Math 121 Homework 5: Notes on Selected Problems

12.1.2. Let M be a module over the integral domain R.

(a) Assume that M has rank n and that $x_1, \ldots, x_n$ is any maximal set of linearly independent elements of M. Prove that N is isomorphic to R^n and that the quotient M/N is a torsion R-module.

(b) Prove conversely that if M contains a submodule N that is free of rank n (i.e., $N \cong R^n$) such that the quotient M/N is a torsion R-module then M has rank n.

Solution.

(a) Write $e_1, \ldots, e_n$ for the standard basis of R^n. The R-linear map $R^n \to N$ given by $e_i \mapsto x_i$ is injective by independence of the set $x_1, \ldots, x_n$ and surjective by definition of N. For any x in M, $x, x_1, \ldots, x_n$ is R-linearly dependent by maximality so we can write an R-linear dependence

$$ax + a_1x_1 + \cdots + a_nx_n = 0$$

for $a, a_1, \ldots, a_n$ in R not all zero. Since $x_1, \ldots, x_n$ are R-linearly independent, a is nonzero. Therefore the image of x in M/N is R-torsion, being killed by the nonzero element a of R.

(b) If N is free on $x_1, \ldots, x_n$, then $x_1, \ldots, x_n$ is an R-linearly independent set of elements of M so the rank of M is at least n. Let $y_1, \ldots, y_{n+1}$ be elements of M. Since M/N is torsion, for each i there exists a nonzero a_i in R such that a_iy_i is in N. Then since N is free of rank n, there exists a nontrivial R-linear dependence among $a_1y_1, \ldots, a_{n+1}y_{n+1}$, which gives a nontrivial R-linear dependence among $y_1, \ldots, y_{n+1}$ since the a_i are nonzero and hence not zero divisors as R is an integral domain. Therefore the rank of M is precisely n. (Instead of appealing to the fact that $n+1$ elements in a free module of rank n over a commutative ring with identity must be dependent—proved in the text in the case that R is a domain—one may also, as indicated in the hint, imitate/repeat either of the proofs.) $\square$

12.1.5. Let $R = \mathbf{Z}[x]$ and let $M = (2, x)$ be the ideal generated by 2 and x, considered as a submodule of R. Show that $\{2, x\}$ is not a basis of M. Show that the rank of M is 1, but that M is not free of rank 1.

Solution. The set $\{2, x\}$ is not a basis of M because it is not $\mathbf{Z}[x]$-linearly independent: $(-x) \cdot 2 + 2 \cdot x = 0$ is a nontrivial $\mathbf{Z}[x]$-linear

dependence. In fact, for any $p(x)$ and $q(x)$ in M, either both of $p(x)$ and $q(x)$ are zero or $(-q(x)) \cdot p(x) + p(x) \cdot q(x) = 0$ is a nontrivial $\mathbf{Z}[x]$-linear dependence. Therefore M does not contain any independent sets with more than one element. Any nonzero element in M is non-torsion, however, so M has rank at least 1. Therefore M has rank precisely 1.

To show that M is not free of rank 1 it suffices to show that no element of M principally generates M. Let $r(x)$ be an element of M so that $r(x)\mathbf{Z}[x]$ contains 2, that is $r(x)$ divides 2. By degree considerations, $r(x)$ is a constant polynomial, which must be equal to some integral multiple of 2. Then x is not divisible by $r(x)$. Therefore $r(x)\mathbf{Z}[x]$ does not contain x and so is a proper $\mathbf{Z}[x]$-submodule of M. Finally, M is not a principal $\mathbf{Z}[x]$-module and hence not free of rank 1. □

12.1.20. Let R be an integral domain with quotient field F and let M be any R-module. Prove that the rank of M equals the dimension of the vector space $F \otimes_R M$ over F.

Proof. We shall assume that the kernel of $M \to F \otimes_R M$ is the torsion submodule of M. This is proved in several ways in the comment and note below.

We first show that every element of $F \otimes_R M$ is an F-multiple of a simple tensor in the image of $M \to F \otimes_R M$. This is true of simple tensors in $F \otimes_R M$: an arbitrary simple tensor $\frac{a}{b} \otimes m$ either has $\frac{a}{b} = 0$ so can be written as $0(1 \otimes m)$ or otherwise can be written as

$$\tfrac{a}{b} \otimes m = a(\tfrac{1}{b} \otimes m) = \tfrac{a}{b} b(\tfrac{1}{b} \otimes m) = \tfrac{a}{b}(1 \otimes m).$$

The set of F-multiples of elements in the image of $M \to F \otimes_R M$ is also closed under addition

$$\begin{aligned} \tfrac{a_1}{b_1}(1 \otimes m_1) + \tfrac{a_2}{b_2}(1 \otimes m_2) &= \tfrac{1}{b_1 b_2}(b_2 a_1 (1 \otimes m_1) + b_1 a_2 (1 \otimes m_2) \\ &= \tfrac{1}{b_1 b_2}(1 \otimes (b_2 a_1 m_1 + b_1 a_2 m_2)) \end{aligned}$$

so the general case follows. Now consider an F-linearly independent set in $F \otimes_R M$, which by the above we may write as $\{f_i(1 \otimes m_i)\}$. Then $\{1 \otimes m_i\}$ is also an F-linearly independent set in $F \otimes_R M$. We claim that $\{m_i\}$ is an R-linearly independent set in M. Assume that for each i there is r_i in R, all but finitely many zero, such that $\sum r_i m_i = 0$. Then $\sum r_i(1 \otimes m_i) = 0$. By independent of $\{1 \otimes m_i\}$, $r_i = 0$ for each i. This proves that $\{m_i\}$ is R-linearly independent.

