Algebraic Structures: Solutions to Homework 2

written by: Motke Porat

November 2017

1 Question 1.

1.1 (f):

Let $n \in \mathbb{Z}_{>0}$ and its decomposition as a product of powers of primes given by

$$n = \prod_{i=1}^{k} p_i^{n_i} = p_1^{n_1} \dots p_k^{n_k}.$$

We will show that $(\mathbb{Z}_n, +, 0) \approx \prod_{i=1}^{k} (\mathbb{Z}_{p_i^{n_i}}, +, 0) = (\mathbb{Z}_{p_1^{n_1}}, +, 0) \times \dots \times (\mathbb{Z}_{p_k^{n_k}}, +, 0)$ by building an explicit isomorphism between the two groups: let

$$\eta : (\mathbb{Z}_n, +, 0) \to (\mathbb{Z}_{p_1^{n_1}}, +, 0) \times \dots \times (\mathbb{Z}_{p_k^{n_k}}, +, 0)$$

defined by

$$\eta(m) = (m \mod p_1^{n_1}, \dots, m \mod p_k^{n_k}).$$

The mapping η is $1-1$: If $m_1, m_2 \in \mathbb{Z}_n$ and $\eta(m_1) = \eta(m_2)$, then

$$(m_1 \mod p_1^{n_1}, \dots, m_1 \mod p_k^{n_k}) = (m_2 \mod p_1^{n_1}, \dots, m_2 \mod p_k^{n_k})$$

and hence $m_1 = m_2 (\mod p_i^{n_i})$ for every $1 \leq i \leq k$, i.e.,

$$p_i^{n_i} \mid m_1 - m_2, \quad \forall 1 \leq i \leq k$$

but since $p_1, \dots, p_k$ are all distinct prime numbers, it implies that

$$n = p_1^{n_1} \cdot \dots \cdot p_k^{n_k} \mid m_1 - m_2$$

therefore $m_1 = m_2 (\mod n)$ and η is $1-1$.

The mapping η is onto: From the Chinese reminder theorem, for every $r_1, \dots, r_p$ such that $0 \leq r_1 \leq p_1^{n_1}, \dots, 0 \leq r_k \leq p_k^{n_k}$ there exists an integer m for which

$$m = r_i (\mod p_i^{n_i}), \quad \forall 1 \leq i \leq k,$$

since $p_1^{n_1}, \dots, p_k^{n_k}$ are all coprime (as powers of distince prime numbers)! Therefore, for every $(r_1, \dots, r_k) \in \mathbb{Z}_{p_1^{n_1}} \times \dots \times \mathbb{Z}_{p_k^{n_k}}$ we found $m \in \mathbb{Z}_n$ such that-

$$\eta(m) = (m \mod p_1^{n_1}, \dots, m \mod p_k^{n_k}) = (r_1, \dots, r_k).$$

The mapping η is a homomorphism: It is easy to see that if $m_1, m_2 \in \mathbb{Z}_n$, then

$$\begin{aligned}\eta(m_1+m_2) &= ((m_1+m_2) \mod p_1^{n_1}, ..., (m_1+m_2) \mod p_k^{n_k}) \\ &= (m_1 \mod p_1^{n_1}, ..., m_1 \mod p_k^{n_k}) + (m_2 \mod p_1^{n_1}, ..., m_2 \mod p_k^{n_k}) \\ &= \eta(m_1) + \eta(m_2).\end{aligned}$$

Example 1.1 (the case $\mathbb{Z}_{10} \approx \mathbb{Z}_2 \times \mathbb{Z}_5$) *let $n = 10 = 2 \cdot 5$, so $p_1 = 2, p_2 = 5, n_1 = 1, n_2 = 1, k = 2$. The isomorphism between $\mathbb{Z}_{10}$ and $\mathbb{Z}_2 \times \mathbb{Z}_5$ is given by-*

$$\eta(m) = (m \mod 2, m \mod 5)$$

and explicitly-

$$\eta(0) = (0,0), \eta(1) = (1,1), \eta(2) = (0,2), \eta(3) = (1,3), \eta(4) = (0,4),$$
$$\eta(5) = (1,0), \eta(6) = (0,1), \eta(7) = (1,2), \eta(8) = (0,3), \eta(9) = (1,4).$$

1.2 (g): No, and here is the proof:

Let G be an infinite cyclic group. By the definition of cyclic groups- there exists $g \in G$ for which $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. We shall consider the mapping $\phi : \mathbb{Z} \to g$ defined by

$$\phi(n) = g^n.$$

It is clear (as G is cyclic) that ϕ is onto G and therefore $|\mathbb{Z}| \geq |G|$ and that proves that $|G|$ has to be countable.

