

10 Classifying Modules

Copyright © 2025 by Gregory G. Smith
Last updated: 2025-11-27

Much like integers factoring into primes, finitely generated modules over a principal ideal domain have a decomposition into a direct sum of cyclic modules. This classification can also be viewed as a normal form for matrices over a principal ideal domain.

10.0 Submodules of Free Modules

Over a field, submodules of a free module are automatically free because every module over a field is free. What condition a ring guarantees that a submodule of a free module is again free?

10.0.1 Theorem. *Let R be a principal ideal domain. Every submodule of a finitely generated free R -module of rank n is free of rank at most n .*

We actually prove a more precise result.

10.0.2 Lemma. *Let R be a principal ideal domain and let V be a finitely generated free R -module. For any nonzero submodule U of V , there exists elements r in R , v in V , and u in U , and submodules V' of V and U' of U such that $u = r v$, $U' = V' \cap U$, $V = \langle v \rangle \oplus V'$, and $U = \langle u \rangle \oplus U'$.*

Proof. For any R -linear map $\varphi: V \rightarrow R$, the submodule $\varphi(U)$ is an ideal in R . The family of these ideals is nonempty. As principal ideal domains are noetherian, this family has a maximal element $\psi(U)$ for some R -linear map $\psi: U \rightarrow R$. By hypothesis, we have $U \neq 0$, so $\psi(U) \neq 0$. Since R is a principal ideal domain, there exists a nonzero element r in R such that $\psi(U) = \langle r \rangle$. As r in $\psi(U)$, there also exists an element u in U such that $\psi(u) = r$.

We claim that, for any R -linear map $\varphi: V \rightarrow R$, the element r divides $\varphi(u)$. Suppose that d generates the ideal $\langle r, \varphi(u) \rangle$. Let a and b be elements in R satisfying $d = a r + b \varphi(u)$. Consider the R -linear map defined by $\theta := a \psi + b \varphi$. As r in $\langle d \rangle$, we have $\psi(U) \subseteq \langle d \rangle$. We also have $d = a r + b \varphi(u) = (a \psi + b \varphi)(u) = \theta(u) \in \theta(U)$, whence $\langle d \rangle \subseteq \theta(U)$, so $\psi(U) \subseteq \theta(U)$. The maximality of $\psi(U)$ implies that $\psi(U) = \theta(U)$ and $\langle r \rangle = \langle d \rangle$, so the element r divides $\varphi(u)$.

By hypothesis, there exists a positive integer n and an R -module isomorphism $V \cong \bigoplus_{i=1}^n R = R^n$. Identify the element u in $U \subseteq V$ with the n -tuple $(s_1, s_2, \dots, s_n)$ in R^n ; each component $s_j := \varpi_j(u)$ is the image of u under the canonical map $\varpi_j: V \rightarrow R$. The previous paragraph shows that r divides s_i for all $1 \leq i \leq n$. Hence, there exists elements $c_1, c_2, \dots, c_n$ in R such that $s_i = r c_i$ for all $1 \leq i \leq n$. Let v in V be the element identified with the n -tuple $(c_1, c_2, \dots, c_n)$ in R^n . By construction, we have $u = r v$, so $r = \psi(u) = \psi(r v) = r \psi(v)$. As $r \neq 0$ and R is a domain, we deduce that $\psi(v) = 1_R$.

Let $V' := \text{Ker}(\psi)$ and set $U' := V' \cap U$. Every element w in V may be written as $w = \psi(w) v + (w - \psi(w) v)$. By linearity, we obtain

$\psi(w - \psi(w)v) = \psi(w) - \psi(w)\psi(v) = 0$, so $w - \psi(w)v \in \text{Ker}(\psi)$ and $V = \langle v \rangle + V'$. The relation $sv \in V'$ for some s in R implies that $0 = \psi(sv) = s\psi(v)$, which shows that $s = 0$ and $\langle v \rangle \cap V' = 0$. We deduce that $V = \langle v \rangle \oplus V'$.

