ANT 2024 Exercise session 1

Matilde Costa, Aalto University
matilde.costa@aalto.fi

February 29, 2024

References

- Stewart, I. and Tall, D. Algebraic Number Theory and Fermat's Last Theorem (Third Edition). Chapman and Hall. (pp. 22–34)
- Hungerford, T. W. Algebra. Vol. 73. Springer Science & Business Media (in case you are interested in reviewing some algebra)

Table of Contents

Permutation of polynomials

Let R be a ring and consider the ring of polynomials $R[t_1, \dots, t_n]$. Denote by S_n the group of permutations of $\{1, 2, \dots, n\}$. For $f \in R[t_1, \dots, t_]$ and $\pi \in S_n$, we define

$$f^{\pi}(t_1, \dots, t_n) \coloneqq f\left(t_{\pi(1), \dots, \pi(n)}\right).$$

Example

Let $f(t_1, t_2, t_2) = t_1 + t_2 t_3$ and $\pi = (123)$. Then, $f^{\pi}(t_1, t_2, t_n) = t_2 + t_1 t_3$.

Symmetric polynomials

We say $f \in R[t_1, \ldots, t_n]$ is *symmetric* if $f^\pi = f$ for all $\pi \in S_n$.

Example

- $f(t_1, \ldots, t_n) = t_1 + \ldots + t_n$ is symmetric.
- The previous example, $f(t_1, t_2, t_3) = t_1 + t_2 t_3$, is not symmetric since $f^\pi = t_2 + t_1 t_3 \neq t_1 + t_2 t_3$.

Elementary symmetric polynomials

Let $n \geq 1$. For every $1 \leq r \leq n$, the *elementary symmetric polynomial* $s_r(t_1, \ldots, t_n)$ is the sum of all possible **distinct** products of r **distinct** t_i's:

$$s_1(t_1, \ldots, t_n) = t_1 + \ldots + t_n$$
$$s_2(t_1, \ldots, t_n) = t_1 t_2 + t_1 t_3 + \ldots + t_1 t_n + t_2 t_3 + \ldots + t_{n-1} t_n$$
$$\vdots$$
$$s_n(t_1, \ldots, t_n) = t_1 \ldots t_n$$

These are called elementary for a reason: every symmetric polynomial can be written in terms of the elementary symmetric polynomials.

Elementary symmetric polynomials

Theorem (Theorem 1.12)

Let R be a ring. Every symmetric polynomial $p \in R[t_1, \ldots, t_n]$ can be written as a polynomial in $R[s_1, \ldots, s_n]$.

Sketch of proof.

$p \in R[t_1, \ldots, t_n] \implies$ monomials of p are of the form $at_1^{\alpha_1} \ldots t_n^{\alpha_n}$.

1. Order the monomials of p by a lexicographic order.
2. Since p is symmetric, the leading term of p (under the lexicographic order) is of the form $at_1^{\alpha_1} \ldots t_n^{\alpha_n}$ with $\alpha_1 \geq \ldots \geq \alpha_n$.
3. The leading term of $as_1^{k_1} \ldots s_n^{k_n} = a(t_1 + \ldots + t_n)^{k_1} \ldots (t_1 \ldots t_n)^{k_n}$ is $at_1^{k_1+\ldots+k_n} t_2^{k_2+\ldots+k_n} \ldots t_n^{k_n}$ for all positive integers $k_1, \ldots, k_n$.

Elementary symmetric polynomials

4. If we put $k_1 = \alpha_1 - \alpha_2, \ldots, k_{n-1} = \alpha_{n-1} - \alpha_n$, $k_n = \alpha_n$, the leading term of p is equal to the leading term of $as_1^{k_1} \ldots s_n^{k_n}$.
5. So consider $p_1 = p - as_1^{k_1} \ldots s_n^{k_n}$ with $k_1 = \alpha_1 - \alpha_2, \ldots,$ $k_{n-1} = \alpha_{n-1} - \alpha_n$, $k_n = \alpha_n$. The leading term of p is canceled and we get a smaller degree symmetric polynomial $p_1 \in R[t_1, \ldots, t_n]$.
6. Apply step 5 to p_1. After a finite amount m of iterations we get $p_{m+1} = p_m - g_m = 0$ for some $g_m \in R[s_1, \ldots, s_n]$.

