Math 121 Homework 1: Notes on Selected Problems

10.1.2. Prove that $R^\times$ and M satisfy the two axioms in Section 1.7 for a *group action* of the multiplicative group $R^\times$ on the set M.

Solution. If $s(rm) = (sr)m$ for all r and s in R, then in particular the same is true for r and s in $R^\times \subseteq R$. The condition that 1 in the module R act on M as the identity is precisely the condition that 1 in the group $R^\times$ act on M as the identity. □

10.1.7. Let $N_1 \subseteq N_2 \subseteq \cdots$ be an ascending chain of submodules of M. Prove that $\bigcup_{i=1}^{\infty} N_i$ is a submodule of M.

Solution. Clearly 0 is in $\bigcup_{i=1}^{\infty} N_i$ as 0 is in fact in each subgroup N_i. If m is in $\bigcup_{i=1}^{\infty} N_i$, say m is in N_k, then, as the subgroup N_k is closed under additive inverses, $-m$ is in N_k and hence also in $\bigcup_{i=1}^{\infty} N_i$. Now assume m_1 and m_2 are in $\bigcup_{i=1}^{\infty} N_i$, say m_1 is in N_{k_1} and m_2 is in N_{k_2}. For any k_3 greater than or equal to both of k_1 and k_2, $N_{k_1} \subseteq N_{k_3}$ and $N_{k_2} \subseteq N_{k_3}$ so m_1 and m_2 are both in N_{k_3}. The subgroup N_{k_3} is closed under addition so $m_1 + m_2$ is also in N_{k_3}, and hence in $\bigcup_{i=1}^{\infty} N_i$. This proves that $\bigcup_{i=1}^{\infty} N_i$ is a subgroup of M.

Let r be a ring element and m be an element of $\bigcup_{i=1}^{\infty} N_i$, say m is in N_k. Then since N_k is a submodule, rm is also in N_k. Therefore rm is in $\bigcup_{i=1}^{\infty} N_i$. This proves that the subgroup $\bigcup_{i=1}^{\infty} N_i$ of M is a submodule of M. □

10.2.5. Exhibit all $\mathbf{Z}$-module homomorphisms from $\mathbf{Z}/30\mathbf{Z}$ to $\mathbf{Z}/21\mathbf{Z}$.

Solution. Let m and n be positive integers. We examine the relationship between the top and bottom homomorphisms in the commutative square

$$\begin{array}{ccc} \mathbf{Z} & \longrightarrow & \mathbf{Z} \\ \downarrow & & \downarrow \\ \mathbf{Z}/m\mathbf{Z} & \longrightarrow & \mathbf{Z}/n\mathbf{Z}. \end{array}$$

Given a homomorphism $\mathbf{Z} \to \mathbf{Z}$ on top, there is at most one possible homomorphism $\mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ on the bottom since $\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ is surjective. Given a homomorphism $\mathbf{Z} \to \mathbf{Z}$ on top carrying $m\mathbf{Z}$ to $n\mathbf{Z}$, that is with image in $\mathbf{Z}/n\mathbf{Z}$ constant on each coset $\mathbf{Z}/m\mathbf{Z}$, we may use it to define a homomorphism $\mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$. Thus there is a map

$$\mathrm{Hom}((\mathbf{Z}, m\mathbf{Z}), (\mathbf{Z}, n\mathbf{Z})) \to \mathrm{Hom}(\mathbf{Z}/m\mathbf{Z}, \mathbf{Z}/n\mathbf{Z})$$

where the notation on the left means homomorphisms $\mathbf{Z} \to \mathbf{Z}$ sending $m\mathbf{Z}$ to $n\mathbf{Z}$. Since $\{1\} \hookrightarrow \mathbf{Z}$ is free and $\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ is surjective, homomorphisms $\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ lift to homomorphisms $\mathbf{Z} \to \mathbf{Z}$. Therefore the above mapping of Hom-sets is surjective.

