Math 676: Algebra 1

Jeffrey Ayers

Fall 2020

About This Course

This course is the first of the graduate Algebra sequence, and is an introduction to Rings, Modules, Linear Algebra, and Advanced Group theory. It was taken in the Fall of 2019 at UNC Chapel Hill, and taught by Prof. David Rose, and we used Dummit and Foote's text Abstract Algebra. These notes were copied from the ones in my notebook and any mistakes are mine and not the lecturers.

Contents

1 Rings

1.1 Introduction

Definition. A ring is a set R with two binary operations, denoted $+$ and $\cdot$ such that

- $(R, +)$ is an abelian group
- $\cdot$ is associative
- The distributive law should hold
- * There is a unit $1 \in R$

The last requirement is different from Dummit and Foote but we always want to work with unital rings. Dropping this requirement will be called a "rng"

R is commutative if the multiplication is commutative

Example. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$

Definition. A subring is a subset $S \subset R$ which is a ring

Definition. An integral domain, or domain, is a nonzero ring (commutative) R with no zero-divisors: An element $a \in R \setminus \{0\}$ such that there is $b \in R \setminus 0$ which makes $ab = ba = 0$

Definition. A field is a nonzero commutative ring such that every non-zero element is a unit: an element $u \in R$ such that there is v for which $uv = vu = 1$

Remark: In any ring R the set of units $R^\times$ form a group

Proposition. A finite integral domain is a field

Proof. Recall that we can "cancel" in an integral domain:

$$ab = ac \implies ab - ac = 0 \implies a(b - c) = 0$$

Integral domains have no zero-divisors thus $a = 0$ or $b - c = 0$ Now let R be finite int domain, then we need to find multiplicative inverses for all elements.

Let $r \in R \setminus \{0\}$ this defines a function

$$m_r : R \to R$$

$$a \mapsto ra$$

This function is injective because we can cancel, and hence is surjective as R is finite. So there is an element $a \in R$ such that $ra = 1$ □

More examples of rings:

Example.

- Let D be a squarefree integer, and define

$$\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$$

This is a subring of $\mathbb{C}$, and further is a field

- Inside the above field we have the ring of integers

  $$\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$$

  For

  $$\omega = \begin{cases} \sqrt{D} & D \equiv 2, 3 \mod 4 \\ \frac{1+\sqrt{D}}{2} & D \equiv 1 \mod 4 \end{cases}$$

  We want to find the units in $\mathbb{Z}[\omega]$. To do this consider the function

  $$N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$$

  $$a + b\sqrt{D} \mapsto a^2 - Db^2$$

Proposition. $r \in \mathbb{Z}[\omega]$ is a unit iff $N(r) = \pm 1$

Proof. A computation shows that for all $\alpha, \beta \in \mathbb{Q}[\sqrt{D}]$, $N(\alpha\beta) = N(\alpha)N(\beta)$, and if $r \in \mathbb{Z}[\omega]$ then $N(r) \in \mathbb{Z}[\omega]$. Thus if r is a unit we have that there is some $s \in \mathbb{Z}[\omega]$ for which $rs = 1$ hence

$$1 = N(1) = N(rs) = N(r)N(s)$$

Thus $N(r) = \pm 1$

Conversely can check that if $N(r) = \pm 1$ then $(a + b\omega)^{-1} = \pm(a + b\overline{\omega})$ □

Example. Polynomial rings. Let R be commutative and define $R[x]$ to be the ring of polynomials with finite degree, and coefficients in R. This is a ring with polynomial addition and multiplication.

When R is a domain the following hold:

- $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$
- The units in $R[x]$ are the units in R
- $R[x]$ is a domain (iff statement)
- Let R be a ring, then $M_n(R)$, the set of $n \times n$ matrices with entries in R is a ring with the usual operations. For $R \neq 0$ and $n \geq 1$, $M_n(R)$ isn't commutative

Note that for the last item the upper triangular matrices are a subring, and the group of units in $M_n(R)$ is denoted $GL_n(R)$.