Conversely, let $\{m_i\}$ be an R-linearly independent subset of M. We claim that $\{1 \otimes m_i\}$ is an F-linearly independent subset of $F \otimes_R M$.

Assume that for each i there is f_i in F, all but finitely many zero, such that $\sum f_i(1 \otimes m_i) = 0$. Multiplying out denominators for the finitely many nonzero coefficients gives that $\sum r_i(1 \otimes m_i) = 0$ where each r_i is a nonzero multiple of f_i. Therefore $1 \otimes \sum r_i m_i = 0$. Since the kernel of $M \to F \otimes_R M$ consists of torsion elements, there is a nonzero r in R such that $\sum r r_i m_i = 0$. By R-linear independence, for each i we have $r r_i = 0$, but r is nonzero so $r_i = 0$. It follows that each f_i is a zero divisor and hence equal to zero. This proves F-linear independence of $\{1 \otimes m_i\}$.

Given an R-linearly independent subset of M, we demonstrated an F-linearly independent subset of $F \otimes_R M$ of the same cardinality, and the other way around. Therefore the R-rank of M is the same as the F-dimension of $F \otimes_R M$. □

Comment. The harder part is showing that the F-dimension of $F \otimes_R M$ is at least the rank of M. The main difficulty is showing that $1 \otimes m = 0$ in $F \otimes_R M$ implies that m in M is R-torsion. We illustrate a proof of this.

Let $N' \hookrightarrow N$ be an inclusion of R-modules. We show that any R-bilinear map $\varphi' : F \times N' \to F$ extends to an R-bilinear map $\varphi : F \times N \to F$. Assume first that N is generated over N' by a single element n. If $Rn \cap N' = 0$ so $N = N' \oplus Rn$, we set $\varphi(f, n) = 0$ for all f in F and extend linearly. If $Rn \cap N' \neq 0$, then there is a nonzero r in R and n' in N' so that $rn = n'$, and then we set $\varphi(f, n) = r^{-1}\varphi'(f, n')$ for all f in F and extend linearly. Inductively we have proved the existence of extensions when N is finitely generated over N', and the general case follows from Zorn's lemma.

Now consider a non-torsion element m of M. Then Rm is a free R-module on $\{m\}$, and $Rm \otimes_R F$ is a free F-module on $\{m \otimes 1\}$. Since $m \otimes 1$ is not zero in $Rm \otimes_R F$, there exists an R-bilinear map $Rm \times F \to F$ that does not kill $(m, 1)$. An extension to an R-bilinear map of $M \times F \to F$ exists, and by virtue of being an extension also does not kill $(m, 1)$. Therefore $m \otimes 1$ is nonzero in $M \otimes_R F$. □

Note. Alternatively, one may use the "module of fractions", which is defined as an R-module homomorphism $M \to M_F$ with codomain some F-module M_F that is universal, meaning that any R-module homomorphism $M \to Z$ with codomain an F-module factors uniquely through $M \to M_F$. (Every F-module is an R-module via "restriction of scalars" $R \to F$.) A realization of M_F is as follows: As a set M_F is the set of equivalence classes of $M \times (R \setminus 0)$ with the equivalence relation $(m, s) \sim (m', s')$ if and only if there exists s'' in $R \setminus 0$ such that $s''(s'm - sm') = 0$. Denoting the equivalence class of (m, s) by $\frac{m}{s}$ may

help in understanding the definition; we will simply write $[(m,s)]$ for the equivalence class of (m,s). The set map $M \to M_F$ sending m to the equivalence class of $(m,1)$ will be an R-module homomorphism when M_F has the following F-module structure: the zero element is $[(0,1)]$ and addition is given by

$$[(m,s)] + [(m',s')] = [(s'm + sm', ss')]$$

and the action of F is given by

$$\tfrac{r'}{s'}[(m,s)] = [(r'm, s's)].$$

Having discussed the module of fractions M_F, we now return to the original question by showing that $1 \otimes m$ is zero in $F \otimes_R M$ only if m is R-torsion. An R-bilinear map $M \times F \to M_F$ is given as the composition of $F \times M \to F \times M_F$ that is the identity in the second component followed by the F-action, which is a map $F \times M_F \to M_F$. The bilinear map induces an R-linear map $M \otimes_R F \to M_F$ (which is in fact an isomorphism) taking $m \otimes 1$ to $[(m,1)]$. By definition of the equivalence relation, $(m,1) \sim (0,1)$ if and only if there exists a nonzero r in R such that $rm = 0$, that is if and only if m is torsion. In particular, $m \otimes 1$ has nonzero image in M_F when m is not torsion. Therefore $m \otimes 1$ is not zero when m is not torsion.

Note. Another alternative to the first proof, which extended bilinear maps, is to use the adjoint property of the tensor product. We prove the following lemma (which was implicitly proved above).

Lemma. Let R be an integral domain and let F be the fraction field of R. Then for any inclusion of R-modules $N' \hookrightarrow N$, the corresponding map $N' \otimes_R F \to N \otimes_R F$ is injective.