When w in U , we see that the element r divides $\psi(w)$ because $\psi(w) \in \psi(U) = \langle r \rangle$. Writing $\psi(w) = tr$ for some t in R , we have $\psi(w)v = trv = tu$. Since $w - \psi(w)v = w - tu \in U \cap V' = U'$, the argument in the previous paragraph shows that $U = \langle u \rangle \oplus U'$. $\square$

Proof of Theorem 10.0.1. Let V be a finitely generated free R -module V and let U be a nonzero submodule of V . Lemma 10.0.2 gives an element u_1 in U and a submodule U_1 of U such that $U = \langle u_1 \rangle \oplus U_1$. If $U_1 = 0$, then we are done. Otherwise Lemma 10.0.2 produces u_2 in U_1 and a submodule U_2 of U_1 such that $U = \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus U_2$. Continuing this process gives $u_1, u_2, \dots, u_j$ in U and a submodule U_j such that $U = \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus \dots \oplus \langle u_j \rangle \oplus U_j$. However, we must have $j \leq \text{rank}_R V$ because the elements $u_1, u_2, \dots, u_m$ are linearly independent in V . Thus, the process must terminate, so we conclude that $U = \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus \dots \oplus \langle u_m \rangle$ for some $u_1, u_2, \dots, u_m$ in U . $\square$

10.0.3 Remark. The hypothesis that the ring R is a principal ideal domain is necessary. A ring R fails to be a principal ideal domain if it has a zerodivisor or a nonprincipal ideal. When R is not a domain, there exists nonzero elements a and b in R such that $ab = 0$. In this case, the principal ideal $\langle a \rangle$ is not a free R -module. When the domain R has a nonprincipal ideal I , no pair of nonzero elements f and g in I are linear independent because $(f)g + (-g)f = 0$.

10.0.4 Corollary. A domain R is a principal ideal domain if and only if, for any finitely generated R -module V and any surjective R -linear map $\varphi_0: R^{m_0} \rightarrow V$, there exists a nonnegative integer m_1 and an R -linear map $\varphi_1: R^{m_1} \rightarrow R^{m_0}$ such that the sequence

$$0 \longrightarrow R^{m_1} \xrightarrow{\varphi_1} R^{m_0} \xrightarrow{\varphi_0} V \longrightarrow 0$$

is exact.

Proof. Suppose that R is a principal ideal domain. Corollary 9.2.9 establishes that there is a nonnegative integer m_0 and a surjective R -linear map $\varphi_0: R^{m_0} \rightarrow V$. By Theorem 10.0.1, the submodule $\text{Ker}(\varphi_0)$ is free, so the choice of an isomorphism $\varphi_1: R^{m_1} \rightarrow \text{Ker}(\varphi_0)$ gives the desired exact sequence.

Conversely, let I be an ideal in R and consider the exact sequence

$$0 \longrightarrow I \longrightarrow R \longrightarrow \frac{R}{I} \longrightarrow 0.$$

The existence of the short exact sequence implies that the ideal I is a free submodule of R^1 of rank at most 1. Thus, any nonzero ideal is principal. $\square$

10.1 Matrices

By choosing bases for the source and the target for an R -linear map between free modules, we obtain a concrete representation.

10.1.1 Definition. Let R be a commutative ring. An $(m \times n)$ -matrix over R is a rectangular array

$$\mathbf{A} := \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{bmatrix} = [a_{i,j}]$$

where each $a_{i,j}$ lies in R . The set $\text{Mat}(m, n, R)$ of all $(m \times n)$ -matrices over R has a R -module structure defined entrywise: for any r and s in R , and any $\mathbf{A}$ and $\mathbf{B}$ in $\text{Mat}(m, n, R)$, we have

$$r\mathbf{A} + s\mathbf{B} = r[a_{i,j}] + s[b_{i,j}] = [ra_{i,j} + sb_{i,j}].$$

10.1.2 Definition. Let V be a finitely generated free R -module with basis $(v_1, v_2, \dots, v_n)$. For any v in V , there exists unique elements $b_1, b_2, \dots, b_n$ in R such that $v = b_1 v_1 + \cdots + b_n v_n$. The *matrix of v* with respect to this basis is defined to be

$$\mathbf{M}(v) := \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \in \text{Mat}(n, 1, R).$$

Let W be a free R -module with basis $(w_1, w_2, \dots, w_m)$ and consider an R -module homomorphism $\varphi: V \rightarrow W$. For any $1 \leq k \leq n$, there exists unique elements $a_{1,k}, a_{2,k}, \dots, a_{m,k}$ in R such that

$$\varphi(v_k) = a_{1,k} w_1 + a_{2,k} w_2 + \cdots + a_{m,k} w_m.$$

The *matrix of φ* with respect to these bases is

$$\mathbf{M}(\varphi) := \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{bmatrix} = [a_{i,j}]$$

This definition implies that, for any r and s in R , and any φ and ψ in $\text{Hom}_R(V, W)$, we have $\mathbf{M}(r\varphi + s\psi) = r\mathbf{M}(\varphi) + s\mathbf{M}(\psi)$. Once the bases of the source and target free modules are fixed, the map $\mathbf{M}: \text{Hom}_R(V, W) \rightarrow \text{Mat}(m, n, R)$ is an R -module isomorphism.