Definition. Let R, S be rings. A ring homomorphism $\varphi : R \to S$ is a homomorphism of abelian groups so that

- $\varphi(ab) = \varphi(a)\varphi(b)$ for $a, b \in R$
- $\varphi(1_R) = 1_S$

Observation. There are no ring homomorphisms from 0 to any ring. $\varphi(0) = 0 \neq 1_R$

Recall that $\ker \varphi = \{a \in R : \varphi(a) = 0\}$ is an ideal in R, but not a subring as it does not contain 1.

Definition. We call $\varphi : R \to S$ an isomorphism provided there is a ring homomorphism $\psi : S \to R$ such that $\varphi \circ \psi = Id_S$ and $\psi \circ \varphi = Id_R$

The above is a better formulation of isomorphism, but note we could also just say that φ would need to be a bijection, or that it's a surjective map with 0 kernel.

Example. There is a unique ring homomorphism $\mathbb{Z} \to \mathbb{R}$ determined by 1

Example. $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is defined by $a \mapsto a \mod n$

Definition. Let R be a ring, and $I \subset R$ a subgroup with respect to $+$.

- I is called a left ideal if for all $r \in R, a \in I$, $ra \in I$
- I is a right ideal if $ar \in I$
- I is an ideal if both a left and right ideal.

Since $(R, +)$ is abelian, every subgroup is normal, thus we can consider the quotient group R/I for any subgroup $I \subset R$. If I is an ideal, then the operations

- $(a + I) + (b + I) = (a + b) + I$
- $(a + I)(b + I) = (ab) + I$

Turn R/I into a ring called the quotient ring.

We now discuss the analogues of isomorphism theorems for ring.

Theorem (Ring Isomorphism Theorems)**.** These are similar to the group ones.

1) Let $\varphi : R \to S$ be a ring homomorphism, then
$$\text{im}\varphi \cong R/\ker\varphi$$
as rings

2) Let $I \subset R$ be an ideal and $S \subset R$ be a subring. Then
$$S + I/I \cong S/S \cap I$$
as rings

3) Let $I \subset J \subset R$ be ideals, then
$$(R/I)\,/\,(J/I) \cong R/J$$

4) Let $I \subset R$ be an ideal, then there is a bijection between
$$\text{Ideals } J \subset R \text{ with } I \subset J \iff \text{Ideals in } R/I$$

Proposition. Let I, J be ideals in R, then the following are ideals:

- $I + J = \{i + j : i \in I, j \in J\}$
- $IJ = \{\sum a_i b_i : a_i \in I, b_i \in J\}$

- $I \cap J$

Example. Every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$, and $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$ where d is the $\gcd(n, m)$

Definition. Let $A \subset R$ be a subset, then the ideal generated by A, denoted (A) is the smallest ideal in R that contains A.

We say that this ideal is principal if $A = \{a\}$ and denote it (a). We say it's finitely generated if $A = \{a_1, ..., a_n\}$, and write $(A) = (a_1, ..., a_n)$. Note: If R if commutative then $(a) = \{ra : r \in R\}$ and $(a_1, ..., a_n) = \{r_1a_1 + \cdots + r_na_n\}$

Next we look at the relation between ideals, domains, and fields.

Note: An ideal $I = R$ if and only if I contains a unit, which implies that R is a field if and only if the only ideals are 0 and R.

Definition. An ideal $M \neq R$ is called maximal if $M \subsetneq I$ for some ideal I means that $I = R$

Recall that an argument using Zorn's lemma implies that any proper ideal $I \subset R$ is contained in some maximal ideal. Thus the lattice isomorphism theorem yields the following:

Proposition. Let R be commutative, then $I \subset R$ is maximal if and only if R/I is a field.

Finally we recall

Definition. An ideal $P \neq R$ is called prime if $ab \in P$ means that $a \in P$ or $b \in P$

Which gives the following:

Proposition. Let R be commutative, then $I \subset R$ is prime if and only if R/I is an integral domain

Corollary. Every maximal ideal is prime

1.2 Special kinds of integral domains

Recall that every ideal in $\mathbb{Z}$ takes the form $n\mathbb{Z} = (n)$ and $(n) + (m) = (\gcd(n, m))$ this follows from the Euclidean Algorithm, which gives Bezout's lemma.