1.3 (h):

Let $\mathbb{K}$ be a field with $char(\mathbb{K}) = 0$ and assume that its multiplicative group $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$ is cyclic, so there exists $g \in \mathbb{K}^\times$ for which $\mathbb{K}^\times = \langle g \rangle$. As $1+1 \neq 0$ and $1+1+1 \neq 0$, there exists $n, m \in \mathbb{Z}$ such that $2 := 1+1 = g^n$ and $3 := 1+1+1 = g^m$. Therefore,

$$3^n = (g^m)^n = g^{nm} = (g^n)^m = 2^m$$

and that is a contradiction. (Remark: that proof is working with any two other different prime numbers p_1, p_2 instead of $2, 3$)

1.4 (i): No, and here is the proof:

Suppose there exists a cyclic group G with the property that for every $n \in \mathbb{N} \setminus \{0, 1\}$ there exists $a \in G \setminus \{e\}$ for which $a^n = e$. We notice two cases:

- If G is finite: denote by $n_1, ..., n_m$ the orders of all elements of G and let $n = 1 + n_1 \cdot ... \cdot n_m$. Then, for every $a \in G \setminus \{e\}$ we have

  $$a^n = a^{1+n_1...n_m} = a \cdot a^{n_1...n_m} = a \neq e$$

  so we found an integer n that contradicts our assumption! (in this case we did not even use the fact that G is cyclic)

- If G is infinite, then there exists $g \in G$ such that $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ and the order of the element g is not finite, or in other words

$$g^n \neq e$$

for any $0 \neq n \in \mathbb{Z}$. By the assumption, there exists $a \in G \setminus \{e\}$ such that $a^2 = e$, but $G = \langle g \rangle$ so we can find $0 \neq m \in \mathbb{Z}$ such that $a = g^m$ and hence $e = a^2 = (g^m)^2 = g^{2m}$. We found that

$$g^{2m} = e, \quad 2m \neq 0$$

and that is a contradiction.

2 Question 2.

2.1 (a): No, here is a counterexample:

Let G be any infinite (countable will work here) product of copies of $(\mathbb{Z}_2, +, 0)$, say

$$G = \prod_{i=1}^{\infty} \mathbb{Z}_2.$$

So G is of order $2^{|\mathbb{N}|} = 2^{\aleph_0} > \aleph_0$ that is uncountable and all the elements of G are of order 2.

2.2 (b):

Let V be a vector space over a field $\mathbb{K}$ that is finite dimensional $\dim V = n < \infty$. Recall that $GL_{\mathbb{K}}(V) = \{\phi : V \to V | \phi \text{ is automorphism}\}$ and let us show it is a group with respect to the operation of composition:

- If $\phi_1, \phi_2 \in GL_{\mathbb{K}}(V)$, then $\phi_1 \circ \phi_2 : V \to V$ is an automorphism of v and so $\phi_1 \circ \phi_2 \in GL_{\mathbb{K}}(V)$.
- If $\phi_1, \phi_2, \phi_3 \in GL_{\mathbb{K}}(V)$, then clearly

$$\phi_1 \circ (\phi_2 \circ \phi_3) = (\phi_1 \circ \phi_2) \circ \phi_3.$$

- The identity mapping $id : V \to V$ is in $GL_{\mathbb{K}}(V)$ and $\phi \circ id = id \circ \phi$ for every $\phi \in GL_{\mathbb{K}}(V)$.
- If $\phi \in GL_{\mathbb{K}}(V)$, then as ϕ is $1-1$ and onto V, the inverse mapping ϕ^{-1} exists and it is an automorphism of V, so $\phi^{-1} \in GL_{\mathbb{K}}(V)$.