$p_m - g_m = 0 \implies p_m \in R[s_1, \ldots, s_n]$. Note that $p_{j-1} = p_j + g_{j-1}$ with $g_{m-1} \in R[s_1, \ldots, s_n]$ so by reverse induction we conclude $p \in R[s_1, \ldots, s_n]$.

Example 1.13

$$p(t_1,t_2,t_3) = t_2^2 t_3 + t_1 t_2^2 + t_1^2 t_2 + t_2 t_3^2 + t_1 t_3^2 + t_1^2 t_3$$

1. Lexicographic order

$$p(t_1,t_2,t_3) = t_1^2 t_2 + t_1^2 t_3 + t_1 t_2^2 + t_1 t_3^2 + t_2^2 t_3 + t_2 t_3^2$$

2. leading term of p: $t_1^2 t_2$

$n=3,\ \alpha_1 = 2,\ \alpha_2 = 1,\ \alpha_3 = 0$

3. $$s_1^{k_1} s_2^{k_2} s_3^{k_3} = (t_1+t_2+t_3)^{k_1}(t_1t_2+t_1t_3+t_2t_3)^{k_2}(t_1t_2t_3)^{k_3}$$
$$= \underbrace{t_1^{k_1+k_2+k_3}\, t_2^{k_2+k_3}\, t_3^{k_3}}_{\text{leading term}} + \dots$$

4. $\alpha_1 = 2,\ \alpha_2 = 1,\ \alpha_3 = 0 \Rightarrow k_1 = 2-1 = 1,\ k_2 = 1-0 = 1,\ k_3 = 0$

$$s_1 s_2 = (t_1+t_2+t_3)(t_1t_2+t_1t_3+t_2t_3)$$
$$= \underbrace{t_1^2 t_2}_{\text{leading term}} + t_1^2 t_3 + t_1 t_2^2 + t_1 t_3^2 + 3t_1t_2t_3 + t_2^2 t_3 + t_2 t_3^2$$

5. $p_1 = p - s_1 s_2 = -3t_1t_2t_3$

Clearly, $p_1 = -3s_3$, so we conclude already

$$p = p_1 + s_1 s_2 = s_1 s_2 - 3s_3 \in R[s_1,s_2,s_3].$$

Elementary symmetric polynomials

The next corollary is important (for instance, to show that the field polynomial has coefficients in $\mathbb{Q}$, Theorem 2.5.).

Corollary (Corollary 1.14)

Consider a field extension $L : K$ and $p \in K[t]$ such that all of its zeros $\theta_1, \dots, \theta_n$ are in L. If $h(t_1, \dots, t_n) \in K[t_1, \dots, t_n]$ is a symmetric polynomial, then $h(\theta_1, \dots, \theta_n) \in K$.

Moral: Every symmetric expression on the roots of a polynomial $p \in K[t]$ is in K.

Proof of Corollary 1.14

$$p(t) = a_n t^n + \ldots + a_0 \in K[t]$$
$$= a_n (t-\theta_1)\ldots(t-\theta_n), \text{ with } \theta_i \in L$$
(check this) $$= a_n (t^n - s_1(\theta_1, \ldots, \theta_n) t^{n-1} + \ldots + (-1)^n s_n(\theta_1, \ldots, \theta_n))$$

$$\Rightarrow s_1(\theta_1, \ldots, \theta_n) = -a_{n-1} \in k,$$
$$s_2(\theta_1, \ldots, \theta_n) = a_{n-2} \in k, \ldots$$
$$s_n(\theta_1, \ldots, \theta_n) = (-1)^n a_0 \in k$$

By theorem 1.12, $h(t_1, \ldots, t_n) = g(s_1, \ldots, s_n)$ for some $g \in k[s_1, \ldots, s_n]$. Hence,

$h(\theta_1, \ldots, \theta_n) = g(s_1(\theta_1, \ldots, \theta_n), \ldots, s_n(\theta_1, \ldots, \theta_n)) \in k$ since the coefficients of g are in k and $s_i(\theta_1, \ldots, \theta_n) \in k$ $\forall\, 1 \leq i \leq n$. $\square$

