GALOIS THEORY
TOPIC VII
VECTOR SPACES

PAUL L. BAILEY

ABSTRACT. Vector spaces are algebraic structures which admit addition and scalar multiplication. The scalar can come from any field. We wish to show that to each vector space we may attach a unique nonnegative integer known as its *dimension*, which is the size of any *basis*.

1. FIELDS

We begin by reviewing some aspects of the mathematical objects called fields.

Definition 1. A *field* is a set F, together with a pair of operations,

$$+ : F \times F \to F \quad \text{and} \quad \cdot : F \times F \to F,$$

called addition and multiplication, satisfying

- **(F1)** if $a, b \in F$, then $a + b = b + a$;
- **(F2)** if $a, b, c \in F$, then $(a + b) + c = a + (b + c)$;
- **(F3)** there exists $0 \in F$ such that $a + 0 = a$ for every $a \in F$;
- **(F4)** for every $a \in F$ there exists $-a \in F$ such that $a + (-a) = 0$;
- **(F5)** if $a, b \in F$, then $ab = ba$;
- **(F6)** if $a, b, c \in F$, then $(ab)c = a(bc)$;
- **(F7)** there exists $1 \in F \setminus \{0\}$ such that $a \cdot 1 = a$ for every $a \in F$;
- **(F8)** if $a \in F \setminus \{0\}$ there exists $a^{-1} \in F$ such that $aa^{-1} = 1$;
- **(F9)** if $a, b, c \in F$, then $(a + b)c = ac + bc$.

We define two more operations: *subtraction* is an operator $- : F \times F \to F$ defined by $a - b = a + (-b)$ for all $a, b \in F$, and *division* is an operator $\div : F \times F^* \to F$ defined by $a \div b = ab^{-1}$, where $F^* = F \setminus \{0\}$

We give some examples of fields, beginning with the set of numbers emphasized by calculus.

Example 1. The set $\mathbb{R}$ of real numbers is a field.

Example 2. The set $\mathbb{Q}$ of rational numbers is a field. It adheres to properties **(F1)** through **(F9)**, as does any subset of $\mathbb{R}$; moreover, the operations are closed on $\mathbb{Q}$; the sum, difference, product, and quotient of two rational numbers is another rational number.

A field is not required to be an ordered set.

Example 3. The set $\mathbb{C}$ of complex numbers is a field. One can show that $\mathbb{C}$ does not admit a total ordering which is compatible with its algebraic structure.

Date: October 27, 2006.

Neither is a field required to be infinite, and there are finite fields.

Example 4. Let $\mathbb{Z}_2 = \{0, 1\}$. Define addition and multiplication on $\mathbb{Z}_2$ by the following tables:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Together with these operations, $\mathbb{Z}_2$ is a field.

Example 5. Let $\mathbb{Z}_3 = \{0, 1, 2\}$. Define addition and multiplication on $\mathbb{Z}_3$ by the following tables:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Together with these operations, $\mathbb{Z}_3$ is a field.

Let the symbol $\triangleq$ mean "is defined to be".

Example 6. The previous examples are special cases of the fields $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, where p is a prime integer, and addition and multiplication are performed modulo p. The multiplicative inverses of nonzero elements exist, and may be found via the Euclidean algorithm, which produces the formula $xm + yp = 1$ when m is relatively prime to p. The inverse of m in $\mathbb{Z}_p$ is then the residue of x modulo p.

2. Subfields

Definition 2. Let E be a field. A *subfield* of E is subset $F \subset E$ satisfying

- **(S0)** F is nonempty;
- **(S1)** if $a, b \in F$, then $a + b \in F$;
- **(S2)** if $a \in F$, then $-a \in F$;
- **(S3)** if $a, b \in F$, then $ab \in F$;
- **(S4)** if $a \in F \setminus \{0\}$, then $a^{-1} \in F$.

We write $F \leq E$ to mean that F is a subfield of E.

Conditions **(S0)** through **(S5)** are necessary and sufficient for F to itself be a field.

The fields we will deal with in this course are the subfields of $\mathbb{C}$.