Proof. Any R-linear map $N' \to F$ can be extended to an R-linear map $N \to F$ as follows. For any n in N, either $Rn \cap N' = 0$ in which case the extension may send n anywhere, or there is a nonzero r in R such that $rn = n'$ for some n' in N', in which case we send n to $1/r$ times the image of n'. This allows us to create the extension in steps; when N is not finitely generated over N' we invoke Zorn's lemma. Hence the natural R-linear map $\mathrm{Hom}_R(N,F) \to \mathrm{Hom}_R(N',F)$ is surjective.

We now show that the natural F-linear map

$$\mathrm{Hom}_F(N \otimes_R F, F) \to \mathrm{Hom}_F(N' \otimes_R F, F)$$

is surjective.[1] Let $\varphi\colon N' \otimes_R F \to F$ be an F-linear map. Then an R-linear map $N' \to F$ is given by $n' \mapsto \varphi(n' \otimes 1)$. Choose an extension α to an R-linear map $N \to F$. The R-bilinear map $N \times F \to F$ given by $(n, f) \mapsto \alpha(n)f$ induces an R-linear map $N \otimes_R F \to F$ whose image in $\mathrm{Hom}_R(N' \otimes_R F, F)$ satisfies

$$\begin{aligned} n' \otimes \tfrac{a}{b} \mapsto \alpha(n')\tfrac{a}{b} = \varphi(n' \otimes 1)\tfrac{a}{b} &= \varphi\big((n' \otimes 1)\tfrac{a}{b}\big) \\ &= \varphi\big((n' \otimes \tfrac{a}{b}b)\tfrac{1}{b}\big) = \varphi(n' \otimes \tfrac{a}{b}) \end{aligned}$$

for n' in N' and a in R and nonzero b in R, and therefore equals φ. We have proved that every element of $\mathrm{Hom}_F(N' \otimes_R F, F)$ comes from an element of $\mathrm{Hom}_F(N \otimes_R F, F)$.

If x in $N \otimes_R F$ is nonzero, there exists an F-linear map $N \otimes_R F \to F$ that does not kill x, and hence there exists an F-linear map $N' \otimes_R F \to F$ not killing the image of x in $N' \otimes_R F$. Consequently the natural map $N' \otimes_R F \to N \otimes_R F$ is injective. □

Problem 2. Find, with proof, a free basis for the subgroup of $\mathbf{Z}^4$ defined by the constraint $\{(x, y, z, w) \in \mathbf{Z}^4 : 11x + 8y + 3z - 9w = 0\}$.

Solution. Define a $\mathbf{Z}$-linear map $\rho\colon \mathbf{Z}^4 \to \mathbf{Z}$ by

$$\rho(x, y, z, w) = 11x + 8y + 3z - 9w.$$

Using the Euclidean algorithm we may find a preimage of 1 under ρ, for example $\rho(3, -4, 0, 0) = 1$. Then we may define a section $\iota\colon \mathbf{Z} \to \mathbf{Z}^4$ of ρ as the unique $\mathbf{Z}$-linear map sending 1 to $(3, -4, 0, 0)$. If $\iota(x)$ is in $\ker\rho$, then $x = \rho \circ \iota(x) = 0$ so $\iota(x) = 0$. Therefore $\ker\rho$ and $\mathrm{im}\,\iota$ intersect trivially. Any $\mathbf{x}$ in $\mathbf{Z}^4$ can be written as $\mathbf{x} = (\mathbf{x} - \iota \circ \rho(\mathbf{x})) + \iota \circ \rho(\mathbf{x})$, but $\mathbf{x} - \iota \circ \rho(\mathbf{x})$ is in $\ker\rho$ and $\iota \circ \rho(\mathbf{x})$ is in $\mathrm{im}\,\iota$. Thus $\mathbf{Z}^4$ is the internal direct sum of $\ker\rho$ and $\mathrm{im}\,\iota$. Then

$$\mathrm{im}(\mathbb{1}_{\mathbf{Z}^4} - \iota \circ \rho) = \ker\rho \qquad \text{and} \qquad \ker(\mathbb{1}_{\mathbf{Z}^4} - \iota \circ \rho) = \mathrm{im}\,\iota.$$

Hence $\ker\rho$ has the following presentation: generators

$$\begin{aligned} v_1 &= (\mathbb{1}_{\mathbf{Z}^4} - \iota \circ \rho)(1, 0, 0, 0) = (-32, 44, 0, 0) \\ v_2 &= (\mathbb{1}_{\mathbf{Z}^4} - \iota \circ \rho)(0, 1, 0, 0) = (-24, 33, 0, 0) \\ v_3 &= (\mathbb{1}_{\mathbf{Z}^4} - \iota \circ \rho)(0, 0, 1, 0) = (-9, 12, 1, 0) \\ v_4 &= (\mathbb{1}_{\mathbf{Z}^4} - \iota \circ \rho)(0, 0, 0, 1) = (27, -36, 0, 1) \end{aligned}$$

[1] This follows directly from the natural F-linear isomorphism between F and $\mathrm{Hom}_F(F, F)$ and adjointness: for any R-module E there is a natural bijection

$$\mathrm{Hom}_R(E, \mathrm{Hom}_F(F, F)) \leftrightarrow \mathrm{Hom}_F(E \otimes_R F, F),$$

but we will argue directly.