Definition. An integral domain R is a Euclidean Domain provided there exists a "Euclidean norm" function

$$N : R \to \mathbb{Z}^{\geq 0}$$

so that for all $a, b \in R$ with b nonzero, there exists $q, r \in R$ so that $a = qb + r$ with either

- $r = 0$, or
- $N(r) < N(b)$

This implies we can run the Euclidean algorithm for our Euclidean Domain.

Example. Any field K with $N(a) = 0$ for all $a \in K$ (as we can always divide in a field)

Example. $\mathbb{Z}$ with $N(a) = |a|$

Example. $K[x]$ with $N(a) = \deg(p(x))$

Example. $\mathbb{Z}[i]$ with $N(a+bi) = a^2 + b^2$.

Be careful! Not all $\mathbb{Z}[\omega]$'s are Euclidean domains

Example. Any discrete valuation ring

Proposition. Every ideal in a Euclidean domain is principal

Proof. Let $I \neq 0$ be an ideal. Note that the following set $\{N(a) : a \in I, a \neq 0\}$ is a nonempty subset in $\mathbb{Z}^{\geq 0}$ thus it hasa smallest element by well-ordering. Let $d \in I$ be a nonzero element with this smallest norm.

Claim: $(d) = I$. Clearly $(d) \subset I$. Now for the other direction take $a \in I$ then write $a = qd + r$, either $r = 0$, in which case $a|d$ so $I \subset (d)$, or $N(r) < N(d)$, but the latter case cannot happen as d was assumed to have smallest norm. □

This suggests the following definition:

Definition. An integral domain R is called a PID if every ideal in R is principal.

Corollary. Every Euclidean domain is a PID

PID's are nice, as they provide the natural setting for studying the greatest common division.

Definition. Let R be commutative, and let $a, b \in R$. We say that d is a greatest common divisior of a and b provided

1: $d|a$ and $d|b$

2: If $d'|a$ and $d'|b$ then $d'|d$

Note that we always have $x|y \iff y \in (x) \iff (y) \subset (x)$. Thus $d = \gcd(a,b) \iff (a,b) \subset (d)$ and if $(a,b) \subset (d')$ then $(d) \subset (d')$. Hence we can say that the gcd generates the smallest principal ideal containing (a,b).

Proposition. Let R be a PID, then

1) $(a,b) = (d) \iff d = \gcd(a,b)$

2) $\gcd(a,b)$ can be written as a linear combination of a, b (This is saying Bezout's lemma holds). $\gcd(a,b) = xa + yb$

3) If d_1, d_2 are both $\gcd(a,b)$ then there is a unit u for which $d_1 = ud_2$

Claim: The last nonzero remainder in the Euclidean Algorithm is a $\gcd(a,b)$. This can be shown via induction.

Recall that all nonzero prime ideals in $\mathbb{Z}$ take the form (p) for a prime p, hence is maximal as $\mathbb{Z}/p\mathbb{Z}$ is a field. This leads to the next proposition

Proposition. Any nonzero prime ideal in a PID is maximal

Proof. Let $P \neq 0$ be prime and in a PID R. Thus $P = (p)$, and assume that $P \subseteq I$ for some ideal I generated by a, hence $(p) \subset (a)$. As such $am = p$ for some $m \in R$. So we have two possibilities:

If $a \in (p)$ then we're done as this means that $(a) \subset (p)$, hence $I = P$

If $m \in (p)$ then $m = pk = (am)k \implies 1 = ak$ so a is a unit and hence $(a) = R$ □

Corollary. Let R be commutative, then $R[x]$ is a PID iff R is a field.

Proof. If R is a field, then $R[x]$ is a Euclidean domain, and hence a PID.

If $R[x]$ is a PID, then $R[x]/(x)$ is an integral domain, so (x) is prime, and nonzero so it's maximal, therefore $R[x]/(x) \cong R$ is a field □

We now turn our attention to UFDs which allow us to study an abstraction of the Fundamental Theorem of Arithmetic.

Definition. Let R be an integral domain, then

1) $r \in R \setminus (R^\times \cup \{0\})$ is called irreducible provided whenever $r = ab$ either a or b is a unit.

2) $p \in R \setminus \{0\}$ is prime whenever (p) is a prime ideal.

