Problem Set 12 Solutions

Igor Rapinchuk

1. It follows from the properties of determinants that multiplying a row (column) of a matrix by an element of our ring and adding it to a different row (column) does not change the determinant of a given matrix. Interchanging two rows (columns) multiplies the determinant by (-1). Multiplying a row (column) by an element of our ring results in multiplying the determinant by the same element. However, in doing row and column operations, we are allowed to multiply rows and columns only by the *units* of our ring $R = F[t]$. We showed in an earlier assignment that the units are precisely the nonzero elements of F. So, $\det A' = \alpha \det A$ for some $\alpha \in F^*$.

2.(a)

$$A = \begin{pmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \end{pmatrix} \overset{\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}}{\longrightarrow} \begin{pmatrix} 0 & -1 & -10 \\ 2 & 4 & 6 \end{pmatrix} \overset{\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}}{\longrightarrow} \begin{pmatrix} 0 & -1 & -10 \\ 2 & 0 & -34 \end{pmatrix}$$

$$\overset{\begin{pmatrix} 1 & 0 & 17 \\ 0 & 1 & -10 \\ 0 & 0 & 1 \end{pmatrix}}{\longrightarrow} \begin{pmatrix} 0 & -1 & 0 \\ 2 & 0 & 0 \end{pmatrix} \overset{\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} = B.$$

So,

$$P^{-1} = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 4 & -7 \end{pmatrix}$$

and

$$Q = \begin{pmatrix} 1 & 0 & 17 \\ 0 & 1 & -10 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 17 \\ -1 & 0 & -10 \\ 0 & 0 & 1 \end{pmatrix}.$$

(b) We have $A = PBQ^{-1}$, where $P = \begin{pmatrix} -7 & 2 \\ -4 & 1 \end{pmatrix}$ and $Q^{-1} \begin{pmatrix} 0 & -1 & -10 \\ 1 & 0 & 17 \\ 0 & 0 & 1 \end{pmatrix}$. So, $AX = 0$ is equivalent to $BY = 0$, where $Y = Q^{-1}X$ (and integral X's correspond to integral Y's because Q is an invertible integer matrix). But the solutions of $BY = 0$ are $Y = \begin{pmatrix} 0 \\ 0 \\ t \end{pmatrix}$ for $t \in \mathbb{Z}$. So,

$$X = QY = \begin{pmatrix} 0 & -1 & 17 \\ 1 & 0 & -10 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ t \end{pmatrix} = \begin{pmatrix} 17t \\ -10t \\ t \end{pmatrix}.$$

3. Example #1 Let $R = \mathbb{C}[x_1, x_2, \ldots, x_n, \ldots]$ and $I = (x_1, \ldots, x_n, \ldots)$. Suppose I is finitely generated, say $I = (f_1, \ldots, f_r)$, where $f_i \in I$. The polynomials $f_1, \ldots, f_r$ involve

only finitely many variables, say $x_1, \ldots, x_n$. Since $x_{n+1} \in I$, there exists a relation

$$x_{n+1} = f_1 g_1 + \cdots + f_r g_r, \quad g_i \in R.$$

Clearly, $f_1(0, \ldots, 0) = \cdots = f_r(0, \ldots, 0) = 0$. Specializing $x_1, \ldots, x_n$ to zero and x_{n+1} to 1, we get $1 = 0$, a contradiction. So, I is not finitely generated.

Example #2 Let R be the ring of all algebraic integers, $I = (\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \ldots, \sqrt[2^n]{2}, \ldots)$. Suppose I is finitely generated, say $I = (a_1, \ldots, a_r)$, $a_i \in I$. Each a_i can be written as a finite linear combination, with coefficients in R, of some $\sqrt[2^n]{2}$'s. Then, all $a_1, \ldots, a_r$ involve only finitely many of $\sqrt[2^n]{2}$'s, say $\sqrt{2}, \ldots, \sqrt[2^n]{2}$, and therefore, $I = (\sqrt{2}, \ldots, \sqrt[2^n]{2}) = (\sqrt[2^n]{2})$. But $\sqrt[2^{n+1}]{2} \in I$; however, $\frac{\sqrt[2^{n+1}]{2}}{\sqrt[2^n]{2}} = \frac{1}{\sqrt[2^{n+1}]{2}} \notin R$, a contradiction.