10.1.3 Definition. Consider positive integers ℓ , m , and n . For any matrix $\mathbf{A}$ in $\text{Mat}(\ell, m, R)$ and any $\mathbf{B}$ in $\text{Mat}(m, n, R)$, the *product $\mathbf{AB}$* in $\text{Mat}(\ell, n, R)$ is defined by $\mathbf{AB} := [\sum_k a_{i,k} b_{k,j}]$. This multiplication map $\text{Mat}(\ell, m, R) \times \text{Mat}(m, n, R) \rightarrow \text{Mat}(\ell, n, R)$ inherits properties from the ring R : for any r in R , and any compatible matrices $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$, we have

$$\begin{aligned} (\mathbf{AB})\mathbf{C} &= \mathbf{A}(\mathbf{BC}) & r(\mathbf{AB}) &= (r\mathbf{A})\mathbf{B} = \mathbf{A}(r\mathbf{B}) \\ \mathbf{A}(\mathbf{B} + \mathbf{C}) &= \mathbf{AB} + \mathbf{AC} & (\mathbf{A} + \mathbf{B})\mathbf{C} &= \mathbf{AC} + \mathbf{BC}. \end{aligned}$$

10.1.4 Example. Matrix multiplication is typically noncommutative. For instance, observe that

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}. \quad \diamond$$

10.1.5 Lemma. Let V and W be finitely generated free R -modules with chosen bases. For any v in V and any φ in $\text{Hom}_R(V, W)$, we have

$$M(\varphi(v)) = M(\varphi) M(v).$$

Proof. Let $(v_1, v_2, \dots, v_n)$ be the basis for V and let $(w_1, w_2, \dots, w_m)$ be the basis for W . When $M(\varphi) = [a_{i,j}]$ in $\text{Mat}(m, n, R)$ for some elements $a_{1,1}, \dots, a_{m,n}$ in R and $v = b_1 v_1 + b_2 v_2 + \dots + b_n v_n$ for some elements $b_1, b_2, \dots, b_n$ in R , we have

$$\varphi(v) = \sum_{j=1}^n b_j \varphi(v_j) = \sum_{j=1}^n b_j \left(\sum_{i=1}^m a_{i,j} w_i \right) = \sum_{i=1}^m \left(\sum_{j=1}^n a_{i,j} b_j \right) w_i,$$

so $M(\varphi(v)) = [\sum_j a_{i,j} b_j]$ as required. $\square$

10.1.6 Theorem. Let U, V , and W be finitely generated free R -modules with chosen bases. For any R -linear maps $\psi: U \rightarrow V$ and $\varphi: V \rightarrow W$, we have $M(\varphi \circ \psi) = M(\varphi) M(\psi)$.

Theorem 10.1.6 justifies the definition of matrix multiplication.

Proof. For any element u in U , Lemma 10.1.5 gives

$$\begin{aligned} M(\varphi \circ \psi) M(u) &= M((\varphi \circ \psi)(u)) \\ &= M(\varphi(\psi(u))) \\ &= M(\varphi) M(\psi(u)) = M(\varphi) M(\psi) M(u). \end{aligned}$$

Since $M(u)$ is arbitrary, the claim follows. $\square$

10.1.7 Definition. A matrix whose rows and columns have the same index set is *square*. Addition and multiplication of square matrices over a commutative ring R induce a noncommutative ring structure on $\text{Mat}(n, n, R)$. The multiplicative unit is identity matrix $I := [\delta_{i,j}]$. The group of invertible elements is $\text{GL}(n, R)$.

10.1.8 Proposition. Let R be a commutative ring and let V be a finitely generated free R -module with a chosen basis. The map $\varphi \mapsto M(\varphi)$ defines both a ring isomorphism between $\text{End}_R(V)$ and $\text{Mat}(n, n, R)$ and a group isomorphism between $\text{Aut}_R(V)$ and $\text{GL}(n, R)$.

Proof. Follows immediately from the definitions. $\square$

10.2 Diagonalizing Matrices

Since a finitely generated module over a principal ideal domain has a presentation, it is determined by a matrix. We may classify these modules by choosing appropriate bases of the source and target.