with the only relations among the v_i being multiples of $3v_1 - 4v_2 = 0$ (which is obtained from the choice of section ι). In other words, $\ker \rho$ has presentation matrix

	v_1	v_2	v_3	v_4
1st relation	3	-4	0	0

Replacing v_1 with $v_1 - v_2$ gives the presentation matrix

	$v_1 - v_2$	v_2	v_3	v_4
1st relation	3	-1	0	0

Replacing v_2 with $v_2 - 3(v_1 - v_2)$ gives the presentation matrix

	$v_1 - v_2$	$-3v_1 + 4v_2$	v_3	v_4
1st relation	0	-1	0	0

or equivalently

	$3v_1 - 4v_2$	$v_1 - v_2$	v_3	v_4
1st relation	1	0	0	0

Finally, a free basis for $\ker \rho$ is given by

$$\begin{aligned} v_1 - v_2 &= (-8, 11, 0, 0) \\ v_3 &= (-9, 12, 1, 0) \\ v_4 &= (27, -36, 0, 1). \end{aligned}$$

□

Note. One method to find integer kernels in general is (to use Hermite normal form) as follows. We use elementary integer column operations to transform $\begin{bmatrix} 11 & 8 & 3 & -9 \end{bmatrix}$ to its Hermite normal form:

$$\begin{bmatrix} 11 & 8 & 3 & -9 \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} 11 & -1 & 3 & -9 \end{bmatrix} = \begin{bmatrix} 11 & 8 & 3 & -9 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -3 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} 0 & -1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 11 & -1 & 3 & -9 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 11 & 1 & 3 & -9 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

that is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 11 & 8 & 3 & -9 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 11 & 3 & -9 \\ 3 & -33 & -8 & 27 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

where

$$U = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 11 & 3 & -9 \\ 3 & -33 & -8 & 27 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

is unimodular because it is a composition of matrices corresponding to elementary integer operations. In particular we see that the list

$$\mathscr{B} = \left(\begin{bmatrix} 1 \\ 11 \\ -33 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \\ -8 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -9 \\ 27 \\ 1 \end{bmatrix} \right)$$

of three elements of $\mathbf{Z}^4$, which corresponds to the last 3 columns of U, consists of elements in the kernel of $\begin{bmatrix} 11 & 8 & 3 & -9 \end{bmatrix}$. Conversely assume that $\begin{bmatrix} a_1 & a_2 & a_3 & a_4 \end{bmatrix}^{\text{transpose}}$ in $\mathbf{Z}^4$ is in the kernel of $\begin{bmatrix} 11 & 8 & 3 & -9 \end{bmatrix}$. Then

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 11 & 3 & -9 \\ 3 & -33 & -8 & 27 \\ 0 & 0 & 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix}$$

is in the kernel of $\begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}$. Thus we may write

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 11 & 3 & -9 \\ 3 & -33 & -8 & 27 \\ 0 & 0 & 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} = \begin{bmatrix} 0 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix}$$

where necessarily b_1, b_3, b_4 are integers since U^{-1} has integral coefficients. Therefore

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} = b_2 \begin{bmatrix} 1 \\ 11 \\ -33 \\ 0 \end{bmatrix} + b_3 \begin{bmatrix} 0 \\ 3 \\ -8 \\ 0 \end{bmatrix} + b_4 \begin{bmatrix} 0 \\ -9 \\ 27 \\ 1 \end{bmatrix}$$

is in the $\mathbf{Z}$-span of $\mathscr{B}$. Finally we have proved that $\mathscr{B}$ is a basis for the kernel of $\begin{bmatrix} 11 & 8 & 3 & -9 \end{bmatrix}$.

In general, to find a basis for the kernel of an integer matrix M, we find a unimodular matrix U such that MU is in Hermite normal form, whose kernel is the span of the elementary basis vectors corresponding to 'non-pivot columns'. The images under left multiplication by U of these elementary basis vectors is then a basis for the kernel of M.

Problem 3. In this exercise we give a direct proof that a submodule of a free module is free in the case of the ring $\mathbf{Z}$.

Let $K \subseteq \mathbf{Z}^m$. Let $K_{\mathbf{Q}}$ be the $\mathbf{Q}$-subspace spanned by K; let r be the dimension of $K_{\mathbf{Q}}$, and let ω be an alternating r-form on $K_{\mathbf{Q}}$.

- Prove that there exists a rational number q so that $\omega(v_1, \ldots, v_r)$ is in $q\mathbf{Z}$ whenever $v_1, \ldots, v_r \in K$.
- Let $x_1, \ldots, x_r \in K$ be chosen to minimize $|\omega(x_1, \ldots, x_r)|$ among nonzero values. (In words, the volume of the parallelepiped that the x_i span is as small as possible.) Prove that K is free on $x_1, \ldots, x_r$.

Solution. The space of alternating r-forms on the r-dimensional vector space $K_{\mathbf{Q}}$ has dimension 1 so we may choose ω to be a nonzero alternating r-form on $K_{\mathbf{Q}}$. Write e_i for the ith standard basis vector in $\mathbf{Z}^n$ that has 1 in the ith component and zeros elsewhere and set

$$E = \{e_1, \ldots, e_n\}.$$

Then $E^{\times r}$ is a finite set so $\omega(E^{\times r})$ is a finite subset of $\mathbf{Q}$ and hence there exists a rational number q so that $\omega(E^{\times r}) \subseteq q\mathbf{Z}$. Then by linearity $\omega((\mathbf{Z}^n)^{\times r}) \subseteq q\mathbf{Z}$, but $K^{\times r} \subseteq (\mathbf{Z}^n)^{\times r}$ so $\omega(v_1, \ldots, v_r)$ is in $q\mathbf{Z}$ whenever $v_1, \ldots, v_r$ are in K.