Now we will show that $GL_{\mathbb{K}}(V) = GL_n(V)$: Let $b = \{e_1, ..., e_n\}$ be a basis of V over the field $\mathbb{K}$. For every $\phi \in GL_{\mathbb{K}}(V)$ recall that $[\phi]_B$ is the representing matrix of ϕ with respect to B, given by the definition

$$\phi(\alpha_1 e_1 + ... + \alpha_n e_n) = [\phi]_B \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \quad \forall \alpha_1, ..., \alpha_n \in \mathbb{K}.$$

Define a mapping $\psi : GL_{\mathbb{K}}(V) \to GL_n(\mathbb{K})$ in the following way

$$\psi(\phi) := [\phi]_B.$$

The mapping ψ is an isomorphism between the groups $GL_{\mathbb{K}}(V)$ and $GL_n(\mathbb{K})$:

- If $\psi(\phi_1) = \psi(\phi_2)$ for some $\phi_1, \phi_2 \in GL_{\mathbb{K}}(V)$, then $[\phi_1]_B = [\phi_2]_B$ and then for every $v \in V$, there exists $\alpha_1, ..., \alpha_n \in \mathbb{K}$ such that $v = \alpha_1 e_1 + .. + \alpha_n e_n$,

$$\phi_1(v) = \phi_1(\alpha_1 e_1 + ... + \alpha_n e_n) = [\phi_1]_B \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

$$= [\phi_2]_B \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \phi_2(\alpha_1 e_1 + ... + \alpha_n e_n) = \phi_2(v),$$

  i.e., $\phi_1 = \phi_2$ and the mapping ψ is $1-1$.

- For every $A \in GL_n(\mathbb{K})$, define $\phi_A : V \to V$ by

$$\phi_A(v) = A[v]_B = A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \quad \forall v = \alpha_1 e_1 + ... + \alpha_n e_n \in V.$$

  As A is invertible matrix, it is easily seen that ϕ_A is an automorphism of V, i.e., that $\phi_A \in GL_{\mathbb{K}}(V)$ and also that

$$\psi(\phi_A) = [\phi_A]_B = A,$$

  so the mapping ψ is onto $GL_n(\mathbb{K})$.

- For every $\phi_1, \phi_2 \in GL_{\mathbb{K}}(V)$, we have

$$\psi(\phi_1 \circ \phi_2) = [\phi_1 \circ \phi_2]_B = [\phi_1]_B [\phi_2]_B = \psi(\phi_1)\psi(\phi_2).$$

2.3 (e):

Recall that if $S = \{x_\alpha\}_{\alpha \in A}$ then $\langle S \rangle = \{x_{\alpha_1}^{\pm 1} \cdot ... \cdot x_{\alpha_n}^{\pm 1} : n \in \mathbb{N}\}$ is a subgroup of G and that $S \subset \langle S \rangle$.

- For every $H_\beta \leq G$ such that $S \subset H_\beta$, as H_β is a group then H_β must contain all products of elements and inverses of elements from S, that means $\langle S \rangle \subset H_\beta$ and therefore

$$\langle S \rangle \subset \bigcap_{S \subset H_\beta \leq G} H_\beta.$$

- As $\langle S \rangle \leq G$ and $S \subset \langle S \rangle$, one of the $H_\beta' s$ is equal to $\langle S \rangle$, then

$$\bigcap_{S \subset H_\beta \leq G} H_\beta \subset \langle S \rangle.$$

2.4 (f):

We will show two examples as required.

- Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ the product of the group $(\mathbb{Z}_2, +, 0)$ with itself, $H_1 = \langle(1,0)\rangle$ and $H_2 = \langle(0,1)\rangle$. Clearly $H_1, H_2 \leq G$ as they are the subgroups generated by an element of G, $H_1 \neq H_2$ as $(1,0) \in H_1$ but $(1,0) \notin H_2$ and $H_1 \approx H_2$ as one can easily consider the isomorphism from H_1 to H_2 given by
$$\phi((1,0)) = (0,1), \phi((0,0)) = (0,0),$$
or using a more general fact that any two groups of rder 2 are isomorphic.
- Let $G = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, H_1 = \langle(1,0,0)\rangle$ and $H_2 = \{0\} \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Clearly $H_1 \leq G$ as a cyclic subgroup of G, whereas $H_2 \leq G$ since $\{0\} \leq \mathbb{Z}_4$ and $|H_1| = |H_2| = 4$. Finally, $H_1 \not\approx H_2$ can be easily seen as H_1 contains an element of order 4 (for example $(1,0,0)$) and if $H_! \approx H_2$ then also H_2 contains an element of order 4, which is clearly not true.