Proposition. Let p be prime, then it is irreducible

Proof. Assume p is prime, and that $p = ab$. Then (p) is a prime ideal, and so $a \in (p)$ or $b \in (p)$. WLOG assume $a \in (p)$, then $a = pm \implies a = (ab)m \implies 1 = bm$ so b is a unit. □

We now observe that the converse is generally false. Consider the ring $\mathbb{Z}[\sqrt{-5}]$ and recall its field norm

$$N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}^{\geq 0}$$
$$a + b\sqrt{-5} \mapsto a^2 + 5b^2$$

Recall also that $u \in \mathbb{Z}[\sqrt{-5}]$ is a unit iff $N(u) = 1$.

Claim: $3 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible. Assume that $3 = \alpha\beta = (a + b\sqrt{-5})\beta$. Then

$$9 = N(3) = N(\alpha\beta) = N(\alpha)N(\beta) = (a^2 + 5b^2)N(\beta)$$

So $a^2 + 5b^2 = 1, 3, 9$. If it's 1 or 9 then α, or β is a unit, and 3 has no integer solutions.

Claim: $3 \in \mathbb{Z}[\sqrt{-5}]$ is not prime. Note that $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$ so $3|6$ which means $3|(1 + \sqrt{-5})(1 - \sqrt{-5})$ but we cannot have this. If $3(x + y(\sqrt{-5})) = (1 \pm \sqrt{-5})$ then $3x = 1$ and $x \notin \mathbb{Z}$

But not all is lost:

Proposition. Let R be a PID, then $r \in R$ is irreducible iff prime

Proof. $(\Leftarrow)$ Done.

$(\Rightarrow)$ If $r \in R$ is irreducible, then for $r = ab$ one of a or b is a unit. Consider the ideal (r), then suppose $(r) \subset (a)$, hence $r = ab$ so one of these is a unit. If a is a unit, then $(a) = R$, if b is a unit, then $(a) = (r)$. In either case we have a maximal ideal, which is prime in a PID. □

Corollary. $\mathbb{Z}[\sqrt{-5}]$ is not a PID

In fact this proposition holds for a larger class of rings

Definition. An integral domain R is a UFD provided given any $r \in R \setminus (R^\times \cup \{0\})$ the following hold

1) r can be written as $r = r_1 \cdots r_n$ with each r_i irreducible
2) This factorization is unique up to units and reordering

Here is the full picture of containments in integral domains:

$$\{\text{Fields}\} \subsetneq \{\text{Euclidean Domains}\} \subsetneq \{\text{PIDs}\} \subsetneq \{\text{UFDs}\} \subsetneq \{\text{Integral Domains}\}$$

Example. An example of a Euclidean Domain that is not a Field is $\mathbb{Z}$

Example. An example of a PID that is not a Euclidean Domain is $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$

Example. An example of a UFD that is not a PID is $\mathbb{Z}[x]$

Example. An example of an Integral Domain that is not a UFD is $\mathbb{Z}[\sqrt{-5}]$

Proposition. Let R be a UFD, then $r \in R$ is irreducible if and only if it's prime.

Proof. Let $r \in R$ be irreducible, and suppose that $r|ab$, so $rc = ab$ for some $c \in R$. Then since we can assume that a, b, c are not zero or units we can factor into irreducibles:

$$(a_1 \cdots a_n)(b_1 \cdots b_n) = r(c_1 \cdots c_n)$$

Thus WLOG $a_1 = ru$ for $u \in R^\times$ hence $a = r(ua_1a_2 \cdots a_n)$ so $r|a$ □

Theorem. Let R be a PID, then it's a UFD

In a PID prime ideals are the same as maximal ideals. In a UFD prime elements are the same as irreducible elements.

Lemma. Let $\alpha \in \mathbb{Z}[i]$ with $N(\alpha) = p$, a prime in $\mathbb{Z}$, then α is prime.

Proof. Let $\alpha = \beta\gamma$ then $\pm p = N(\beta)N(\gamma)$ thus WLOG $N(\gamma) = \pm 1$ so γ is a unit. Thus α is irreducible, hence prime. □

This is not an iff statement however.