Now choose $x_1, \ldots, x_r$ in K so that $\omega(x_1, \ldots, x_r)$ has minimal absolute value among nonzero values of ω restricted to $K \times \cdots \times K$. That $\omega(x_1, \ldots, x_r)$ is nonzero immediately implies that $x_1, \ldots, x_r$ are $\mathbf{Q}$-linearly independent, hence a $\mathbf{Q}$-basis for $K_{\mathbf{Q}}$, and in particular independent over $\mathbf{Z}$. Let λ_i be the $\mathbf{Q}$-linear functional on $K_{\mathbf{Q}}$ that sends x in $K_{\mathbf{Q}}$ to the value obtained by replacing x_i by x in the expression $\omega(x_1, \ldots, x_r)$, which is just $\omega(x_1, \ldots, x_r)$ times the dual basis element corresponding to x_i. Therefore the map

$$x \mapsto \sum \frac{\lambda_i(x)}{\omega(x_1, \ldots, x_r)} x_i$$

is the identity of $K_{\mathbf{Q}}$. For d an integer such that $\omega(K^{\times r}) \subseteq \frac{1}{d}\mathbf{Z}$, we may write $\omega(x_1, \ldots, x_r) = a/d$ for some integer a. Consider an index i and assume x satisfies $\lambda_i(x) = b/d$. Then there exist integers r and s so that $ra + sb = \gcd(a, b)$ and so $\lambda(rx_i + sx) = \gcd(a, b)/d$. By

minimality, it follows that $|a| \leq \gcd(a,b)$ and so a divides b. This proves that $\lambda_i(K) \subseteq \omega(x_1,\ldots,x_r)\mathbf{Z}$. Consequently for x in K,

$$x = \sum \frac{\lambda_i(x)}{\omega(x_1,\ldots,x_r)} x_i$$

is an expression for x as a $\mathbf{Z}$-linear combination of $x_1,\ldots,x_r$. Therefore $x_1,\ldots,x_r$ is a free $\mathbf{Z}$-basis for K. □

Problem 4. Let $v = (x,y,z)$ and $v' = (x',y',z')$ be elements of $\mathbf{Z}^3$. Show that v, v' are be extended to a basis if and only if $\gcd(xy' - yx', xz' - zx', yz' - zy') = 1$.

Solution. The vector $v'' = (x'',y'',z'')$ extends v, v' to a basis if and only if

$$\det \begin{pmatrix} x & y & z \\ x' & y' & z' \\ x'' & y'' & z'' \end{pmatrix}$$

is a unit in $\mathbf{Z}$. The units in $\mathbf{Z}$ are ± 1 so, by the cofactor expansion, the latter is equivalent the existence of x'', y'', z'' in $\mathbf{Z}$ such that

$$x''(yz' - zy') - y''(xz' - zx') + z''(xy' - yx') = \pm 1,$$

which is the statement that $\gcd(xy' - yx', xz' - zx', yz' - zy') = 1$. The result follows. □

Problem 5. How many subgroups $K \subseteq \mathbf{Z}^3$ have the property that $\mathbf{Z}^3/K$ is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^3$? For how many K is $\mathbf{Z}^3/K$ isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$?

Solution. The group $\mathrm{GL}(\mathbf{Z}^n)$ of group automorphisms of $\mathbf{Z}^n$ acts on subgroups of $\mathbf{Z}^n$. If K is a subgroup of $\mathbf{Z}^n$ and ϕ is an automorphism of $\mathbf{Z}^n$, then $\mathbf{Z}^n/K$ is isomorphic to $\mathbf{Z}^n/\phi(K)$. Conversely, assume that K_1 and K_2 are subgroups of $\mathbf{Z}^n$ such that $\mathbf{Z}^n/K_1$ and $\mathbf{Z}^n/K_2$ are isomorphic to each other. For each i there is a basis $v_{i,1},\ldots,v_{i,n}$ of $\mathbf{Z}^n$ and integers $a_{i,1},\ldots,a_{i,\ell_i}$ (for some ℓ_i with $0 \leq \ell_i \leq n$) such that $a_{i,1}v_{i,1},\ldots,a_{i,\ell_i}v_{i,\ell_i}$ is basis of K_i. Then $\ell_1 = \ell_2$ and after reordering if necessary $a_{1,j} = a_{2,j}$ for each j. The automorphism $v_{1,j} \mapsto v_{2,j}$ of $\mathbf{Z}^n$ sends K_1 to K_2, and in particular K_1 and K_2 are conjugates under the action of $\mathrm{GL}(\mathbf{Z}^n)$. We have proved that for any subgroup K_0 of $\mathbf{Z}^n$, $\mathrm{GL}(\mathbf{Z}^n)$ acts transitively on the collection of subgroups K of $\mathbf{Z}^n$ such that $\mathbf{Z}^n/K$ is isomorphic to $\mathbf{Z}^n/K_0$. Therefore the set of such subgroups is in bijective correspondence with the collection of cosets in $\mathrm{GL}(\mathbf{Z}^n)$ of the stabilizer of K_0.

Let K_0 be the subgroup $2\mathbf{Z}^3$ of $\mathbf{Z}^3$, which satisfies $\mathbf{Z}^3/K_0 \cong (\mathbf{Z}/2\mathbf{Z})^3$. Note that K_0 is a characteristic subgroup (because it is fully invariant) so the stabilizer of K_0 is all of $\mathrm{GL}(\mathbf{Z}^3)$. Hence there is precisely one subgroup K of $\mathbf{Z}^3$ such that $\mathbf{Z}^3/K \cong (\mathbf{Z}/2\mathbf{Z})^3$.