10.2.1 Definition. An $(m \times n)$ -matrix $A = [a_{i,j}]$ over a commutative ring R is *diagonal* if $a_{i,j} = 0$ whenever $i \neq j$.

10.2.2 Definition. Two $(m \times n)$ -matrices A and B over the ring R are *equivalent* if there is an invertible $(m \times m)$ -matrix C over R and an invertible $(n \times n)$ -matrix D over R such that $A = CBD$.

Equivalent matrices represent the same R -module homomorphism under different choices bases for the source and target.

10.2.3 Lemma. *Every matrix over a principal ideal domain is equivalent to a diagonal matrix.*

Proof. Let R be a principal ideal domain. For any elements a and b in R , Theorem 7.0.5 demonstrates that there exists x and y in R such that $d := \gcd(a, b) = ax + by$. Hence, for any p and q in R , we have

$$\begin{bmatrix} a & b \\ p & q \end{bmatrix} \begin{bmatrix} x & -b/d \\ y & a/d \end{bmatrix} = \begin{bmatrix} d & 0 \\ px + qy & (aq - bp)/d \end{bmatrix}$$

$$\begin{bmatrix} x & y \\ -b/d & a/d \end{bmatrix} \begin{bmatrix} a & p \\ b & q \end{bmatrix} = \begin{bmatrix} d & px + qy \\ 0 & (aq - bp)/d \end{bmatrix}$$

and

$$\det \begin{bmatrix} x & -b/d \\ y & a/d \end{bmatrix} = \det \begin{bmatrix} x & y \\ -b/d & a/d \end{bmatrix} = \frac{ax + by}{d} = 1.$$

Thus, if a and b are entries in the same row (respectively column) of a matrix B , we can multiply B on the right (respectively left) by an invertible matrix leaving d in the position occupied by a , leaving 0 in the position occupied by b , and fixing the entries not in the rows or columns of a and b .

Given a matrix A over the ring R , we claim that we can multiply on the left and right by invertible matrices to obtain a diagonal matrix. The case $A = 0$ is trivial, so assume that $A \neq 0$. Row and column interchanges (left and right multiplications by suitable permutation matrices) bring a nonzero element a_1 to the upper left corner. By a sequence of right multiplications by invertible matrices, replace a_1 by a_2 , the greatest common divisor of all elements in the first row, leaving zeros in the rest of the first row. Similarly, by left multiplications, replace a_2 by a_3 , the greatest common divisor of all elements now in the first column, leaving zeros in the rest of the first column. Continue by replacing a_3 by a_4 , the greatest common divisor of all elements now in the first row, and so on. In this manner, we create a sequence $\langle a_1 \rangle \supseteq \langle a_2 \rangle \supseteq \langle a_3 \rangle \supseteq \cdots$ of ideals. As R is a unique factorization domain, there exists an index m such that $a_{m+1} = a_m$. It follows that a_m is the greatest common divisor of the elements in the first row (or column) and the remaining elements

in the first column (or row) are zero. Hence, by elementary row or column operations, we can clear both the first row and first column, making all elements zero except for the corner. By induction on the size of the matrix, we can diagonalize A . $\square$

10.2.4 Definition. An $(m \times n)$ -matrix $A = [a_{i,j}]$ over a commutative ring R is in **Smith normal form** if it is diagonal and $a_{i,i}$ divides $a_{i+1,i+1}$ for all $1 \leq i < r \leq \min(m, n)$ and $a_{j,j} = 0$ for all $r \leq j \leq \min(m, n)$.

Working over the integers, this form was introduced by [Henry Smith \(1861\)](#).

10.2.5 Theorem. Every matrix over a principal ideal domain is equivalent to a matrix in Smith normal form.

Proof. By Lemma 10.2.3, it is enough to consider a diagonal matrix. For any a and b in R , Theorem 7.0.5 shows that there exists elements x and y in R such that $d := \gcd(a, b) = ax + by$. It follows that

$$\begin{aligned} \begin{bmatrix} x & y \\ -b/d & a/d \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} 1 & -by/d \\ 1 & ax/d \end{bmatrix} &= \begin{bmatrix} ax & by \\ -ab/d & ab/d \end{bmatrix} \begin{bmatrix} 1 & -by/d \\ 1 & ax/d \end{bmatrix} \\ &= \begin{bmatrix} d & 0 \\ 0 & ab/d \end{bmatrix}. \end{aligned}$$

Repeated application of this observation allow one to convert the diagonal matrix into a diagonal matrix with the property that the corner element divides all the remaining elements. By induction on the size of the matrix, we obtain a matrix in Smith normal form. $\square$

10.2.6 Lemma. Let A and B be equivalent $(m \times n)$ -matrix over a principal ideal domain. For all $1 \leq i \leq \min(m, n)$, the ideals generated by the determinants of all $(i \times i)$ -submatrices are equal.