Elementary symmetric polynomials

Example

Consider the field extension $\mathbb{Q}\left(\omega, \sqrt[3]{2}\right) : \mathbb{Q}$, where $\omega = e^{2\pi i/3}$. Let $p(t) = t^3 - 2 \in \mathbb{Q}[t]$. The roots of p are

$$\theta_1 = \sqrt[3]{2}, \quad \theta_2 = \omega\sqrt[3]{2}, \quad \theta_3 = \omega^2\sqrt[3]{2}.$$

By Corollary 1.14, we get that for instance

$$\theta_1\theta_2\theta_3 - \theta_1\theta_2 - \theta_1\theta_3 - \theta_2\theta_3 \in \mathbb{Q}.$$

Table of Contents

Modules

Modules are a generalization of vector spaces.

Definition (R-module)

Let R be a ring. An *R-module* (or module if R is clear) M is

- an abelian group $(M, +)$ together with
- a function $\alpha : R \times M \to M$, $\alpha(r, m) = rm$, satisfying
  - (a) $(r+s)m = rm + sm \quad \forall r, s \in R, \forall m \in M$
  - (b) $r(m+n) = rm + rn \quad \forall r \in R, \forall m, n \in M$
  - (c) $r(sm) = (rs)m \quad \forall r, s \in R, \forall m \in M$
  - (d) $1m = m \quad \forall m \in M$.

Function α is called an R-action on M.

If R is a field then M is an R-module if and only if it is a vector space over R (check this!).

Submodules and quotient modules

Definition (R-submodule)

Let M be an R-module. N is an *R-submodule* of M if

- $(N, +) \leqslant (M, +)$
- for all $n \in N$ and $r \in R$, $\alpha(r, n) = rn \in N$.

Let M be an R-module and N be an R-submodule of M. The quotient group M/N has a structure of R-module with R-action

$$r(N + m) := N + rm.$$

Some facts about modules

1. Suppose R is a subring of S. Then S is an R-module with action rs, for all $r \in R$ and $s \in S$.
2. Suppose I is an ideal of the ring R. Then I is an R-module with action ri for all $r \in R$ and $i \in I$.
3. Suppose $J \subseteq I$ are ideals of R. Then the quotient I/J is an R-module with action $r(J + i) := J + ri$.

Submodule generated by a set

Let M be an R-module. Given $X \subseteq M$ and $Y \subseteq R$,

$$YX := \left\{ \sum_{i=1}^{m} y_i x_i : x_i \in X, y_i \in Y, m \geq 1 \right\}.$$

The *R-submodule of M generated by X* is the smallest R-submodule of M containing X. We denote it by $\langle X \rangle_R$.

Fact: $\langle X \rangle_R = RX$.

If

$$N = \langle x_1, \ldots, x_n \rangle_R$$

with $x_1, \ldots, x_n \in M$, we say N is a *finitely generated* R-module.

$\mathbb{Z}$-modules

- A $\mathbb{Z}$-module is nothing more than an abelian group M (check this by taking $R = \mathbb{Z}$ in the definition of R-module).
- Given an abelian group M, we can make it into a $\mathbb{Z}$-module by defining the action recursively
  - $0m = 0 \quad \forall m \in M$
  - $1m = m \quad \forall m \in M$
  - $(n+1)m = nm + m \quad \forall m \in M$ and positive n
  - $(-n)m = -nm \quad \forall m \in M$ and positive n.

So any abelian group can be interpreted as a $\mathbb{Z}$-module and vice-versa.

Exercise 12

Let $\mathbb{Z}$ be a $\mathbb{Z}$-module with the obvious action. Find all the submodules.

Hints:

- What is the action?
- Recall what are the subgroups of $\mathbb{Z}$.

Solution

The $\mathbb{Z}$-action on $\mathbb{Z}$ is given by

$$\alpha : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$(n,m) \mapsto nm$$

The subgroups of $\mathbb{Z}$ are of the form $a\mathbb{Z}$ with $a \in \mathbb{N}$ (including $a=0$)

Since $\alpha(n, am) = nam = a(nm) \in a\mathbb{Z}$ for all $am \in a\mathbb{Z}$, we conclude that $a\mathbb{Z}$ is a $\mathbb{Z}$-submodule of $\mathbb{Z}$ for all $a \in \mathbb{N}$.