Let K_0 be the subgroup of $\mathbf{Z}^3$ generated by $(2,0,0)$, $(0,4,0)$, and $(0,0,8)$, which satisfies $\mathbf{Z}^3/K_0 \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$. If the matrix

$$\begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix}$$

represents an automorphism ϕ of $\mathbf{Z}^3$ with respect to the standard basis, then the condition that $\phi(K_0) = K_0$ (equivalently $\phi(K_0) \subseteq K_0$) is that

$$2\begin{pmatrix} c_{11} \\ c_{21} \\ c_{31} \end{pmatrix}, 4\begin{pmatrix} c_{12} \\ c_{22} \\ c_{32} \end{pmatrix}, 8\begin{pmatrix} c_{13} \\ c_{23} \\ c_{33} \end{pmatrix} \in \begin{pmatrix} 2\mathbf{Z} \\ 4\mathbf{Z} \\ 8\mathbf{Z} \end{pmatrix},$$

that is $2 \mid c_{21}$, $2 \mid c_{32}$, and $4 \mid c_{31}$. Thus the subgroup H of $G = \mathrm{GL}_3(\mathbf{Z})$ whose lower left coefficients satisfy the above divisibility conditions is the isotropy subgroup of K_0 under the action of G. We wish to calculate the order of G/H. The kernel of the surjective[2] group homomorphism

$$\mathrm{GL}_3(\mathbf{Z}) \to \mathrm{GL}_3(\mathbf{Z}/4\mathbf{Z}),$$

is a normal subgroup of $\mathrm{GL}_3(\mathbf{Z})$ contained in H. The above homomorphism then identifies G/H as the quotient of $\mathrm{GL}_3(\mathbf{Z}/4\mathbf{Z})$ by the image $\overline{H}$ of H in $\mathrm{GL}_3(\mathbf{Z}/4\mathbf{Z})$:

$$\begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ 0 & c_{32} & c_{33} \end{pmatrix}$$

in $\mathrm{GL}_3(\mathbf{Z}/4\mathbf{Z})$ with $2 \mid c_{21}$ and $2 \mid c_{32}$. One can check that $\overline{H}$ is precisely determined by the conditions $c_{21}, c_{32} \in \{0,2\}$ and $c_{11}, c_{22}, c_{33} \in \{-1,+1\}$. Therefore the cardinality of $\overline{H}$ is $2^5 \cdot 4^3 = 2^{11}$.

The surjective[3] homomorphism

$$\mathrm{GL}_3(\mathbf{Z}/4\mathbf{Z}) \to \mathrm{GL}_3(\mathbf{Z}/2\mathbf{Z})$$

[2]Surjectivity follows, for example, by factoring into a unimodular times a diagonal times a unimodular, and then noting that every unit in $\mathbf{Z}/4\mathbf{Z}$ has a lift to a unit of $\mathbf{Z}$, something that is only true for $\mathbf{Z}/2^a3^b\mathbf{Z}$ with $a \le 2$ and $b \le 1$ and at least one inequality strict. In general the image under reduction modulo n is the subgroup of diagonal matrices with diagonal entries in $(\mathbf{Z}/n\mathbf{Z})^\times$ along with all possible left and right translates by unimodular matrices.

[3]Reduction $\mathbf{Z}/p^{r+1}\mathbf{Z} \to \mathbf{Z}/p^r\mathbf{Z}$ always induces a surjective map on invertible matrices because every lift of a unit in $\mathbf{Z}/p^r\mathbf{Z}$ is a unit in $\mathbf{Z}/p^{r+1}\mathbf{Z}$.

has kernel the set of

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix}$$

for which $2 \mid c_{ij}$ for all i and j, which has order 2^9. Since $\mathrm{GL}_3(\mathbf{Z}/2\mathbf{Z})$ has order $(2^3 - 2^0)(2^3 - 2^1)(2^3 - 2^2) = 2^3 \cdot 3 \cdot 7$, it follows that $\mathrm{GL}_3(\mathbf{Z}/4\mathbf{Z})$ has order $2^{12} \cdot 3 \cdot 7$. Consequently the index of $\overline{H}$ in $\mathrm{GL}_3(\mathbf{Z}/4\mathbf{Z})$ is $2^{12} \cdot 3 \cdot 7/2^{11} = 2 \cdot 3 \cdot 7$.

Finally, the number of subgroups K of $\mathbf{Z}^3$ such that $\mathbf{Z}^3/K$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ is $2 \cdot 3 \cdot 7 = 42$. □

Note. The task is to compute the number of Hermite normal forms for a given Smith normal form, which has been computed in general when the invariant factors are powers of a single prime. For any subgroup L of $\mathbf{Z}^n$ of finite index $[\mathbf{Z}^n : L]$, $[\mathbf{Z}^n : L]\mathbf{Z}^n \subseteq L$ by Lagrange's theorem applied to the quotient $\mathbf{Z}^n/L$. In particular, by the third isomorphism theorem, the set of subgroups K such that $\mathbf{Z}^3/K$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ is in bijection with the set of subgroups H of $\mathbf{Z}^3/2^6\mathbf{Z}^3 = (\mathbf{Z}/2^6\mathbf{Z})^3$ such that $(\mathbf{Z}/2^6\mathbf{Z})^3/H$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ via $K \mapsto K/2^6\mathbf{Z}^3 \subseteq \mathbf{Z}^3/2^6\mathbf{Z}^3 = (\mathbf{Z}/2^6\mathbf{Z})^3$.