Lemma. Let $\alpha \in \mathbb{Z}$ be prime, then there is a prime $p \in \mathbb{Z}$ so that

- $\alpha = up$ for unit $u \implies N(\alpha) = \pm p^2$, OR
- There is a prime $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = p$ so $N(\alpha) = p = N(\beta)$ hence $p = a^2 + b^2$

Proof. FILL IN □

Thus we conclude that

Proposition. Up to multiplication by units, the primes in $\mathbb{Z}[i]$ are precisely

- $p \in \mathbb{Z}$ that cannot be written as $a^2 + b^2$, OR
- $\alpha = a \pm bi$ where $a^2 + b^2 = p$ is a prime in $\mathbb{Z}$

Note that if p is odd, then $p = a^2 + b^2 \implies p \equiv 1 \mod 4$

Lemma. A prime $p \in \mathbb{Z}$ divides an integer of the form $n^2 + 1 \iff p = 2$ or $p \equiv 1 \mod 4$

Proof. FILL IN □

1.3 Polynomial Rings

Proposition. Let K be a field, then $K[x]$ is a Euclidean domain, where $N(p(x)) = \deg p(x)$. Moreover the quotient and remainder in the division algorithm are unique

This implies $K[x]$ is a PID and a UFD. This proposition immediately gives the following

Corollary. Let K be a field, and $p(x) \in K[x]$, then $p(x)$ has a root in K iff $p(x)$ has a degree one factor

Corollary. Let K be a field, and $p(x) \in K[x]$ of degree n, then $p(x)$ has at most n roots.

This fact gives the following:

Proposition. A finite subgroup of the group of units in a field is cyclic

Proof. Let K be a field, and $G \subseteq K^\times$ be finite. Since G is abelian we know that

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

such that $n_1|n_2|\cdots|n_k$. Thus G has (at least) n_1^k elements of order dividing n_1. However each element of order dividing n_1 gives a root of the polynomial $x^n - 1$, thus we must have $k = 1$ □

Corollary. $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic

Next note that since $K[x]$ is a PID we exactly know the structure of its ideals:

- Every ideal takes the form $(f(x))$ for $f(x) \in K[x]$
- Such ideals are irreducible iff prime iff maximal

But how do we tell if $f(x)$ is irreducible?

Let R be an integral domain, and recall that we can consider its field of fractions

$$F = \{(a, d) : a \in R, d \in R \setminus \{0\}\}/\{(a_1, d_1) \sim (a_2, d_2) \iff a_1 d_2 = a_2 d_1\}$$

We know we have the Gauss Lemma

Proposition. Let R be a UFD, and F it's field of fractions, if $p(x) \in R[x]$ is reducible in $F[x]$ then $p(x)$ is reducible when viewed as an element in $R[x]$.

Proof. FILL IN □

Definition. Let R be a UFD and $p(x) \in R[x]$ then the content of $p(x)$ is the gcd of all its coefficients. We say that $p(x)$ is primitive if its content is 1

Corollary. FILL IN

Theorem. R is a UFD iff $R[x]$ is a UFD

Proof. FILL IN □

Corollary. $\mathbb{Z}[x]$ is a UFD, but not a PID

Let's discuss criterion for irreducibility. First is the rational roots test

Proposition. Let R be a UFD, F its field of fractions. If $\frac{r}{s} \in F$ is a root of a polynomial in $R[x]$ then r divides the constant term and s divides the leading coefficient.

Proof. FILL IN □

This is especially useful for when $p(x)$ is monic.

Example. $x^3 - 7x - 1$ is irreducible in $\mathbb{Z}[x]$. Indeed, it's primitive, so if it wasn't it would factor in $\mathbb{Q}[x]$. If this is the case it would have a degree 1 factor, hence a root in $\mathbb{Q}$, but such a root must be ± 1 and these aren't roots.

Next, the idea we saw of reducing coefficients modulo an ideal can also be useful.

Proposition. Let R be an integral domain and $I \subsetneq R$ a proper ideal. Let $p(x) \in R[x]$ be monic and nonconstant such that $\overline{p(x)} \in (R/I)[x]$ cannot be factored into polynomials of strictly lower degree, then $p(x)$ is irreducible.