Table of Contents

Motivation

Throughout the course we will study many subrings of $\mathbb{C}$, namely rings of algebraic integers of a given subfield of $\mathbb{C}$. One example is the ring of Gaussian integers

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

As an additive group, $\mathbb{Z}[i] \cong \mathbb{Z} \times \mathbb{Z}$. Many of the subrings we will study are also isomorphic to a direct product of a finite number of copies of $\mathbb{Z}$.

Finitely generated abelian groups

Let G be an abelian group. We say G is *finitely generated* if it is finitely generated as a $\mathbb{Z}$-module, that is, if there exist $g_1, \ldots, g_n \in G$ such that

$$G = \langle g_1, \ldots, g_n \rangle_{\mathbb{Z}} = \left\{ \sum_{i=1}^{n} m_i g_i : m_i \in \mathbb{Z} \right\}.$$

We say $g_1, \ldots, g_n \in G$ are *linearly independent* over $\mathbb{Z}$ if the only solution over the integers for

$$m_1 g_1 + \ldots + m_n g_n = 0$$

is $m_1 = \ldots = m_n = 0$.

Free abelian groups

Definition ($\mathbb{Z}$-basis)

Let G be an abelian group. We say $\{g_1, \ldots, g_n\} \subseteq G$ is a *$\mathbb{Z}$-basis* for G if

- $G = \langle g_1, \ldots, g_n \rangle_{\mathbb{Z}}$
- $g_1, \ldots, g_n$ are linearly independent over $\mathbb{Z}$.

Definition (Free abelian group)

A *free abelian group* G of rank n is an abelian group with a $\mathbb{Z}$-basis of n elements.

Free abelian groups

Example

$\mathbb{Z}[i]$ is a free abelian group of rank 2 with $\mathbb{Z}$-basis $\{1, i\}$.

Facts:

1. If $\{g_1, \ldots, g_n\}$ and $\{h_1, \ldots, h_m\}$ are two $\mathbb{Z}$-basis for G then $n = m$. Hence the rank of G is well-defined, in the sense that it does not depend on the basis.
2. Every free abelian group of rank n is isomorphic to $\mathbb{Z}^n$ (consider for instance $\phi : \mathbb{Z}^n \to G$ given by $\phi(m_1, \ldots, m_n) = m_1 g_1 + \ldots + m_n g_n$, where $\{g_1, \ldots, g_n\}$ is a $\mathbb{Z}$-basis of G).

Change of basis

Lemma (Lemma 1.15)

Let G be a free abelian group of rank n with basis $\{x_1, \ldots, x_n\}$. Let $A = (a_{ij})$ be an $n \times n$ matrix with integer coefficients. Then the elements

$$y_i = \sum_{j=1}^{n} a_{ij} x_j \quad i = 1, \ldots, n$$

form a basis of G if and only if A is unimodular, that is, $\det A = \pm 1$.

Proof of lemma 1.15

"$\Rightarrow$" Suppose $y_i = \sum_{j=1}^{n} a_{ij} x_j$, $i = 1, \dots, n$, form a $\mathbb{Z}$-basis for G. Then, there exist integers b_{ij} such that

$$x_i = \sum_{j=1}^{n} b_{ij} y_j \, , \quad i = 1, \dots, n.$$

Let $B = (b_{ij})$. Then $AB = I_n$ and so $\det(A)\det(B) = 1$. Since A, B are matrices with integer coefficients, $\det(A), \det(B) \in \mathbb{Z}$. $\therefore \det(A) = \pm 1$.

