\alpha_1, \ldots, \alpha_n) \quad \overset{\varphi}{\mapsto} \quad \alpha_1 b_1 + \ldots + \alpha_1 b_n.$$

Clearly it satisfies $\varphi(e_i) = b_i$. It is easy to see that it is a homomorphism, because for any $(\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)$ $\mathbb{Z}^n$ we have the same

$$\varphi((\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n)) = \varphi((\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)) = (\alpha_1 + \beta_1)b_1 + \ldots + (\alpha_n + \beta_n)b_n$$

and

$$\varphi((\alpha_1, \ldots, \alpha_n)) + \varphi((\beta_1, \ldots, \beta_n)) = \alpha_1 b_1 + \ldots + \alpha_n b_n + \beta_1 b_1 + \ldots + \beta_n b_n.$$

That proves (b).

Thus, there is a one to one correspondence between homomorphisms $\varphi : \mathbb{Z}^n \to \mathbb{Z}_2$ and n-tuples $b_1, \ldots, b_n$. There are 2^n tuples. Hence, there are 2^n homomorphisms. □

A **hidden subgroup problem** algorithm is one of the most advanced algorithms in quantum computing. The factorization problem and the dlp problem are particular cases of HSP. The goal of that algorithm is to learn the algebraic structure of some abelian group G "hidden inside an algebraic operator".

- By assumption, we know the generators $x_1, \ldots, x_n$ for G.
- Roughly speaking, each iteration of the algorithm produces a random relation for $x_1, \ldots, x_n$, i.e., a tuple $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$ satisfying $\alpha_1 x_1 + \ldots + \alpha_n x_n = 0$.
- It can produce a useless relation, like $(0, \ldots, 0)$.
- It can produce a redundant relation, i.e., one that follows from already found relations.

Exercise 7.3. [10pts] Suppose that G is an abelian group generated by x_1 and x_2. Using a quantum algorithm we learn that x_1 and x_2 are subject to the following relations:

$$\begin{aligned}r_1 &= 6x_1 + 10x_2 = 0\\ r_2 &= 14x_1 - 2x_2 = 0\\ r_3 &= -4x_1 + 18x_2 = 0.\end{aligned}$$

Assuming that this set of relations is complete (all other relations follow from r_1, r_2, r_3) express G as a direct product of cyclic groups.

Solution: The group G is generated by x_1 and x_2 that are subject to three relations. Construct the matrix of relations and apply elementary row and column operations

$$\begin{bmatrix} 6 & 10 \\ 14 & -2 \\ -4 & 18 \end{bmatrix} \to \begin{bmatrix} 14 & -2 \\ 6 & 10 \\ -4 & 18 \end{bmatrix} \to \begin{bmatrix} 0 & -2 \\ 76 & 10 \\ 122 & 18 \end{bmatrix} \to \begin{bmatrix} 0 & -2 \\ 76 & 0 \\ 122 & 0 \end{bmatrix} \to \begin{bmatrix} 0 & 2 \\ 2 & 0 \\ 0 & 0 \end{bmatrix} \to \begin{bmatrix} 2 & 0 \\ 0 & 2 \\ 0 & 0 \end{bmatrix}$$

Hence, $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. □

Exercise 7.4. [10pts] Suppose that G is an abelian group generated by x_1, x_2, x_3. Using a quantum algorithm we learn that x_1, x_2, x_3 are subject to the following relations:

$$\begin{aligned}r_1 &= 2x_1 + 4x_2 - 4x_3 = 0\\ r_2 &= -4x_1 + 2x_2 + 8x_3 = 0.\end{aligned}$$

Assuming that this set of relations is complete (all other relations follow from r_1, r_2) express G as a direct product of cyclic groups.

Solution: Construct the matrix of relations and apply elementary row and column operations

$$\begin{bmatrix} 2 & 4 & -4 \\ -4 & 2 & 8 \end{bmatrix} \to \begin{bmatrix} 2 & 4 & 0 \\ -4 & 2 & 0 \end{bmatrix} \to \begin{bmatrix} 2 & 0 & 0 \\ -4 & 10 & 0 \end{bmatrix} \to \begin{bmatrix} 2 & 0 & 0 \\ 0 & 10 & 0 \end{bmatrix}$$

Hence, $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}$. □

Definition 7.1. A ring R is a **commutative** if $\cdot$ is commutative.

All rings in our course are commutative!

Definition 7.2. $a \in R$ is a **unit** if R contains a **multiplicative inverse** for a, i.e., for some $b \in R$, $ab = 1$, denoted by a^{-1}.

Definition 7.3. A **field** is a commutative ring in which **every non-trivial element is a unit**.

Exercise 7.5. [+6pts] Which of the following rings are fields? If R is a field, then find inverses for all nontrivial elements, or a formula to compute the inverse. If R is not a field, then find a nontrivial element that has no inverse (prove that it has no inverse).

(a) $(\mathbb{Z}_5, +, \cdot)$
(b) $(\mathbb{Z}_6, +, \cdot)$
(c) $\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ with the usual addition and multiplication.

Solution:

(a) $(\mathbb{Z}_5, +, \cdot)$ is a field because

$$1^{-1} = 1 \qquad 2^{-1} = 3 \qquad 3^{-1} = 2 \qquad 4^{-1} = 4.$$

(b) $(\mathbb{Z}_6, +\cdot)$ is not a field because 2 is a non-trivial element that has no inverse (congruence $2x \equiv_6 1$ has no solutions).

(c) $\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ is a field because

$$(a + b\sqrt{5})^{-1} = \frac{1}{a + b\sqrt{5}} = \frac{a - b\sqrt{5}}{(a + b\sqrt{5})(a - b\sqrt{5})} = \frac{a - b\sqrt{5}}{a^2 - 5b^2} = \frac{a}{a^2 - 5b^2} - \frac{b}{a^2 - 5b^2}\sqrt{5}$$

which is itself a number of the form $a + b\sqrt{5}$.

□