The diagram

$$\begin{array}{ccc} \mathrm{Hom}((\mathbf{Z}, m\mathbf{Z}), (\mathbf{Z}, n\mathbf{Z})) & \twoheadrightarrow & \mathrm{Hom}(\mathbf{Z}/m\mathbf{Z}, \mathbf{Z}/n\mathbf{Z}) \\ \downarrow & & \downarrow \\ \mathrm{Hom}(\mathbf{Z}, \mathbf{Z}) & \twoheadrightarrow & \mathrm{Hom}(\mathbf{Z}, \mathbf{Z}/n\mathbf{Z}) \end{array}$$

commutes because both compositions correspond to methods of obtaining the diagram morphism from the earlier commutative square. The kernel of the top surjective homomorphism is $\mathrm{Hom}((\mathbf{Z}, \mathbf{Z}), (\mathbf{Z}, n\mathbf{Z}))$, which is identified with an obvious submodule of $\mathrm{Hom}(\mathbf{Z}, \mathbf{Z})$. We have the diagram

$$\begin{array}{ccccc} \mathrm{Hom}((\mathbf{Z}, \mathbf{Z}), (\mathbf{Z}, n\mathbf{Z})) & \hookrightarrow & \mathrm{Hom}((\mathbf{Z}, m\mathbf{Z}), (\mathbf{Z}, n\mathbf{Z})) & \twoheadrightarrow & \mathrm{Hom}(\mathbf{Z}/m\mathbf{Z}, \mathbf{Z}/n\mathbf{Z}) \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Hom}(\mathbf{Z}, \mathbf{Z}) & \hookrightarrow & \mathrm{Hom}(\mathbf{Z}, \mathbf{Z}) & \twoheadrightarrow & \mathrm{Hom}(\mathbf{Z}, \mathbf{Z}/n\mathbf{Z}). \end{array}$$

We seek the images of the two leftmost vertical homomorphisms after applying the natural isomorphism $\mathrm{Hom}(\mathbf{Z}, \mathbf{Z}) \to \mathbf{Z}$ given by evaluation at 1. The leftmost vertical homomorphism has image $n\mathbf{Z}$. An integer r is in the image of the middle vertical homomorphism if and only if n divides mr, that is if and only if $\gcd(m, n)$ divides r. Thus the middle vertical homomorphism has image $(n/\gcd(m, n))\mathbf{Z}$. From the sequence

$$n\mathbf{Z} \hookrightarrow (n/\gcd(m, n))\mathbf{Z} \twoheadrightarrow \mathrm{Hom}(\mathbf{Z}/m\mathbf{Z}, \mathbf{Z}/n\mathbf{Z})$$

with first homomorphism the kernel of the second homomorphism, the first isomorphism theorem gives an isomorphism

$$\mathrm{Hom}(\mathbf{Z}/m\mathbf{Z}, \mathbf{Z}/n\mathbf{Z}) \cong \frac{(n/\gcd(m, n))\mathbf{Z}}{n\mathbf{Z}}$$

The composition

$$(n/\gcd(m, n))\mathbf{Z} \hookrightarrow \mathbf{Z} \twoheadrightarrow \mathbf{Z}/\gcd(m, n)\mathbf{Z}$$

has kernel $n\mathbf{Z}$ so we then have an isomorphism

$$\mathrm{Hom}(\mathbf{Z}/m\mathbf{Z}, \mathbf{Z}/n\mathbf{Z}) \cong \mathbf{Z}/\gcd(m, n)\mathbf{Z}$$

again by the first isomorphism theorem.

The problem asked that we find the homomorphisms $\mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$, and they can be obtained from the above, recalling that the first isomorphism theorem is more than just a statement of two objects being isomorphic, but is an explicit isomorphism. The homomorphism

$$(n/\gcd(m,n))\mathbf{Z} \twoheadrightarrow \mathrm{Hom}(\mathbf{Z}/m\mathbf{Z}, \mathbf{Z}/n\mathbf{Z})$$

takes an integer r divisible by $n/\gcd(m,n)$ and yields the unique map completing the bottom of the commutative square

$$\begin{array}{ccc} \mathbf{Z} & \longrightarrow & \mathbf{Z} \\ \downarrow & & \downarrow \\ \mathbf{Z}/m\mathbf{Z} & \longrightarrow & \mathbf{Z}/n\mathbf{Z} \end{array}$$

with top map give by multiplication by r. Therefore the

$$\gcd(m,n) = \#(\mathbf{Z}/\gcd(m,n)\mathbf{Z})$$

possible homomorphisms $\mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ are each induced by multiplication by some multiple of $n/\gcd(m,n)$ and two such homomorphisms are equal if and only if they differ by a multiple of n.

