MATH 123: ABSTRACT ALGEBRA II
SOLUTION SET # 7

GREGG MUSIKER

1. Chapter 12, Section 4

Problem 4 *Let $d_1, d_2, \ldots$ be the integers referred to in Theorem (4.3).*

a) Prove that d_1 is the greatest common divisor of the entries of a_{ij} of A.
b) Prove that $d_1 d_2$ is the greatest common divisor of the determinants of the 2×2 minors of A.
c) State and prove an extension of (a) and (b) to d_i for arbitrary i.

I only do part (c) since (a) and (b) are the special cases $i = 1$ and $i = 2$ respectively.

Claim Let $M = \begin{bmatrix} d_1 & 0 & 0 & \ldots & 0 & \ldots & 0 \\ 0 & d_2 & 0 & \ldots & 0 & \ldots & 0 \\ 0 & 0 & d_3 & \ldots & 0 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & d_n & \ldots & 0 \\ & & \ldots & & & & \\ 0 & 0 & 0 & \ldots & 0 & \ldots & 0 \end{bmatrix}$. Then $d_1 d_2 \cdots d_i$ is the gcd of any $i \times i$ minor of M.

Since $d_1 | d_2 | \ldots | d_n$, an $i \times i$ minor which is zero or the product of i distinct d_j will be divisible by the product of the first i d_j $(d_1 \cdots d_i)$ and this product is the greatest since $d_1 \cdots d_i$ is a possible $i \times i$ minor.

By Theorem 4.3, any integer matrix can be diagonalized into a form like M by invertible row and column operations. Thus it suffices to show the following:

If N is a matrix where $d_1 \cdots d_i$ is the gcd of all of the $i \times i$ minors, then PNQ also has this property where P is an elementary row operation and Q is an elementary column operation.

1) Assume P (Q) is the row (column) operation which adds an integer multiple of row (column) I to row (column) J.

For any $i \times i$ minor not involving I or J, the minor is unchanged. For any minor containing both I and J, by the properties of determinants (pages 20-23 Artin), the determinant is unchanged. Since $\gcd(a, b) = \gcd(a, a + b)$, even if only one out of I and J is in minor, the gcd of all the minors will be unchanged.

2) Assume P (Q) is the row (column) operation which interchanges row (column) I with row (column) J.

For any $i \times i$ minor not involving I or J, the minor is unchanged. For any minor containing both I and J, the determinant is changed by -1 which is a unit, hence it does not affect gcd. If only one out of I or J is in the minor, then we have just switched the labeling of two minors in our list of minors and gcd is unaffected.

3) Assume P (Q) is the row (column) operation which multiplies row (column) I by a unit, ± 1.

For any $i \times i$ minor not involving I, the minor is unchanged. For any minor containing both I, the determinant is changed by ± 1 which is a unit, hence it does not affect gcd.

Problem 5 *Determine all integer solutions to the system of equations $AX = 0$, when $A = \begin{bmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \end{bmatrix}$.*

We first diagonalize this matrix:

$\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} A = \begin{bmatrix} 0 & -1 & -10 \\ 2 & 4 & 6 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 & -10 \\ 2 & 4 & 6 \end{bmatrix} = \begin{bmatrix} 0 & -1 & -10 \\ 2 & 0 & -34 \end{bmatrix}$,

$\begin{bmatrix} 0 & -1 & -10 \\ 2 & 0 & -34 \end{bmatrix} \begin{bmatrix} 1 & 0 & 17 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -1 & -10 \\ 2 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & -1 & -10 \\ 2 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -10 \\ 0 & 0 & 1 \end{bmatrix} =$

$\begin{bmatrix} 0 & -1 & 0 \\ 2 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 & 0 \\ 2 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$.

Thus $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} = PAQ$ for matrices $P = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -4 & 8 \\ 1 & -2 \end{bmatrix}$

and $Q = \begin{bmatrix} 1 & 0 & 17 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -10 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 17 \\ 0 & 1 & -10 \\ 0 & 0 & 1 \end{bmatrix}$

$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} X = 0$ only if $x_1 = x_2 = 0$ but x_3 can be any number.