3 Question 4.

3.1 (c):

Denote $K_n = \{1, ..., n\}$. Let $\sigma \in S_n$ be any permutation.

- If $\sigma(x) = x$ for all $x \in K_n$, then $\sigma = (1)$ and it is cyclic.
- If $\sigma \neq (1)$, let a_1 be the smallest number satisfies $\sigma(a_1) \neq a_1$. Write the list
$$\begin{aligned} \sigma(a_1) &= a_2 \\ \sigma(a_2) &= a_3 \\ &\vdots \\ \sigma(a_j) &= a_{j+1} \\ &\vdots \end{aligned}$$
As K_n is finite, there exists i such that $\sigma(a_i)$ is equal to one of the values $a_1, ..., a_i$. Let k be the smallest number i with this property. So we know that $\sigma(a_k) = a_j$ for some $1 \leq j \leq k$. We will show that $j = 1$: otherwise, $j > 1$ and then $\sigma(a_{k-1}) = a_k, \sigma(a_{j-1}) = a_j$ imply that
$$\sigma(a_{j-1}) = a_j = \sigma(a_k) = \sigma(\sigma(a_{k-1}))$$
ad hence $a_{j-1} = \sigma(a_{k-1})$, as σ is $1-1$. But that is a contradiction to the minimality of k, and therefore $j = 1$. Then $\sigma(a_k) = a_1$ and we got k distinct elements $a_1, ..., a_k$ such that $\sigma(a_1) = a_2, ..., \sigma(a_k) = a_1$, i.e., the set $a_1, ..., a_k$ determines one cyclic $\sigma_1 = (a_1, ..., a_k)$ in the requested product formula for σ.
- If $\sigma(b) = b$ for all $b \in K_n \setminus \{a_1, ..., a_k\}$, then $\sigma = (a_1, ..., a_k)$ is a cyclic.

- Otherwise, let $b_1 \in K_n \setminus A_1$ satisfies $\sigma(b_1) \neq b_1$ and in a similar way construct a cyclic σ_2 of the form $\sigma = (b_1, b_2, ..., b_t)$.
- In every step we start to construct a cyclic from an element $x \in K_n$ which does not appear in any of the previous cycles that satisfies $\sigma(x) \neq x$. This process will end after finitely any steps, as K_n is finite and in every step we omit at least two elements from K_n. Clearly, all the cycles we get at the end of the process, say $\sigma_1, ..., \sigma_r$ are all disjoint and that

$$\sigma = \sigma_1 \cdot ... \cdot \sigma_r.$$

- As any two disjoint cycles are commutating and the order of a cyclic is equal to its length, it follows that the order of $\sigma = \sigma_1 \cdot ... \cdot \sigma_r$ is equal to the smallest common multiple of all the orders $ord(\sigma_1), ..., ord(\sigma_r)$, i.e.,

$$ord(\sigma) = [|\sigma_1|, ..., |\sigma_r|].$$

3.2 (d):

- S_n is of order $n!$.
- The number of all of cycles in S_n of length k is given by

$$\binom{n}{k}(k-1)! :$$

to get all cycles of the form $(a_1, ..., a_k)$ one should choose k elements out of $\{1, ..., n\}$-there are $\binom{n}{k}$ many such choices, however there are k ways to describe the same cyclic

$$(a_1, ..., a_k) = (a_2, ..., a_k, a_1) = ... = (a_k, a_1, ..., a_{k-1}),$$

so one should also fix the first element a_1 on the cycle and then you have $(k-1)!$ ways to get all the possible cycles consists of $a_2, ..., a_k$.