For example, the homomorphisms $\mathbf{Z}/30\mathbf{Z} \to \mathbf{Z}/21\mathbf{Z}$ are induced by multiplication by $21/\gcd(30,21) = 7$ and two such homomorphisms are equal if and only if they are induced by multiples of 7 differing by a multiple of 21. In particular, multiplication by 0, 7, and 14 give the $3 = \gcd(30,21)$ possible homomorphisms $\mathbf{Z}/30\mathbf{Z} \to \mathbf{Z}/21\mathbf{Z}$. □

10.2.13. Let I be a nilpotent ideal in a commutative ring R (cf. Exercise 37, Section 7.3), let M and N be R-modules and let $\varphi\colon M \to N$ be an R-module homomorphism. Show that if the induced map $\overline{\varphi}\colon M/IM \to N/IN$ is surjective, then φ is surjective.

Solution. For any n in N, $n + IN$ is in the image of the surjective homomorphism $\overline{\varphi}$, say m in M is such that $\overline{\varphi}(m + IM) = n + IN$. This means that $\varphi(m) - n$ is in IN. Since n in N was arbitrary, this proves that $N = \varphi(M) + IN$. Then

$$N = \varphi(M) + I(\varphi(M) + IN) = \varphi(M) + I^2N,$$

and by induction $N = \varphi(M) + I^rN$ for every positive integer r. Since I is nilpotent, it follows that $N = \varphi(M)$, as desired. □

10.3.1. Prove that if A and B are sets of the same cardinality, then the free modules $F(A)$ and $F(B)$ are isomorphic.

Solution. Given any set map $X \to Y$, the universal property of the free module $X \hookrightarrow F(X)$ gives a unique module homomorphism, which we call $F(X \to Y)$ completing the diagram

$$\begin{array}{ccc} X & \longrightarrow & Y \\ \downarrow & & \downarrow \\ F(X) & \longrightarrow & F(Y). \end{array}$$

Then compositions are preserved:

$$F(Y \to Z) \circ F(X \to Y) = F((Y \to Z) \circ (X \to Y))$$

as well as identity maps: $F(\mathbb{1}_X) = \mathbb{1}_{F(X)}$. It follows that isomorphisms are preserved for if $X \to Y$ and $Y \to X$ are inverse set maps, the above two properties show that $F(X \to Y)$ and $F(Y \to X)$ are inverse module homomorphisms.

If A and B are sets of the same cardinality, that is there is a set isomorphism $A \to B$, then $F(A) \to F(B)$ is a module isomorphism. □

10.3.15. An element $e \in R$ is called a *central idempotent* if $e^2 = e$ and $er = re$ for all $r \in R$. If e is a central idempotent in R, prove that $M = eM \oplus (1 - e)M$. [Recall Exercise 14 in Section 1.]

Solution. Let e be a central idempotent in R. Since e is central and 1 is central, $1 - e$ is also central. Therefore eM and $(1 - e)M$ are submodules of M. Note that $1 - e$ is also idempotent. One can show, using that e and $1 - e$ are idempotent that inverse homomorphisms between $eM \oplus (1 - e)M$ and M are given by

$$(a, b) \mapsto a + b \qquad \text{and} \qquad r \mapsto (er, (1 - e)r).$$

Therefore M is the (internal) direct sum $eM \oplus (1 - e)M$. □

10.3.24. *(An arbitrary direct product of free modules need not be free)* For each positive integer i let M_i be the free $\mathbf{Z}$-module $\mathbf{Z}$, and let M be the direct product $\prod_{i \in \mathbf{Z}^+} M_i$ (cf. Exercise 20). Each element of M can be written uniquely in the form $(a_1, a_2, a_3, \dots)$ with $a_i \in \mathbf{Z}$ for all i. Let N be the submodule of M consisting of all such tuples with only finitely many nonzero a_i. Assume M is a free $\mathbf{Z}$-module with basis $\mathcal{B}$.

- **(a)** Show that N is countable.
- **(b)** Show that there is some countable subset $\mathcal{B}_1$ of $\mathcal{B}$ such that N is contained in the submodule, N_1, generated by $\mathcal{B}_1$. Show also that N_1 is countable.

(c) Let $\overline{M} = M/N_1$. Show that $\overline{M}$ is a free $\mathbf{Z}$-module. Deduce that if $\overline{x}$ is any nonzero element of $\overline{M}$ then there are only finitely many distinct positive integers k such that $\overline{x} = k\overline{m}$ for some $m \in M$ (depending on k).

(d) Let $S = \{(b_1, b_2, b_3, \dots) \mid b_i = \pm i! \text{ for all } i\}$. Prove that S is uncountable. Deduce that there is some $s \in S$ with $s \notin N_1$.