$\begin{bmatrix} 1 & 0 & 17 \\ 0 & 1 & -10 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ x_3 \end{bmatrix} = \begin{bmatrix} 17x_3 \\ -10x_3 \\ x_3 \end{bmatrix}$ so the integer solutions to $AX = 0$ are of the form $\begin{bmatrix} 17x_3 \\ -10x_3 \\ x_3 \end{bmatrix}$.

Problem 7 *Prove that the two matrices $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ generate the group $SL_2(\mathbb{Z})$.*

Any matrix M in $SL_2(\mathbb{Z})$ has rank 2 (is invertible) and a determinant of 1 hence M can be diagonalized as the 2×2 identity. In other words there exists row operations P and column operations Q such that $M = PIQ = PQ$.

The row (column) operation of adding an integer multiple of the second row (first column) to the first row (second column) is represented by the matrix $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = A^n$ for all integers n and the row (column) operation of adding an integer multiple of the first row (second column) to the second row (first column) is represented by the matrix

$\begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix} = (ABA)^n$ for all integers n. While multiplying one row or column by -1 would result in a matrix of determinant -1, which is not allowed. We thus combine this operation with the operation permuting the rows or columns to get an operation with determinant equal to $(-1)(-1) = 1$, B. $A, B, I \in SL_2(\mathbb{Z})$ and all matrices in $SL_2(\mathbb{Z})$ are equal to a composition of As and Bs, consequently, A and B generate $SL_2(\mathbb{Z})$.

2. Chapter 12, Section 5

Problem 2 *Find a ring R and an ideal I of R which is not finitely generated.*

A good example is the following: $R = F[x_1, x_2, \dots]$ a polynomial ring in a countably infinite number of variables. (Note: we need a ring like this since any polynomial ring (over a field) with a finite number of variables) is Noetherian by the Hilbert Basis Theorem, and thus all ideals would be finitely generated.)

Let I be the ideal generated by all (or an infinite subset of) the variables. One can check that I is an ideal by showing that for $a, b \in I$, $r \in R$. then $a + b$ and $ra \in I$. $x_i \in I$ for all $i \in \mathbb{N}$, and $1 \notin I$ thus the smallest basis for I is $(x_1, x_2, \dots,)$ an infinite collection of all the variables. The span of any smaller basis would not include the element x_i for some x_i since there are no relations that allow x_i to be written as a R-linear combination of the other variables.

Another good example is $R = \{$ Continuous functions from $\mathbb{R} \to \mathbb{R}\}$. This is a ring using $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x) \cdot g(x)$. Remember that addition and multiplication preserve continuity. $I = \{f : f(0) = 0\}$. To see that I is an ideal, note that if $f(0) = 0$ and $g(0) = 0$ then $(f + g)(0) = f(0) + g(0) = 0$ and $(f \cdot g)(0) = f(0)g(0) = 0$.

To see that I is not finitely generated, one can show that $\sin(x), \sin(2x), \sin(3x), \dots$ are all linearly independent and have no common divisor but are all in I.

Interesting note: if we had looked at the subring of polynomial functions from $\mathbb{R} \to \mathbb{R}$ ($\mathbb{R}[x]$), then I would still be an ideal, but in this case it would have been finitely generated, in fact $I = (x)$ the ideal of polynomials with no constant terms.

Problem 3 *Prove that existence of factorization holds in a noetherian integral domain.*

By Proposition (12.5.17), every submodule of V, a finitely generated module over a noetherian ring R, is finitely generated.

By Proposition (12.5.13), the *ascending chain condition* holds, there is no infinite strictly increasing chains of submodule of V.

In light of (12.1.3), we can let V be R, itself, which changes these statements to the fact that there is no infinite strictly increasing chain of ideals of R. Thus there is no infinite increasing chain of principal ideals, and by Proposition (10.2.3), factorization exists.