"$\Leftarrow$" Suppose A is unimodular. In particular, $\det A \neq 0$, so $y_1, \dots, y_n$ are linearly independent. Moreover, $A^{-1} = (\det(A))^{-1} \tilde{A}$, where $\tilde{A}$ is the adjoint matrix of A. Note that $\tilde{A}$ has integer entries and since $\det(A) = \pm 1$, we have that A^{-1} has integer entries as well. Consider $B = A^{-1}$. Then

$$x_i = \sum_{j=1}^{n} b_{ij} y_j \, , \quad i = 1, \dots, n$$

which shows $G = \langle y_1, \dots, y_n \rangle_{\mathbb{Z}}$. $\therefore \{y_1, \dots, y_n\}$ is a $\mathbb{Z}$-basis for G. $\square$

Subgroups of free abelian groups

Theorem (Theorem 1.16)

Let G be a free abelian group of rank n and let H be a subgroup of G. Then H is a free abelian group of rank $s \leq n$. Moreover, there exists a basis of G $\{u_1, \dots, u_n\}$ and positive integers $\alpha_1, \dots, \alpha_s$ such that $\alpha_1 u_1, \dots, \alpha_s u_s$ is a basis for H.

Theorem (Theorem 1.17)

Let G be a free abelian group of rank n and H be a subgroup of G. The quotient group G/H is finite if and only if $\operatorname{rank} G = \operatorname{rank} H$. In that case, if G has a basis $\{x_1, \dots, x_r\}$ and H has a basis $\{y_1, \dots, y_r\}$ with $y_i = \sum_{j=1}^{r} a_{ij} x_j$ then

$$|G/H| = |\det(a_{ij})|.$$

Proof of Theorem 1.16 (inspired by Thm 1.16 in Stewart, but also by Thm 1.6 in Hungerford)

Induction on $n \geq 1$.

- $n=1$: $G = \langle u_1 \rangle_{\mathbb{Z}}$ for some $u_1 \in G$

  $\Rightarrow$ G is cyclic $\Rightarrow$ H is cyclic $\Rightarrow$ H is free abelian of rank 1 with $H = \langle \alpha_1 u_1 \rangle_{\mathbb{Z}}$ for some $\alpha_1 \geq 1$.
- Let $n > 1$ and suppose the statement holds for $n-1$.

If $H = \{0\}$, the theorem is trivial. So suppose $H \neq \{0\}$.

Idea: Decompose G in a direct product of a free abelian group of rank 1 and a free abelian group of rank $n-1$, G'. Then H will be also a direct product of a free abelian group of rank 1 and a subgroup H' of G'. Then, by induction hypothesis H' is free abelian of rank $s' \leq n-1$ so H is free abelian of rank $s'+1 \leq n$. Let's do that.

Let

$S = \{ s \in \mathbb{Z}$:

$\exists$ basis $\{w_1, \ldots, w_n\}$ of G s.t. $sw_1 + h_2 w_n + \ldots + h_n w_n \in H$ for some $h_i \in \mathbb{Z} \}$

($s \in S$ if s is a coefficient for an element of H)

Note that, e.g. $\{w_1, w_2, \ldots, w_n\}$ are seen as "different" basis so $h_2, \ldots, h_n$ above are in S as well. Since $H \neq \{0\}$, S contains a least positive integer α_1 and for some basis $\{w_1, \ldots, w_n\}$ of G, $\exists v_1 \in H$ s.t.

$$v_1 = \alpha_1 w_1 + \beta_2 w_n + \ldots + \beta_n w_n \,, \quad \text{with } \beta_i \in \mathbb{Z}.$$

By the division algorithm,

$$\beta_i = \alpha_1 q_i + r_i \quad \text{with } 0 \leq r_i < \alpha_1$$

$i = 2, \ldots, n$, and so

$$v_1 = \alpha_1 (w_1 + q_2 w_2 + \ldots + q_n w_n) + r_2 w_2 + \ldots + r_n w_n .$$

let $u_1 = w_1 + q_2 w_2 + \ldots + q_n w_n$. We now apply lemma 1.15. to conclude that $\{u_1, w_2, \ldots, w_n\}$ is a basis of G. Indeed, we have

$$\begin{bmatrix} u_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & q_1 & q_2 & \cdots & q_n \\ & 1 & & & 0 \\ & & \ddots & & \\ & 0 & & & 1 \end{bmatrix}}_{A} \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix}$$

where $\det(A) = 1 \Rightarrow A$ is unimodular $\Rightarrow \{u_1, w_2, \ldots, w_n\}$ is a basis of G.