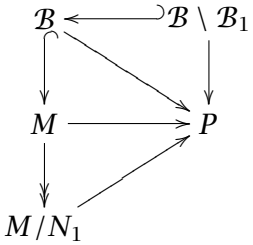
(e) Show that the assumption M is free leads to a contradiction: By (d) we may choose $s \in S$ with $s \notin N_1$. Show that for each positive integer k there is some $m \in M$ with $\overline{s} = k\overline{m}$, contrary to (c). [Use the fact that $N \subseteq N_1$.]

Solution.

(a) A finite product of countable sets is countable so for each positive integer r, the submodule $\mathbf{Z}^r$ of M is countable, and N is a countable union of such countable sets.

(b) Any single element of M is contained in a submodule generated by a finite number of elements of $\mathcal{B}$ since we may take as generating set the finitely many elements of $\mathcal{B}$ appearing in an expression in terms of the basis $\mathcal{B}$. It follows that each submodule $\mathbf{Z}^r$ of M is contained in a submodule generated by countably many elements of $\mathcal{B}$, and consequently the submodule N of M is contained in a submodule N_1 generated by countably many elements of $\mathcal{B}$. A countable product of countable sets is countable so N_1 is countable.

(c) We show that the inclusion $\mathcal{B} \setminus \mathcal{B}_1 \hookrightarrow M$ followed by the projection $M \twoheadrightarrow M/N_1$ satisfies the universal property for free modules. Let $\mathcal{B} \setminus \mathcal{B}_1 \to P$ be a set map into some module P. This extends to a set map $\mathcal{B} \to P$, by sending every element of $\mathcal{B}_1$ to zero. This induces, by the universal property of the free module $\mathcal{B} \to M$ a module homomorphism $M \to P$, which by construction kills N_1. Therefore this factors uniquely to a module homomorphism $M/N_1 \to P$ extending $\mathcal{B} \setminus \mathcal{B}_1 \to P$. The diagram



illustrates how $\mathcal{B} \setminus \mathcal{B}_1 \to P$ induces a map $M/N_1 \to P$. Two extensions $M/N_1 \to P$ of $\mathcal{B} \setminus \mathcal{B}_1 \to P$ give two maps $M \to P$ having the same restrictions to $\mathcal{B} \setminus \mathcal{B}_1$, but also killing N_1 and hence

having the same restriction to all of $\mathcal{B}$. Therefore uniqueness in the universal property for $B \hookrightarrow M$ implies that the two maps $M \to P$ are equal so the two maps $M/N_1 \to P$ must also be equal. Thus $\mathcal{B} \setminus \mathcal{B}_1 \to M/N_1$ is a free module.

Let $\overline{x}$ be a nonzero element of $\overline{M} = M/N_1$. It is a finite $\mathbf{Z}$-linear combination of $\mathcal{B} \setminus \mathcal{B}_1$ with at least one nonzero coefficient. It follows from uniqueness of the representations as $\mathbf{Z}$-linear combinations of $\mathcal{B} \setminus \mathcal{B}_1$ that for a positive integer k, there exists $\overline{m}$ in $\overline{M}$ such that $\overline{x} = k\overline{m}$ only if k divides each coefficient in the representation of $\mathbf{Z}$-linear combination of $\mathcal{B} \setminus \mathcal{B}_1$. Thus there are only finitely many such k.

(d) The mapping that takes $(b_1, b_2, b_3, \dots)$ to the real number

$$\sum \frac{\frac{1}{2}(1 + b_i/i!)}{2^i}$$

is a surjection of S onto $[0,1]$ since every element of $[0,1]$ has a binary expansion. Since $[0,1]$ is uncountable, S must be as well. Since $N_1 \cap S$ is countable, being contained in N_1, it cannot be all of S. Therefore there exists s in S with s not in N_1.