We now show that for finite abelian groups, the number of subgroups of a certain cotype (isomorphism class of cokernel) equals the number of subgroups of that type (isomorphism class). For a finite abelian group G, write $G^\vee = \mathrm{Hom}(G, \mathbf{T})$ for the dual group where $\mathbf{T}$ is the multiplicative group of complex numbers of modulus 1. To each subgroup H of the finite abelian group G associate H^0, the annihilator of H in G, which is the subgroup $(G/H)^\vee \to G^\vee$. Then $H^0 \cong G/H$ and $G^\vee/H^0 \cong H$ so $H \mapsto H^0$ takes a group H of type K_1 and cotype K_2 to a group H^0 of type K_2 and cotype K_1. By Pontryagin duality,

$$H^{00} = (G^\vee/(G/H)^\vee)^\vee = H^{\vee\vee} = H$$

so the association is a bijection from the subgroups of G of type K_1 and cotype K_2 with subgroups of $G^\vee$ of type K_2 and cotype K_1, but $G^\vee$ is (non-canonically) isomorphic to G so this implies the desired equality of the number of subgroups of given type and the number of subgroups of the same cotype.

We must now compute the number of subgroups of $(\mathbf{Z}/2^6\mathbf{Z})^3$ isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$. Represent an element of $(\mathbf{Z}/2^6\mathbf{Z})^3$ as a row vector with 3 components each in $(0, 2^6]$. Then a subgroup can be represented as a matrix of width 3 whose rows represent the generators. The $p^4 + 2p^3 + 2p^2 + p$ subgroups of $(\mathbf{Z}/p^6\mathbf{Z})^3$ isomorphic to

$\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p^2\mathbf{Z} \times \mathbf{Z}/p^3\mathbf{Z}$ are represented by the following matrices.

$$\begin{bmatrix} p^3 & (0,p]p^3 & (0,p^2]p^3 \\ p^6 & p^4 & (0,p]p^4 \\ p^6 & p^6 & p^5 \end{bmatrix}, \qquad \begin{bmatrix} p^3 & (0,p^2]p^3 & (0,p]p^3 \\ p^6 & p^5 & p^4 \\ p^6 & p^5 & p^6 \end{bmatrix},$$
$$\begin{bmatrix} p^4 & p^3 & (0,p^2]p^3 \\ p^4 & p^6 & (0,p]p^4 \\ p^6 & p^6 & p^5 \end{bmatrix}, \qquad \begin{bmatrix} (0,p]p^4 & p^3 & (0,p]p^3 \\ p^5 & p^6 & p^4 \\ p^5 & p^6 & p^6 \end{bmatrix},$$
$$\begin{bmatrix} p^4 & (0,p]p^4 & p^3 \\ p^4 & (0,p]p^4 & p^6 \\ p^6 & p^5 & p^6 \end{bmatrix}, \qquad \begin{bmatrix} (0,p]p^4 & p^4 & p^3 \\ p^5 & p^4 & p^6 \\ p^5 & p^6 & p^6 \end{bmatrix}.$$

Another possibility is to write down the possible Hermite normal forms and determine which have the desired Smith normal form. A subgroup of $\mathbf{Z}^n$ generated by at most m elements can be represented as the row space of an $m \times n$ matrix, but two matrices represent the same subgroup when they are left equivalent (in the same orbit under the action of the $n \times n$ unimodular matrices). Therefore subgroups of $\mathbf{Z}^n$ correspond to orbits under the action of unimodular matrices, that is equivalence classes of left equivalent matrices. There is exactly one Hermite normal form in each equivalence class so subgroups of $\mathbf{Z}^n$ generated by at most m elements are in bijective correspondence with $m \times n$ Hermite normal forms.

In particular each subgroup $K \subseteq \mathbf{Z}^3$ is the row space of a unique 3×3 matrix in Hermite normal form. When $\mathbf{Z}^3/K$ is finite, its order is the product of the diagonal entries of the Hermite normal form matrix corresponding to K. Therefore the index $2 \cdot 4 \cdot 8 = 2^6$ subgroups of $\mathbf{Z}^3$ are each uniquely expressable as the row space of a matrix of the form

$$\begin{bmatrix} c_{11} & 0 & 0 \\ c_{21} & c_{22} & 0 \\ c_{31} & c_{32} & c_{33} \end{bmatrix}$$

where each c_{ij} is nonnegative, $c_{11}c_{22}c_{33} = 2^6$, $c_{21} < c_{22}$, $c_{31}, c_{32} < c_{33}$. By considering the diagonalized form, we see that if d_i is the greatest common divisor of the set of $i \times i$ minor matrix determinants, then $\mathbf{Z}^3/K$ is isomorphic to $\mathbf{Z}/d_1 \times \mathbf{Z}/d_1^{-1}d_2\mathbf{Z} \times \mathbf{Z}/d_2^{-1}d_3\mathbf{Z}$. We want $d_1 = 2$, $d_2 = 2^3$, $d_3 = 2^6$. In particular $2 \mid d_1$ so each c_{ij} must be even and then the possible diagonal entries are permutations of $2, 2, 16$ or $2, 4, 8$ or $4, 4, 4$. We already see that $2, 2, 16$ is impossible for in that case a 2×2 minor matrix would have determinant 4, but we want $8 \mid d_2$. In the case of matrices with diagonal entries $4, 4, 4$ we find that the

possibilities for the lower left are

$$\begin{bmatrix} 0 & \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 2 & \\ 2 & 0 \end{bmatrix}.$$

Finally we consider the six possible diagonals with entries $2,4,8$. In this case the only condition on the Hermite normal forms is that the entries in the lower left are even (this ensures $d_1 = 2$ since 2 already appears on the diagonal) and every 2×2 minor matrix has determinant determinant a multiple of 8 (which is sufficient to ensure $d_2 = 8$ since the triangular minor matrix with diagonal entries 2 and 4 has determinant 8).