Proof. For any $(m \times n)$ -matrix A and any $1 \leq i \leq \min(m, n)$, let $\Delta_i(A)$ be the ideal generated by the determinants of all $(i \times i)$ -submatrices of A . It suffices to show that, for any invertible $(m \times m)$ -matrix C , we have $\Delta_i(CA) = \Delta_i(A)$. The definition of matrix multiplication implies that the rows in the product CA are linear combinations of the rows in A . It follows that the determinants of $(i \times i)$ -submatrices of CA are linear combinations of the determinants of $(i \times i)$ -submatrices of A , so $\Delta_i(CA) \subseteq \Delta_i(A)$. Since C is invertible, we also have $\Delta_i(A) = \Delta_i(C^{-1}CA) \subseteq \Delta_i(CA)$, so $\Delta_i(CA) = \Delta_i(A)$. $\square$

10.2.7 Proposition. Two $(m \times n)$ -matrices A and B in Smith normal form over a principal ideal domain are equivalent if and only if there exists a unit u such that $a_{i,i} = u b_{i,i}$ for each $1 \leq i \leq \min(m, n)$.

Each matrix over a principal ideal domain is equivalent to an essentially unique matrix in Smith normal form.

Proof. One verifies that $\Delta_1(A) = \langle a_{1,1} \rangle$ and $\Delta_i(A) \langle a_{i+1,i+1} \rangle = \Delta_{i+1}(A)$ for all $1 \leq i \leq \min(m, n)$. Hence, the diagonal elements are, up to a unit, determined by the ideals $\Delta_i(A)$. Lemma 10.2.6 implies that two matrices in Smith normal form are equivalent if and only if these ideals are equal. $\square$

10.3 Modules over a Principal Ideal Domain

Smith normal form leads to a structure theorem for finitely generated modules over a principal ideal domain.

10.3.1 Theorem. *For any finitely generated module V over a principal ideal domain R , there exists a unique sequence $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ of proper ideals in R such that $V \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n$.*

Proof of existence. By Corollary 10.0.4, there is an exact sequence

$$0 \longrightarrow R^{m_1} \xrightarrow{\varphi} R^{m_0} \longrightarrow V \longrightarrow 0$$

where $m_1 \leq m_0$. Theorem 10.2.5 shows that, by choosing suitable bases for the free modules R^{m_1} and R^{m_0} , we may assume that the matrix $M(\varphi) = [a_{i,j}]$ is in Smith normal form. It follows that

$$V \cong \frac{R}{\langle a_{1,1} \rangle} \oplus \frac{R}{\langle a_{2,2} \rangle} \oplus \cdots \oplus \frac{R}{\langle a_{m_0, m_0} \rangle}$$

where $a_{i,i}$ divides $a_{i+1, i+1}$ for all $1 \leq i \leq m_1$. If $a_{i,i}$ is a unit, then $R/\langle a_{i,i} \rangle = 0$ is a trivial summand. Let ℓ be the largest integer such that $a_{\ell, \ell}$ is a unit. Setting $n := m_0 - \ell$ and $I_j := \langle a_{\ell+j, \ell+j} \rangle$ for all $1 \leq j \leq n$, we obtained the desired sequence of ideals in R . $\square$

Outline for proof of uniqueness. Suppose that there exists a sequence $J_1 \supseteq J_2 \supseteq \cdots \supseteq J_m$ of ideals such that $V \cong R/J_1 \oplus R/J_2 \oplus \cdots \oplus R/J_m$. We first claim that $m > n$ implies that $J_1 = R$. Setting $S := R/J_1$, we obtain the S -module isomorphisms

$$\bigoplus_{j=1}^m \frac{R}{J_j + J_1} \cong \frac{V}{J_1 V} \cong \bigoplus_{i=1}^n \frac{R}{I_i + J_1} = S^n.$$

Hence, we can map S^m onto S^n , which confirms that $S = 0$.