(e) Let s be an element of S not in N_1. For every positive integer k, let π_k be the module endomorphism $M \to M$ that sets the first $k-1$ coordinates to 0. For any positive integer k, $\pi_k(s) - s$ is in N and hence also in N_1 so $\pi_k(s)$ and s have the same image in $\overline{M}$. Say that an element of a module is divisible by k if there is some element of the module that when multiplied by k yields the original element. For a given k, each of the components of $\pi_k(s)$ is divisible by k so $\pi_k(s)$, as well as its image in $\overline{M}$, is divisible by k. Therefore the image of s in $\overline{M}$ is divisible by k for every positive integer k. This contradicts freeness of $\overline{M}$. Finally, the assumption that M was free led to a contradiction so M is not free. □

10.3.27. *(Free modules over noncommutative rings need not have a unique rank)* Let M be the $\mathbf{Z}$-module $\mathbf{Z} \times \mathbf{Z} \times \cdots$ of Exercise 24 and let R be its endomorphism ring, $R = \mathrm{End}_{\mathbf{Z}}(M)$ (cf. Exercises 29 and 30 in Section 7.1). Define $\varphi_1, \varphi_2 \in R$ by

$$\varphi_1(a_1, a_2, a_3, \dots) = (a_1, a_3, a_5, \dots)$$
$$\varphi_2(a_1, a_2, a_3, \dots) = (a_2, a_4, a_6, \dots).$$

(a) Prove that $\{\varphi_1, \varphi_2\}$ is a free basis of the left R-module R. [Define the maps ψ_1 and ψ_2 by $\psi_1(a_1, a_2, \dots) = (a_1, 0, a_2, 0, \dots)$ and $\psi_2(a_1, a_2, \dots) = (0, a_1, 0, a_2, \dots)$. Verify that $\varphi_i\psi_i = 1$,

$\varphi_1\psi_2 = 0 = \varphi_2\psi_1$ and $\psi_1\varphi_1 + \psi_2\varphi_2 = 1$. Use these relations to prove that φ_1, φ_2 are independent and generate R as a left R-module.]

(b) Use (a) to prove that $R \cong R^2$ and deduce that $R \cong R^n$ for all $n \in \mathbf{Z}^+$.

Solution.

(a) The identities may be verified by evaluating the compositions at an arbitrary element of M. Then the identities show that a pair of inverse left$R$-module homomorphisms between R and $R^{\oplus 2}$ are given by

$$\theta \mapsto (\theta\psi_1, \theta\psi_2) \qquad \text{and} \qquad (\theta_1, \theta_2) \mapsto \theta_1\varphi_1 + \theta_2\varphi_2.$$

Finally, R is a free left R-module on the basis $\{\varphi_1, \varphi_2\}$.

(b) The above left R-module homomorphisms are left R-module isomorphisms between R and $R^{\oplus 2}$. Then

$$R^{\oplus 2} = R \oplus R \cong R \oplus (R^{\oplus 2}) = R^{\oplus 3}$$

and so by induction $R \cong R^{\oplus n}$ for every positive integer n.

The explicit isomorphism of left R-modules $R \to R^{\oplus n}$ obtained from the above is

$$\theta \mapsto (\theta\psi_1, \theta\psi_2\psi_1, \ldots, \theta\psi_2^{n-2}\psi_1, \theta\psi_2^{n-1}). \qquad \square$$

Extra Problem. Let R be a commutative ring with 1. Show that there is no injective map of R-modules from $R^{\oplus 3}$ to $R^{\oplus 2}$.

Solution. Let $\phi\colon R^{\oplus 3} \to R^{\oplus 2}$ be an R-module homomorphism. Write $\mathbf{e}_i$ for the element of $R^{\oplus n}$ all of whose components are 0 except that the ith component is 1. Write $\phi(\mathbf{e}_i) = (a_{1i}, a_{2i})$ for $i = 1, 2, 3$. Then using the standard basis of $R^{\oplus n}$ to identify $R^{\oplus n}$ with $n \times 1$ column matrices, ϕ is equivalent to left multiplication by

$$\mathsf{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}.$$

Let r be the greatest nonnegative integer such that not all of the $r \times r$ minors of A vanish (by convention the determinant of a 0×0 matrix is the empty product, which equals 1). If $r = 0$, then ϕ is the zero map and so has nontrivial kernel. (We assume that R is a nonzero ring so $R^{\oplus 3}$ is a nonzero module.)

If $r = 1$, then

$$(1)\quad (-a_{12}, a_{11}, 0), (-a_{22}, a_{21}, 0), \\ (-a_{13}, 0, a_{11}), (-a_{23}, 0, a_{21}), \\ (0, -a_{13}, a_{12}), (0, -a_{23}, a_{22})$$

are all in the kernel of ϕ because each of the components of their images under ϕ may be expressed as either the determinant of a matrix in which one row is negative the other or the determinant of a 2×2 minor matrix of A, and moreover at least one element of $R^{\oplus 3}$ from (1) has a nonzero entry since one of the 1×1 minor matrices of A has nonzero determinant.