- Order: $2,4,8$. The possibilities for the lower left are $\left[\begin{smallmatrix} 0 & \\ 0 & z \end{smallmatrix}\right]$ for $z \in \{0,2\}$, but we must have $8 \mid 2z$ so $z = 0$. The 1 possibility is $\left[\begin{smallmatrix} 0 & \\ 0 & 0 \end{smallmatrix}\right]$.
- Order: $2,8,4$. The possibilities for the lower left are $\left[\begin{smallmatrix} 0 & \\ 0 & z \end{smallmatrix}\right]$ for $z \in \{0,2,4,6\}$, but we must have $8 \mid 2z$, that is $4 \mid z$. Thus in this case the possibilities are $\left[\begin{smallmatrix} 0 & \\ 0 & 0 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & \\ 0 & 4 \end{smallmatrix}\right]$.
- Order: $4,2,8$. The possibilities for the lower left are of the form $\left[\begin{smallmatrix} x & \\ y & 0 \end{smallmatrix}\right]$ so in order that the lower left minor matrix have determinant divisible by 8 the lower left entry y cannot be 2 and must be 0. Thus the possibilities for the lower left are $\left[\begin{smallmatrix} x & \\ 0 & 0 \end{smallmatrix}\right]$ for $x \in \{0,2\}$ so there are 2 in this case.
- Order: $4,8,2$. If the lower left is $\left[\begin{smallmatrix} x & \\ y & z \end{smallmatrix}\right]$ then $2x$ must be divisible by 8 so $x = 0$, but otherwise there are no further restrictions. Thus the possibilities for the lower left are $\left[\begin{smallmatrix} 0 & \\ y & z \end{smallmatrix}\right]$ for $x \in \{0,2,4,6\}$ and $y \in \{0,2\}$ so there are 8 in this case.
- Order: $8,2,4$. If the lower left is $\left[\begin{smallmatrix} x & \\ y & 0 \end{smallmatrix}\right]$ then $y \in \{0,4\}$ and $x \in \{0,2,4,6\}$ so there are 8 in this case.
- Order: $8,4,2$. If the lower left is $\left[\begin{smallmatrix} x & \\ y & z \end{smallmatrix}\right]$ then $8 \mid 2x$ so $x \in \{0,4\}$, $y \in \{0,2,4,6\}$, and $z \in \{0,2\}$ so there are 16 in this case.

We have found the 42 sublattices and found generators for them.

Problem 6. Let M be an $n \times m$ matrix with entries in the PID R. Let K be the submodule of R^n spanned by the columns, and S the submodule of R^m spanned by rows. Prove that the torsion submodules of R^n/K and R^m/S are isomorphic.

Solution. Let A be an element of $\mathrm{GL}_n(R)$. Then AM is obtained from M by elementary row operations so the row spans of M and AM are the same. Write φ_A for the element of $\mathrm{GL}(R^n)$ corresponding to A with respect to the standard basis. We have $R^n/K \cong \varphi_A(R^n)/\varphi_A(K) =$

R^n/K' where K' is the span of the columns of AM. Therefore the result is invariant under left multiplication by an element of $\mathrm{GL}_n(R)$.

Let B be an element of $\mathrm{GL}_m(R)$. Then MB is obtained from M by elementary column operations so the column spans of M and MB are the same. Write ψ_B for the element of $\mathrm{GL}(R^m)$ corresponding to A with respect to the standard basis. We have $R^m/S \cong \psi_A(R^m)/\psi_A(S) = R^m/S'$ where S' is the span of the columns of MB. Therefore the result is invariant under left multiplication by an element of $\mathrm{GL}_m(R)$.

We now show that there exist matrices A in $\mathrm{GL}_n(R)$ and B in $\mathrm{GL}_m(R)$ such that AMB is zero except for the diagonal entries (which can be chosen so that each diagonal entry is divisible by the one before it).[4] This is equivalent to performing elementary row and column operations on M to obtain the desired form. Consider a fixed column (resp. row). If the ith and jth entries are a and b, then it is possible to perform elementary operations to rows (resp. columns) i and j to transform the ith entry to a generator of the ideal generated by a and b and transform the jth entry to 0. With these operations we may make every entry in the first row or the first column to be zero, except possibly the (i, j) entries for $i + j \leq 3$. Along with induction, this reduces to the case where $m = n = 2$. Row operations can transform a 2×2 matrix to the form $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ and column operations can transform a 2×2 matrix to the form $\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)$. Alternately apply the two operations above. Each time, the upper left entry is replaced by a divisor of itself. Since increasing sequences of ideals must stabilize (consider a generator of the union of the sequence), the ideal generated by the upper left entry eventually stabilizes. Then the upper left entry divides both the lower left and upper right entries and so the matrix can be made diagonal.

When M has all nondiagonal entries equal to 0, the result is clear, so this completes the proof. □

[4] I believe this was proved in lecture.