We may now assume that $m = n$. By symmetry, it suffices to show that $I_k \subseteq J_k$ for all $1 \leq k \leq n$. For any element r in I_k , we have

$$\bigoplus_{j=1}^n \frac{R}{(J_j : r)} \cong rV \cong \bigoplus_{i=k+1}^n \frac{R}{(I_i : r)}$$

where $(K : r) = \{a \in R \mid ra \in K\}$. Applying the first paragraph to the R -module rV , we deduce that $(J_1 : r) = (J_2 : r) = \cdots = (J_k : r) = R$, so x is in J_k . $\square$

10.3.2 Definition. The *torsion submodule* of an R -module V is

$$\tau(V) := \{v \in V \mid rv = 0 \text{ for some } 0 \neq r \in R\}.$$

10.3.3 Corollary. *Assume that R is a principal ideal domain. For any finitely generated R -module V , there exists a unique nonnegative integer r such that $V \cong \tau(V) \oplus R^r$.*

Proof. Theorem 10.3.1 gives a unique sequence $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ of proper ideals in R such that $V \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n$. Setting k to be the largest integer such that $I_k \neq \langle 0 \rangle$, it follows that

$$\tau(V) \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_k$$

and $V \cong \tau(V) \oplus R^{n-k}$. $\square$

Over a Euclidean domain, the Smith normal form of any matrix may be obtained via elementary row and columns operations.

10.3.4 Example. We illustrate this process for a matrix over $\mathbb{F}_{11}[x]$.

$$\begin{aligned}
 & \begin{bmatrix} 4x^3 + 4x^2 - x + 4 & -x^3 - x^2 + x + 1 & 3x^3 + 3x^2 + 5 \\ 4x^3 - 5x + 1 & -x^3 + 3x^2 + x - 3 & 3x^3 - 2x^2 - 4x + 3 \\ x^3 - x^2 + x - 1 & -3x^3 - x^2 + 3x + 1 & -2x^3 + x^2 + 4x - 3 \end{bmatrix} \\
 \equiv & \begin{bmatrix} 4x^3 + 4x^2 - x + 4 & -2x + 2 & 3x^3 + 3x^2 + 5 \\ 4x^3 - 5x + 1 & 3x^2 - 3x & 3x^3 - 2x^2 - 4x + 3 \\ x^3 - x^2 + x - 1 & -4x^2 - 5x - 2 & -2x^3 + x^2 + 4x - 3 \end{bmatrix} & \mathbf{c}_2 \mapsto \mathbf{c}_2 + 3\mathbf{c}_1 \\
 \equiv & \begin{bmatrix} 4x^3 + 4x^2 - x + 4 & x - 1 & 3x^3 + 3x^2 + 5 \\ 4x^3 - 5x + 1 & 4x^2 - 4x & 3x^2 - 2x^2 - 4x + 3 \\ x^3 - x^2 + x - 1 & 2x^2 - 3x + 1 & -2x^3 + x^2 + 4x - 3 \end{bmatrix} & \mathbf{c}_1 \mapsto 5\mathbf{c}_1 \\
 \equiv & \begin{bmatrix} x - 1 & 4x^3 + 4x^2 - x + 4 & 3x^3 + 3x^2 + 5 \\ 4x^2 - 4x & 4x^3 - 5x + 1 & 3x^2 - 2x^2 - 4x + 3 \\ 2x^2 - 3x + 1 & x^3 - x^2 + x - 1 & -2x^3 + x^2 + 4x - 3 \end{bmatrix} & \mathbf{c}_2 \leftrightarrow \mathbf{c}_1 \\
 \equiv & \begin{bmatrix} x - 1 & 0 & 0 \\ 4x^2 - 4x & -5x^4 - x^3 + 4x^2 + x + 1 & -x^4 + 2x^3 - 2x^2 - 2x + 3 \\ 2x^2 - 3x + 1 & 3x^4 - 3x^3 + 5x^2 + 3x + 3 & 5x^4 - 5x^3 + 4x^2 + 5x + 2 \end{bmatrix} & \begin{aligned} \mathbf{c}_2 &\mapsto \mathbf{c}_2 + (-4x^2 + 3x + 4)\mathbf{c}_1 \\ \mathbf{c}_3 &\mapsto \mathbf{c}_3 + (-3x^2 + 5x + 5)\mathbf{c}_1 \end{aligned} \\
 \equiv & \begin{bmatrix} x - 1 & 0 & 0 \\ 0 & -5x^4 - x^3 + 4x^2 + x + 1 & -x^4 + 2x^3 - 2x^2 - 2x + 3 \\ 0 & 3x^4 - 3x^3 + 5x^2 + 3x + 3 & 5x^4 - 5x^3 + 4x^2 + 5x + 2 \end{bmatrix} & \begin{aligned} \mathbf{r}_2 &\mapsto \mathbf{r}_2 + (-4x)\mathbf{r}_1 \\ \mathbf{r}_3 &\mapsto \mathbf{r}_3 + (-2x + 1)\mathbf{r}_1 \end{aligned} \\
 \equiv & \begin{bmatrix} x - 1 & 0 & 0 \\ 0 & -5x^4 - x^3 + 4x^2 + x + 1 & -5x^2 + 5 \\ 0 & 3x^4 - 3x^3 + 5x^2 + 3x + 3 & 3x^2 - 3 \end{bmatrix} & \mathbf{c}_3 \mapsto \mathbf{c}_3 + 2\mathbf{c}_2 \\
 \equiv & \begin{bmatrix} x - 1 & 0 & 0 \\ 0 & -5x^4 - x^3 + 4x^2 + x + 1 & x^2 - 1 \\ 0 & 3x^4 - 3x^3 + 5x^2 + 3x + 3 & -5x^2 + 5 \end{bmatrix} & \mathbf{c}_3 \mapsto 2\mathbf{c}_3 \\
 \equiv & \begin{bmatrix} x - 1 & 0 & 0 \\ 0 & x^2 - 1 & -5x^4 - x^3 + 4x^2 + x + 1 \\ 0 & -5x^2 + 5 & 3x^4 - 3x^3 + 5x^2 + 3x + 3 \end{bmatrix} & \mathbf{c}_2 \leftrightarrow \mathbf{c}_3 \\
 \equiv & \begin{bmatrix} x - 1 & 0 & 0 \\ 0 & x^2 - 1 & 0 \\ 0 & 0 & 3x^3 + 3x^2 - 3x - 3 \end{bmatrix} & \begin{aligned} \mathbf{c}_3 &\mapsto \mathbf{c}_3 + (5x^2 + x + 1)\mathbf{c}_2 \\ \mathbf{r}_3 &\mapsto \mathbf{r}_3 + 5\mathbf{r}_2 \end{aligned} \\
 \equiv & \begin{bmatrix} x - 1 & 0 & 0 \\ 0 & (x - 1)(x + 1) & 0 \\ 0 & 0 & (x - 1)(x + 1)^2 \end{bmatrix} & \mathbf{c}_3 \mapsto 4\mathbf{c}_3
 \end{aligned}$$