4. Let R be a Noetherian integral domain. First, we show that every element $a \in R$, $a \neq 0$ has an irreducible divisor. Assume that $a \in R$ does not have this property. Then a is not irreducible, hence $a = bc$, where neither of b, c is a unit. We have $(a) \subsetneqq (b)$. Next, b does not have an irreducible divisor either as otherwise this divisor would also be an irreducible divisor of a. Repeating the argument, we see that $b = de$ and $(b) \subsetneqq (d)$. This gives us a strictly ascending chain of ideals $(a) \subsetneqq (b) \subsetneqq (d) \subsetneqq \cdots$, a contradiction.

Now let $a \in R$ be an arbitrary nonzero non-unit. Then by the above, a has an irreducible divisor p_1, so $a = p_1 a_1$, with $a_1 \in R$. If a_1 is a unit, we are done. If not, then $a_1 = p_2 a_2$ with p_2 irreducible, and $a = p_1 p_2 a_2$. Notice that we have a strictly ascending chain of ideals

$$(a) \subsetneqq (a_1) \subsetneqq (a_2) \subsetneqq \cdots .$$

Since R is Noetherian, this chain must stop, and we will get a factorizaiton $a = p_1 \cdots p_r$.

5. Every module M over $\mathbb{Z}/n\mathbb{Z}$ can be regarded as a module over $\mathbb{Z}$ for the following scalar multiplication: $a \cdot m \stackrel{\text{def}}{=} \bar{a} \cdot m$, where $\bar{a} = a + n\mathbb{Z}$. Converserly, a $\mathbb{Z}-$module M can be regarded as a module over $\mathbb{Z}/n\mathbb{Z}$ iff it is annihilated by multiplication by n. So, if M is a module over $Z/n\mathbb{Z}$, by the Structure Theorem for $\mathbb{Z}-$modules,

$$M = \bigoplus_i \left(\bigoplus_j \mathbb{Z}/p_i^{\alpha_{ij}} \right) \oplus \mathbb{Z}^s.$$

Then n must annihilate each factor. It follows that $s = 0$ and $p_i^{\alpha_{ij}} \mid n$ for all i, j. If $n = q_1^{\beta_1} \cdots q_d^{\beta_d}$, then M is a finite direct sum of modules of the form $\mathbb{Z}/p^\alpha\mathbb{Z}$ where $p = q_i$ and $\alpha \leqslant \beta_i$, for some $i \in \{1, \ldots, d\}$.

6. We have $V \simeq R^m/W$, where W is the submodule generated by $d_1 e_1, \ldots, d_m e_m$ and $e_1, \ldots, e_m$ is the standard basis of R^m. Consider

$$f \colon R^m \to R/(d_1) \oplus \cdots R/(d_m)$$

defined by $f(a_1, \ldots, a_m) = (a_1 + (d_1), \ldots, a_m + (d_m))$. Obviously, f is surjective. It is easy to see that Kef$f$ coincides with the submodule generated by $d_1 e_1, \ldots, d_m e_m$, which is W. So, by the First Isomorphism Theorem for modules, we have

$$V = R^m/W \simeq R^m/\mathrm{Ker} f \simeq \mathrm{Im} f = R/(d_1) \oplus \cdots \oplus R/(d_m).$$

7. (a) Let $\bar{a} = a + (p^e) \in \mathbb{Z}/(p^e)$. Then the order of $\bar{a}$ divides $p^v \cdots \bar{a} = \bar{0}$. If $v \geqslant e$, then all elements of $\mathbb{Z}/(p^e)$ satisfy this condition, and therefore the number of such elements if p^e, Suppose $v < e$. Then $p^v \cdot \bar{a} = \bar{0} \Leftrightarrow p^v a$ is divisible by $p^e \Leftrightarrow a$ is divisible by p^{e-v}. Thus,

$$\{\bar{a} \in \mathbb{Z}/(p^e) \mid p^v \cdot \bar{a} = \bar{0}\} = p^{e-v}\mathbb{Z}/p^e\mathbb{Z} \simeq \mathbb{Z}/p^v\mathbb{Z}$$

under the map $p^{e-v}x + p^e\mathbb{Z} \mapsto x + p^v\mathbb{Z}$. So, the number of such elements is p^v.

(b) Let $w = (w_1, \ldots, w_k) \in V = W_1 \times \cdots \times W_k$. Then $qw = (qw_1, \ldots, qw_k)$. So, the order of w divides q iff the order of each w_i divides q. It follows that the total number of elements in V of order dividing q is $u_1 \cdots u_k$.