Algebra: Chapter 0 Exercises Chapter 2, Section 6

David Melendez

July 13, 2017

Problem 6.2. Prove that the set of upper-triangular matrices form a subgroup of $GL_2(\mathbb{Z})$.

Solution. Let V be an n-dimensional vector space over \mathbb{C} , and let $\mathcal{M}: \mathcal{L}(V) \to \mathbb{C}^{n,n}$ be the isomorphism that takes a linear operator to its matrix with respect to some basis

$$\mathcal{B} = \{v_1, \dots, v_n\}.$$

Let A, B be upper-triangular matrices, and let S, T (respectively) be $\mathcal{M}^{-1}(A)$ and $\mathcal{M}^{-1}(B)$. We then know, due to a theorem in Axler, that $\operatorname{span}(v_1, \ldots, v_k)$ is invariant under S and T for $1 \leq k \leq n$ (this property is equivalent to the matrix being upper-triangular). Using this property and the invertibility of T, it then follows that

$$T^{-1}(a_1v_1 + \dots + a_kv_k) = T^{-1}(T(b_1v_1 + \dots + b_kv_k))$$

= $b_1v_1 + \dots + b_kv_k$

meaning span (v_1, \ldots, v_k) is invariant under T^{-1} , and hence that T^{-1} is upper-triangular. Similarly,

$$(ST^{-1})(a_1v_1 + \dots + a_kv_k) = S(b_1v_1 + \dots + b_kv_k)$$

= $c_1v_1 + \dots + c_kv_k$,

making ST^{-1} upper-triangular and completing the proof.

Problem 6.4. Let G be a commutative group, and let n > 0 be an integer. Prove that $\{g^n | g \in G\}$ is a subgroup of G. Prove that this is not necessarily the case if G is not commutative.

Solution. Let G be a commutative group, and let $G' = \{g^n | g \in G\}$ where n is any positive integer. To prove that this is a group, suppose $g = g_1^n$ and $h = g_2^n$ are elements of G'. We then have:

$$gh^{-1} = (g_1^n)(g_2^n)^{-1}$$
$$= (g_1)^n (g_2^{-1})^n$$
$$= (g_1 g_2^{-1})^n$$
$$\in G'$$

Hence G' is a subgroup of G.

As a counterexample in the case that G is not commutative, let $G = F(\{x,y\})$, the free group generated by x and y, and let n = 2. In order for G' to be closed under its operation, we would need to have $g \in G$ such that

$$g^2 = x^2 y^2.$$

That such a g does not exist is turning out to be harder to prove than I suspected, so I'll come back to this later.

Problem 6.6.

- 1. Let H, H' be subgroups of a group G. Prove that $H \cup H'$ is a subgroup of G only if $H \subseteq H'$ or $H' \subseteq H$.
- 2. On the other hand, let $H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots$ be subgroups of a group G. Prove that $G' = \bigcup_{i \ge 0} H_i$ is a subgroup of G.

Solution.

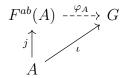
- 1. Suppose $H \cup H'$ is a subgroup of G. We then have, by closure, for all $h \in h$ and $h \in h'$, that hh' = g for some $g \in H \cup H'$. If $g \in H$, we have $h' = h^{-1}g \in H$, meaning $H' \subseteq H$. Alternatively, if $g \in H'$, we have $h = g(h')^{-1} \in H'$ meaning $H \subseteq H'$.
- 2. Let $h_1 \in H_j$ and $h_2 \in H_k$ (both in G', of course), and assume without loss of generality that $j \leq k$. By the sequence of subset relations, we know that $h_1 \in H_k$, so $h_1 h_2^{-1} \in H_k \subseteq G'$, completing the proof.

Problem 6.8. Prove that an abelian group G is finitely generated if and only if there is a surjective homomorphism

$$\bigoplus_{i=1}^n \mathbb{Z} \to G$$

for some n.

Solution. First, suppose that an abelian group G is finitely generated. This, by definition, means that there exists a finite subset A of G such that $\langle A \rangle = G$; in other words, G is the image of the homomorphism φ_A obtained by applying the universal property for the free abelian group over A as follows:



2

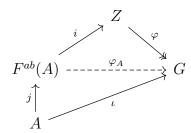
where ι and j are the inclusion maps into G and $F^{ab}(A)$, respectively. We know by exercise 5.7 that $Z = \bigoplus_{i=1}^n \mathbb{Z} \cong F^{ab}(A)$, so we have a surjection

$$Z \xrightarrow{\sim} F^{ab}(A) \xrightarrow{\varphi_A} G$$

For the proof in the other direction, suppose we have a surjective homomorphism $\varphi: Z \to G$. For integers $0 \le m \le n$, let β_m be the *n*-tuple with 0 in every slot except for the *m*th slot, where there is a 1. Define *A* to be the set $\{\varphi(\beta_1), \ldots, \varphi(\beta_n)\}$ (since the coproduct and product in **Ab** are the same), and let a_m be the *m*th element of *A* as listed above. Define the isomorphism $i: F^{ab}(A) \to Z$ by

$$i(m_1a_1+\cdots+m_na_n)=(m_1,\ldots,m_n),$$

and let $f: F^{ab}(A) \to G$ be defined by $f = i\varphi$. Finally, let j and ι be the standard inclusions into $F^{ab}(A)$ and G, respectively.. the following diagram illustrates these morphisms:



Define α_m to be $j(a_m)$, let $a = m_1 a_1 + \cdots + m_n a_n$, and let $\alpha = j(a)$. We then have:

$$(f \circ j)(a) = f(\alpha)$$

$$= (\varphi \circ i)(m_1\alpha_1 + \dots + m_n\alpha_n)$$

$$= \varphi(m_1, \dots, m_n)$$

$$= m_1\varphi(\beta_1) + \dots + m_n\varphi(\beta_n)$$

$$= m_1\iota(a_1) + \dots + m_n\iota(a_n)$$

$$= \iota(a)$$

Since the morphism φ_A is the only morphism that satisfies this property (by the universality of $F^{ab}(A)$, we know that $f = \varphi_A$. But f (and hence φ_A) is surjective, giving us $G = \operatorname{im}(\varphi_A) = \langle A \rangle$, as desired.

Problem 6.9. Prove that every finitely generated subgroup of \mathbb{Q} is cyclic. Prove that \mathbb{Q} is not finitely generated.

Solution. First, I will state (but not prove) a lemma from number theory that will be useful in this proof:

Lemma 1. The diophantine equation

$$a_1x_1 + \cdots + a_nx_n = d$$

has a solution if and only if

$$\gcd(x_1,\ldots,x_n)\mid d.$$

This actually follows quite easily from the case involving two terms, according to a post on stack exchange. ¹ Now, on to the problem:

Proposition. Let $r_1 = \frac{p_1}{q_1}, \ldots, r_n = \frac{p_n}{q_n}$ be (reduced) rational numbers. Then the group $G = \langle r_1, \ldots, r_n \rangle$ is cyclic; in fact, we have

$$M := \left\langle \frac{\gcd(P)}{\operatorname{lcm}(Q)} \right\rangle = G$$

where $P = \{p_1, ..., p_n\}$ and $Q = \{q_1, ..., q_n\}$.

Proof. First, we will prove that $M \subseteq G$ by proving that the generator of M written above is in G. Consider the following equation:

$$a_1r_1 + \dots + a_nr_n = \frac{\gcd(P)}{\operatorname{lcm}(Q)}$$

If we let c = lcm(Q), this is equivalent to the equation

$$a_1(cr_1) + \cdots + a_n(cr_n) = \gcd(P),$$

which, by Lemma 1, has a solution if and only if

$$\gcd(cr_1,\ldots,cr_n)\mid\gcd(P).$$

This is true because each cr_k is a multiple of p_k . Now that we know we can obtain a generator of M from G with coefficients a_1, \ldots, a_n , we know we can obtain any element of M by just multiplying the coefficients by some constant, so $M \subseteq G$.

For the other direction, suppose we have some $a_1r_1 + \cdots + a_nr_n \in G$. That this element is in M is equivalent to the fact that following equation holds for some integer m:

$$a_1r_1 + \dots + a_nr_n = m \frac{\gcd(P)}{\operatorname{lcm}(Q)}$$

multiplying by lcm(Q), we have (for c = lcm(Q)):

$$a_1(cr_1) + \dots + a_n(cr_n) = m \gcd(P)$$

which clearly holds due to the reasoning above. Additionally, we know that dividing the left side by gcd(P) would yield an integer since each cr_k is a multiple of p_k , so there does exist an $m \in \mathbb{Z}$ such that the equation holds. Hence $G \subseteq M$, completing the proof.

The next part of the question is simple. Due to the proof above, \mathbb{Q} being finitely generated would imply that it is cyclic. Suppose this is so, and designate a generator $g \in \mathbb{Q}$. We know, by the density of \mathbb{Q} in \mathbb{R} , that there exists a rational strictly between any kg and (k+1)g, meaning that there are rationals not in $\langle g \rangle$; therefore \mathbb{Q} is not cyclic, and hence not finitely generated.

 $^{^{1}}$ https://math.stackexchange.com/questions/145346/diophantine-equations-with-multiple-variables