Proposition (Eisenstein's Criterion)**.** Let $p \in \mathbb{Z}$ be prime, and suppose that

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

$n \geq 1$ with $p|a_i$, $i \in \{0, 1, ..., n-1\}$ but $p^2 \nmid a_0$, then $f(x)$ is irreducible over both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Proof. FILL IN □

Example. For p-prime the cyclotomic polynomial is ... FILL IN

2 Linear Algebra

2.1 Basic properties

Let k be a field, and let V be a k-vector space

Definition. A basis for V is a subset $B \subset V$ that spans V and is linearly independent

Definition (Span)**.** $\forall v \in V \ v = \sum_{i=1}^{k} \alpha_i b_i$ for $b_i \in B, \alpha_i \in k$

Definition (Linear independent)**.** If $\sum_{i=1}^{k} \alpha_i b_i = 0$ for $b_i \in B, \alpha_i \in k$ then $\alpha_i = 0$ for all i

Recall that Zorn's lemma says

Theorem. Every vector space has a basis

Here is an alternative characterization of bases in the finite dimensional case (finite spanning set)

Proposition. Suppose that a finite set spans V, but no proper subset spans, then the set is a basis.

Next we have

Theorem (Replacement Theorem)**.** Let $\{b_1, ..., b_n\}$ be a basis for V, and let $\{r_1, ..., r_m\}$ be a set of linearly independent vectors, then for all $1 \leq k \leq m$, there is a reordering of the $b_i's$ so that

$$\{r_1, .., r_k, b_{k+1}, ..., b_n\}$$

is a basis. In particular $m < n$

Proof. FILL IN □

This has the important consequence:

- Let V have a basis with exactly n-vectors, then $\dim V = n$, and any linearly independent set has $\leq n$ vectors, and and spanning set has $\geq n$ vectors.
- Any linearly independent subset of a finite dimensional vector space can be extended to a basis.

This then gives

Corollary. Let $W \subseteq V$ be a subspace, then

$$\dim V/W = \dim V - \dim W$$

Proof Sketch. Take a basis for W and extend to one for V □

Which gives the "rank-nullity theorem"

Theorem. Let $\varphi : V \to U$ be a linear map, then

$$\dim V = \dim \ker \varphi + \dim \mathrm{im} \varphi$$

Let V, U be k-vector spaces and let $\mathrm{Hom}_k(V, U)$ be the set of linear transformations

Proposition. $\mathrm{Hom}_k(V, U)$ is a k-vector space under the operations

$$(\alpha\varphi)(v) = \alpha \cdot \varphi(v) \qquad \text{for } \alpha \in K$$

$$(\varphi_1 + \varphi_2)(v) = \varphi_1(v) + \varphi_2(v)$$

Suppose we've chosen bases $\{v_1, ..., v_n\}$ and $\{u_1, ..., u_m\}$ for finite dimensional V, U. This determines isomorphisms $V \cong k^n, U \cong k^m$. Given any $\varphi \in \mathrm{Hom}_k(V, U)$ we can consider

$$\begin{tikzcd} V \arrow[r, "\varphi"] & U \arrow[d, "g"] \\ k^n \arrow[u, "f"] \arrow[r, "A\varphi"] & k^m \end{tikzcd}$$

Where $f : e_i \mapsto v_i$, $g : u_i \mapsto e_i$, and $A\varphi = g \circ \varphi \circ f$

Let $M_{m\times n}(k)$ denote the vector space of all $m \times n$ matrices with entries in k, then

Proposition. $\mathrm{Hom}_k(V, U) \cong M_{m\times n}(k)$

Proof. After choosing f, g we can send $\varphi \mapsto g \circ \varphi \circ f$ and $A \mapsto g^{-1} \circ A \circ f^{-1}$ □

Corollary. If $\dim(V) = n$ and $\dim(U) = m$ then

$$\dim(\mathrm{Hom}_k(V, U)) = mn$$

There are two special cases

1) $U = V$ then we denote $\mathrm{End}_k(V) = \mathrm{Hom}_k(V, V)$ in this case we have an additional operation on this space given by composition: $\varphi_1 \circ \varphi_2 \in \mathrm{End}_k(V)$ for $\varphi_1, \varphi_2 \in \mathrm{End}_k(V)$ which turns

3 Modules

4 Bilinear Forms

5 Group Theory