$\diamond$

10.4 Exercises

10.4.1 Problem. Let $\mathbb{F}_q$ be a finite field with q elements.

- i. For any nonnegative integer n , find the number of elements in the $\mathbb{F}_q$ -vector space $\mathbb{F}_q^n$.
- ii. Let $\text{GL}(n, \mathbb{F}_q)$ denote the group of all invertible $(n \times n)$ -matrices over the field $\mathbb{F}_q$. Determine the order of the group $\text{GL}(n, \mathbb{F}_q)$.
- iii. Let $\text{SL}(n, \mathbb{F}_q)$ be the subgroup of $\text{GL}(n, \mathbb{F}_q)$ consisting of matrices having determinant 1. Find the order of the group $\text{SL}(n, \mathbb{F}_q)$.

10.4.2 Problem. Let $R := \mathbb{Z}/\langle 30 \rangle$. Show that in the matrix

$$\begin{bmatrix} 1 & 1 & -1 \\ 0 & 2 & 3 \end{bmatrix} \in \text{Mat}(2, 3, R),$$

the rows are linearly independent, but any two columns are linearly dependent.

10.4.3 Problem. Consider the ring $\mathbb{Q}[x]$. Find a basis for the submodule of $\mathbb{Q}[x]^3$ generated by

$$f_1 := \begin{bmatrix} 2x - 1 \\ x \\ x^2 + 3 \end{bmatrix}, \quad f_2 := \begin{bmatrix} x \\ x \\ x^2 \end{bmatrix}, \quad \text{and} \quad f_3 := \begin{bmatrix} x + 1 \\ 2x \\ 2x^2 - 3 \end{bmatrix}.$$