Now, since $v_1 \in H$, $r_i < \alpha_1 \;\; \forall i = 2, \ldots, n$ and $\{u_1, w_1, \ldots, w_n\}$ (in any order) is a basis of G, the minimality of α_1 implies that $r_2 = \ldots = r_n = 0$. So

$$\boxed{v_1 = \alpha_1 u_1}$$

let $G' = \langle w_2, \ldots, w_n \rangle_{\mathbb{Z}}$. Then (since $w_2, \ldots, w_n$ are lin. independent) G' is a free abelian group of rank $n-1$ such that $G = \langle u_1 \rangle_{\mathbb{Z}} \times G'$.

<u>Claim</u>: $H = \langle v_1 \rangle_{\mathbb{Z}} \times (H \cap G') = \langle \alpha_1 u_1 \rangle_{\mathbb{Z}} \times H'$.

let's show the claim. Since $\{u_1, w_2, \ldots, w_n\}$ is a basis of G and $G' = \langle w_2, \dots, w_n \rangle_{\mathbb{Z}}$, it should be clear that $\langle \alpha_1 u_1 \rangle_{\mathbb{Z}} \cap (H \cap G') = \{0\}$. Now if

$$h = \gamma_1 u_1 + \gamma_2 w_2 + \dots + \gamma_n w_n \in H \quad \text{with } \gamma_i \in \mathbb{Z}$$

again by the division algorithm

$$\gamma_1 = \alpha_1 q + r_1, \quad \text{with } 0 \leq r_1 < \alpha_1.$$

Since H is a group, it contains

$$\begin{aligned} h - q v_1 &= h - \alpha_1 q u_1 \\ &= \gamma_1 u_1 - \alpha_1 q u_1 + \gamma_2 w_2 + \dots + \gamma_n w_n \\ &= r_1 u_1 + \gamma_2 w_2 + \dots + \gamma_n w_n. \end{aligned}$$

By the minimality of α_1, we get again $r_1 = 0 \Rightarrow \gamma_2 w_2 + \dots + \gamma_n w_n \in H \cap G'$

and $h = q v_1 + (\gamma_2 w_2 + \dots + \gamma_n w_n) \in \langle v_1 \rangle_{\mathbb{Z}} + (H \cap G')$.

This proves that $H = \langle v_1 \rangle_{\mathbb{Z}} \times (H \cap G')$.

Now, $H' = H \cap G' \leq G'$. By induction, H' is free abelian of rank $s' \leq n-1$ and there exist bases $\{u_2, \dots, u_n\}$ of G' and $\{v_2, \dots, v_s\}$ of H' s.t. $\boxed{v_i = \alpha_i u_i}$ for positive integers α_i. Since $G = \langle u_1 \rangle_{\mathbb{Z}} \times G'$ and $H = \langle \alpha_1 u_1 \rangle_{\mathbb{Z}} \times H'$, it follows that H is free abelian of rank $s'+1 \leq n$, $\{u_1, \dots, u_n\}$ is a basis for G and $\{v_1, \dots, v_s\}$ is a basis of H with $v_i = \alpha_i u_i$, $\alpha_i \geq 1$. $\square$

Remark: We can say more: in fact, $\alpha_1 | \alpha_2 | \dots | \alpha_n$ (the bar means "divides"). See Theorem 1.6 in Hungerford, if interested.

Proof of Theorem 1.17

Suppose G has rank r and H has rank s. By Theorem 1.16, let $\{u_1, \dots, u_r\}$ and $\{v_1, \dots, v_s\}$ be basis of G and H, respectively, s.t. $v_i = \alpha_i u_i$ for some positive integers. Since $G \cong \mathbb{Z}^r$, we have

$$G/H \cong \underbrace{\left(\mathbb{Z}^s / \alpha_1 \mathbb{Z} \times \dots \times \alpha_s \mathbb{Z}\right)}_{\text{finite part}} \times \underbrace{\mathbb{Z}^{r-s}}_{\text{infinite part}}$$

so G/H is finite iff $r-s=0 \Rightarrow r=s$. In that case, $|G/H| = \alpha_1 \dots \alpha_n$. Moreover, $\forall i = 1, \dots, n$,

$$y_i = \sum_{j=1}^{n} d_{ij} v_j \quad \text{(change of basis)}$$

$$v_i = \sum_{j=1}^{n} c_{ij} u_j \quad \text{(Thm 1.16)}$$

$$u_i = \sum_{j=1}^{n} b_{ij} x_j \quad \text{(change of basis)}$$

where $B = (b_{ij})$ and $D = (d_{ij})$ are unimodular by lemma 1.15 and

$$C = (c_{ij}) = \begin{bmatrix} \alpha_1 & & 0 \\ & \alpha_2 & \\ & & \ddots \\ 0 & & & \alpha_n \end{bmatrix}$$