If $r = 2$, then

$$(2)\qquad (\det \left[\begin{smallmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{smallmatrix}\right], -\det \left[\begin{smallmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{smallmatrix}\right], \det \left[\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right])$$

is in the kernel of ϕ, as can be seen by cofactor expansion along the bottom rows of the matrices

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{11} & a_{12} & a_{13} \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{21} & a_{22} & a_{23} \end{bmatrix},$$

both with zero determinant, but at least one 2×2 minor of A does not vanish so the element of $R^{\oplus 3}$ in (2) is nonzero. This proves that ϕ is not injective. □

Note. More generally, one can determine conditions for a system of homogeneous R-linear equations to have a nonzero solution. The (McCoy) rank of a matrix with entries in the nonzero ring A is the greatest nonnegative integer r such that the collection of determinants of minor matrices of order r has trivial annihilator. (If $r < s$ then the annihilator of the collection of determinants of minor matrices of order r is contained in the annihilator of the collection of determinants of minor matrices of order s by cofactor expansion.)

Proposition. Over the nonzero ring R, the system of linear homogeneous equations

$$\textstyle\sum_{j=1}^{m} c_{ij} x_j = 0$$

for $i = 1, \ldots, n$ has a nontrivial solution if and only if the coefficient matrix $\mathsf{C} = [c_{ij}]$ has (McCoy) rank less than the number of unknowns.

Proof. Write adj for the adjugate of a square matrix. Let $(x_1, \ldots, x_m)$ be a nontrivial solution and let X be the $m \times 1$ column matrix $[x_i]$. For any $m \times m$ minor matrix C' of C,

$$(\det \mathsf{C}')\mathsf{X} = (\operatorname{adj} \mathsf{C}')\mathsf{C}'\mathsf{X} = 0.$$

Therefore a nonzero entry x_i of X is a nonzero annihilator of

$$\{\det \mathsf{C}' \mid \mathsf{C}' \text{ is an } m \times m \text{ minor matrix of } \mathsf{C}\}$$

so the rank of C is less than m.

Assume that the rank of C is $r < m$. If necessary we may throw in as many instances of the trivial equation $\sum_{j=1}^{m} 0x_j = 0$ needed to assume that $n \geq r+1$. There exists a nonzero element d of R that annihilates the determinant of any minor of C of order $r+1$. If $r = 0$, then $(d, 0, \ldots, 0)$ is a nontrivial solution so assume $r > 0$. There is some minor of C of order r whose determinant is not killed by d. For notational convenience we assume, by permuting the variables and equations, that the upper left $r \times r$ minor of C is not killed by d. Let C_i for $r+1 \leq i \leq n$ be the $(r+1) \times (r+1)$ matrix obtained by taking the $r \times (r+1)$ upper left submatrix of C and adjoining the left $1 \times (r+1)$ submatrix of the ith row of C. Let e_i be the $m \times 1$ matrix with zeros except for a 1 in the ith position. Define X to be the $m \times 1$ column matrix obtained from the $(r+1) \times 1$ column matrix $d(\operatorname{adj} \mathsf{C}_{r+1})\mathsf{e}_{r+1}$ by adjoining 0s. Note that X is nonzero as the $r+1$ entry is d times the determinant of the upper left $r \times r$ minor matrix. For $1 \leq i \leq r+1$,

$$\mathsf{e}_i^{\mathrm{T}} \mathsf{C}\mathsf{X} = d\mathsf{e}_i^{\mathrm{T}} \mathsf{C}_{r+1}(\operatorname{adj} \mathsf{C}_{r+1})\mathsf{e}_{r+1} = d \det(\mathsf{C}_{r+1})\mathsf{e}_i^{\mathrm{T}} \mathsf{e}_{r+1} = 0$$

and for $i \geq r+1$,

$$\mathsf{e}_i^{\mathrm{T}} \mathsf{C}\mathsf{X} = d\mathsf{e}_{r+1}^{\mathrm{T}} \mathsf{C}_i(\operatorname{adj} \mathsf{C}_{r+1})\mathsf{e}_{r+1} = d\mathsf{e}_{r+1}^{\mathrm{T}} \mathsf{C}_i(\operatorname{adj} \mathsf{C}_i)\mathsf{e}_{r+1} = d \det(\mathsf{C}_i) = 0$$

so X is the column matrix of a nontrivial solution. □

In particular, when the number of unknowns exceeds the number of equations there exists a nonzero solution.