Bibliography

- Arnold, Vladimir I. 1998. *On teaching mathematics*, Russian Math. Surveys 53, no. 1, 229–236.
- Cayley, Arthur. 1854. *On the theory of groups, as depending on the symbolic equation $\theta^n = 1$* , Phil. Mag. (4) 42, no. 7, 40–47.
- . 1893. *Note on the so-called quotient G/H in the theory of groups*, Amer. J. Math. 15, no. 4, 387–388.
- Cauchy, Augustin Louis. 1844. *Mémoire sur les arrangements que l'on peut former avec des lettres données et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre*, Exercices d'analyse et de physique mathématique 3, 151–252.
- Chevalley, Claude. 1943. *On the theory of local rings*, Ann. of Math. (2) 44, 690–708.
- Cox, David A. 2011. *Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first*, Amer. Math. Monthly 118, no. 1, 3–21.
- Dedekind, Richard. 1871. *Supplement X*, in *Vorlesungen über Zahlentheorie* by Peter Gustav Lejeune Dirichlet, Braunschweig: Vieweg.
- de Groot, Johannes. 1959. *Groups represented by homeomorphism groups*, Math. Ann. 138, 80–102.
- Dyck, Walther. 1882. *Gruppentheoretische Studien*, Math. Ann. 20, no. 1, 1–44.
- Eisenstein, Gotthold. 1850. *Über die Irreducibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt*, J. Reine Angew. Math. 39, 160–179.
- Frucht, Roberto. 1939. *Herstellung von Graphen mit vorgegebener abstrakter Gruppe*, Compositio Math. 6, 239–250.
- Galois, Évariste. 1846. *Œuvres Mathématiques*, J. Math. Pures Appl. XI, 381–444.
- Granville, Andrew. 2024. *It is not "Bézout's identity"*. available at [arXiv:2406.15642](https://arxiv.org/abs/2406.15642) [math.HO].
- Hilbert, David. 1890. *Über die Theorie der algebraischen Formen*, Mathematische Annalen 36, 473–534.
- . 1897. *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung 4, no. I–XVIII, 175–546.
- Hodges, Wilfrid. 1979. *Krull implies Zorn*, J. London Math. Soc. (2) 19, no. 2, 285–287.
- Jordan, Camille. 1861. *Mémoire sur le nombre des valeurs des fonctions*, Journal de l'École polytechnique 22, 113–194.
- . 1870. *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris. 667 p.
- Klein, Felix. 1884. *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, Teubner, Leipzig.
- Krull, Wolfgang. 1929. *Idealtheorie in Ringen ohne Endlichkeitsbedingung*, Math. Ann. 101, no. 1, 729–744.
- Lagrange, Joseph-Louis. 1771. *Suite des réflexions sur la résolution algébrique des équations. Section troisième. De la résolution des équations du cinquième degré & des degrés ultérieurs*, Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin 5, no. 4, 138–254.
- . 1795. *Leçon Cinquième. Sur l'usage des courbes dans la solution des problèmes*, Leçons Élémentaires sur les Mathématiques. Republished in Serret, Joseph-Alfred, ed. (1877). *Oeuvres de Lagrange*. Vol. 7. Gauthier-Villars. pp. 271–287.
- Miller, George Abram. 1910. *On a method due to Galois*, The Quarterly Journal of Pure and Applied Mathematics 41, 382–384.
- Möbius, August F. 1832. *Über eine besondere Art von Umkehrung der Reihen*, J. Reine Angew. Math. 9, 105–123.
- Noether, Emmy. 1921. *Idealtheorie in Ringbereichen*, Math. Ann. 83, no. 1-2, 24–66.
- . 1927. *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, Math. Ann. 96, no. 1, 26–61.
- Novikov, Pëtr Sergeevich. 1955. *Ob algoritmičeskoj nerazrešimosti problemy toždestva slov v teorii grupp*, Izdat. Akad. Nauk SSSR, Moscow. Trudy Mat. Inst. Steklov. no. 44.

- Poonen, Bjorn. 2019. *Why all rings should have a 1*, Math. Mag. 92, no. 1, 58–62.
- Sabidussi, Gert. 1960. *Graphs with given infinite group*, Monatsh. Math. 64, 64–67.
- Schönemann, Theodor. 1846. *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*, J. Reine Angew. Math. 32, 93–105.
- Smith, Henry J. S. 1861. *On systems of linear indeterminate equations and congruences*, Philos. Trans. Roy. Soc. . 151, 293–32.
- Sylow, Ludwig. 1872. *Théorèmes sur les groupes de substitutions*, Math. Ann. 5, no. 4, 584–594.
- Waring, Edward. 1779. *Problems concerning interpolations*, Philosophical Transactions of the Royal Society 69, 59–67.
- Wielandt, Helmut. 1959. *Ein Beweis für die Existenz der Sylowgruppen*, Arch. Math. 10, no. 1, 401–402.
- Zorn, Max. 1935. *A remark on method in transfinite algebra*, Bull. Amer. Math. Soc. 41, no. 10, 667–670.