Problem 4 *Let $\mathcal{V} \subset \mathbb{C}^n$ be the locus of zeros of an infinite set of polynomials $f_1, f_2, \dots$. Prove that there is a finite subset of these polynomials whose zeros define the same locus.*

$\mathcal{V}$ is a variety and as we saw earlier in section 3 of chapter 11, we can associate an ideal of polynomials to this variety. In particular, let $I = (f_1, f_2, \dots)$. Then the variety associated with I, $V(I)$ is precisely $V(I) = \mathcal{V}$,

$$(f_1) \subseteq (f_1, f_2) \subseteq (f_1, f_2, f_3) \subseteq \dots$$

$$V(f_1) \supseteq V(f_1, f_2) \supseteq V(f_1, f_2, f_3) \supseteq \dots$$

Since $\mathbb{C}^n$ is Noetherian, there can be no infinitely ascending chains of ideals (the chains must stabilize) and there exists n such that $(f_1, \dots, f_n) = I$ and $V(f_1, \dots, f_n) = \mathcal{V}$.

Problem 6 *Determine a presentation matrix for the ideal* $(2, 1+\delta)$ *of* $\mathbb{Z}[\delta]$ *where* $\delta = \sqrt{-5}$ *(over R).*

As explained in class, we consider the surjective map

$$R^2 \to^{\phi} (2, 1+\delta)$$

$$(x, y) \to 2x + (1+\delta)y.$$

$\ker \phi$ has two generators. There is the relation that $2(-1-\delta) + (1+\delta)2 = 0$ and also the relation $2(-3) + (1+\delta)(1-\delta) = 0$

These two relations cannot be derived from each other.

We find $\ker \phi$ by finding $(x, y) \in R$ such that $2x + (1+\delta)y = 0$ which means

$$\ker \phi = \{y : y \in R \text{ and } \frac{(1+\delta)}{2}\text{y is also in R}\}.$$

Thus the presentation matrix is $\begin{bmatrix} -3 & -1-\delta \\ 1-\delta & 2 \end{bmatrix}$

3. Chapter 12, Section 6

Problem 1 *Find a direct sum of cyclic groups which is isomorphic to the abelian group presented by the matrix* $\begin{bmatrix} 2 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{bmatrix}$.

We use the operations *more than just the elementary row and column operations* for manipulating presentation matrices as described in proposition 12.5.12

$$\begin{bmatrix} 2 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{bmatrix} \to \begin{bmatrix} 2 & 0 & 2 \\ 2 & 0 & 0 \\ 2 & -2 & 2 \end{bmatrix} \to \begin{bmatrix} 2 & 0 & 2 \\ 0 & 0 & -2 \\ 0 & -2 & 0 \end{bmatrix} \to \begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & -2 & 0 \end{bmatrix} \to \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

So the presented abelian group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Problem 4. *Determine the number of isomorphism classes of abelian groups of order* $400 = 2^4 \cdot 5^2$.

By Theorem (12.6.13), *the elementary divisor form of the Structure Theorem*, any abelian group G such that $|G| = N = q_1^{e_1} \cdots q_n^{e_n}$ looks like $\mathbb{Z}/q_1^{e_{1,1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/q_1^{e_{1,m}}\mathbb{Z} \times \cdots \times \mathbb{Z}/q_n^{e_{n,1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/q_n^{e_{n,m}}\mathbb{Z}$ where the q_is are distinct primes. Consequently, the number of isomorphism classes of abelian groups of order N is $P(e_1)P(e_2)\cdots P(e_n)$

where $P(k)$ is the number of partitions of k. For example $P(5) = 7$ since $5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$.

For this specific problem, the number of isomorphism classes is $P(2)P(4) = 2 \times 5 = 10$.

More concretely, the possibilities are
$\mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
$\mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$,
$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$,
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$,
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, and
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Note that terms such that are relatively prime such as $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/10\mathbb{Z}$, but $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \ncong \mathbb{Z}/4\mathbb{Z}$.