If $A = (a_{ij})$, since $y_i = \sum_{j=1}^{n} a_{ij} x_j$, $i = 1, \dots, n$, we have $A = BCD$ and hence

$$\det(A) = \det(B)\det(C)\det(D) = (\pm 1)(\alpha_1 \dots \alpha_n)(\pm 1)$$
$$= \pm \alpha_1 \dots \alpha_n$$

$\Rightarrow |\det(A)| = |\alpha_1 \dots \alpha_n| = |G/H|$. $\square$

Exercise 10

Find the order of the groups G/H where G is free abelian with $\mathbb{Z}$-basis x, y, z and H is generated by:

(a) $2x, 3y, 7z$

(b) $x + 3y - 5z, 2x - 4y, 7x + 2y - 9z$

(c) x

(d) $41x + 32y - 999z, 16y + 3z, 2y + 111z$

(e) $41x + 32y - 999z$.

Exercise 10

a) $H = \langle 2x, 3y, 7z \rangle_{\mathbb{Z}}$. By Theorem 1.17,

$$|G/H| = \left| \det \begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 7 \end{bmatrix} \right| = 42$$

c) $H = \langle x \rangle_{\mathbb{Z}} \Rightarrow \operatorname{rank} H = 1 < 3 = \operatorname{rank} G$

$\Rightarrow G/H$ is infinite.

Linearly dependent generators

Theorem (Proposition 1.18)

Every finitely generated abelian group G with n generators satisfies

$$G \cong F \times B,$$

where F is a finite abelian group and B is a free abelian group of rank $k \leq n$.

Theorem (Proposition 1.19)

Every subgroup of a finitely generated group is also finitely generated.

Proof of Proposition 1.18

Let $G = \langle w_1, \dots, w_n \rangle_{\mathbb{Z}}$ where $w_1, \dots, w_n$ are not necessarily independent. Consider

$$f : \mathbb{Z}^n \to G$$

given by $f(m_1, \dots, m_n) = m_1 w_1 + \dots + m_n w_n$. f is surjective since $w_1, \dots, w_n$ generate G. Thus

$$G \cong \mathbb{Z}^n / H$$

where $H = \ker f \leq \mathbb{Z}^n$. By Theorem 1.16, H is free abelian of rank $s \leq n$. By the same theorem, choose a basis $\{u_1, \dots, u_n\}$ of $\mathbb{Z}^n$ in such a way that $\alpha_1 u_1, \dots, \alpha_s u_s$ is a basis for H, with $\alpha_1, \dots, \alpha_s$ positive integers. Let

$$A = \langle u_1, \dots, u_s \rangle_{\mathbb{Z}} \quad \text{and} \quad B = \langle u_{s+1}, \dots, u_n \rangle_{\mathbb{Z}}.$$

Then

$$G \cong (A/H) \times B$$

where A/H is a finite abelian group and B is a free abelian group of rank $k = n - s$. $\square$

Proof of Proposition 1.19

Let $K \leq G$. Writing $G \cong F \times B$ as in Proposition 1.18, we have that $K \cong (F \cap K) \times H$ where $H \leq B$. Then, $F \cap K$ is a finite abelian group ($\Rightarrow$ finitely generated) and by theorem 1.16, H is a free abelian group ($\Rightarrow$ finitely generated). $\therefore$ K is finitely generated.

Exercise 14

An abelian group G is said to be *torsion-free* if $g \in G$, $g \neq 0$ and $kg = 0$ for $k \in \mathbb{Z}$ implies $k = 0$. Prove that a finitely generated torsion-free abelian group is a finitely generated free group.

Hints:

- Proposition 1.18