Example 7. Consider the subset of $\mathbb{R}$ given by

$$\mathbb{Q}[\sqrt{2}] = \{x \in \mathbb{R} \mid x = a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

This is set clearly satisfies properties **(S0)** through **(S3)**; for example, if $x_1 = a_1 + b_1\sqrt{2}$ and $x_2 = a_2 + b_2\sqrt{2}$, then $x_1 x_2 = (a_1 a_2 + 2b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{2}$, which is of the correct form to be an element of $\mathbb{Q}[\sqrt{2}]$. The multiplicative inverse of $a + b\sqrt{2}$ is

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2},$$

which is also in $\mathbb{Q}[\sqrt{2}]$. Notice that it is impossible for nonzero rational numbers a and b to satisfy $a^2 = 2b^2$.

Thus $\mathbb{Q}[\sqrt{2}]$ is a subfield of $\mathbb{R}$, and as such, is itself a field.

If $\mathcal{C}$ is a collection of sets, we denote the union and intersection of all the sets in $\mathcal{C}$ by $\cup\mathcal{C}$ and $\cap\mathcal{C}$, respectively; that is,

- $\cup\mathcal{C} \triangleq \{c \mid c \in C \text{ for some } C \in \mathcal{C}\}$;
- $\cap\mathcal{C} \triangleq \{c \mid c \in C \text{ for all } C \in \mathcal{C}\}$.

Proposition 1. *Let E be a field and let $\mathcal{F}$ be a collection of subfields of E. Then $\cap\mathcal{F}$ is a subfield of E.*

Proof. We verify properties **(S0)** through **(S4)**.

(S0) Every member of $\mathcal{F}$ contains 0, so $\cap\mathcal{F}$ contains zero.

(S1) Let $a, b \in \cap\mathcal{F}$. Then $a, b \in F$ for every $F \in \mathcal{F}$. Since each F in $\mathcal{F}$ is a subfield of E, $a + b \in F$ for every $F \in \mathcal{F}$. Thus $a + b \in \cap\mathcal{F}$.

(S2) Let $a \in \cap\mathcal{F}$. Then $a \in F$ for every $F \in \mathcal{F}$. Since each F in $\mathcal{F}$ is a subfield of E, $-a \in F$ for every $F \in \mathcal{F}$. Thus $-a \in \cap\mathcal{F}$.

(S3) Let $a, b \in \cap\mathcal{F}$. Then $a, b \in F$ for every $F \in \mathcal{F}$. Since each F in $\mathcal{F}$ is a subfield of E, $ab \in F$ for every $F \in \mathcal{F}$. Thus $ab \in \cap\mathcal{F}$.

(S4) Let $a \in \cap\mathcal{F}$ be nonzero. Then $a \in F$ for every $F \in \mathcal{F}$. Since each F in $\mathcal{F}$ is a subfield of E, $a^{-1} \in F$ for every $F \in \mathcal{F}$. Thus $a^{-1} \in \cap\mathcal{F}$. □

Definition 3. Let F be a field and let $A \subset F$. The *subfield of F generated by A*, denoted $\langle A \rangle$, is the intersection of all subfields of F which contain A.

Clearly, $\langle A \rangle$ is the smallest subfield of F which contains A.

Example 8. The subfield of $\mathbb{R}$ generated by the set $\{\sqrt{2}\}$ is $\mathbb{Q}[\sqrt{2}]$.

Recall that a *ring* is a field without property **(F8)**, and a subring is a a subfield without property **(S4)**. It is equally true that the intersection of a collection of subrings of a given ring is itself a ring; the proof is identical, except you don't need to prove **(S4)**, which doesn't hold for subrings.

3. Vector Spaces

Definition 4. A *vector space* over a field F is a set V together with a pair of operations,

$$+ : V \times V \to V \quad \text{and} \quad \cdot : F \times V \to V,$$

called vector addition and scalar multiplication, satisfying

- **(V1)** if $x, y \in V$, then $x + y = y + x$;
- **(V2)** if $x, y, z \in V$, then $(x + y) + z = x + (y + z)$;
- **(V3)** there exists $0 \in V$ such that $x + 0 = x$ for every $x \in V$;
- **(V4)** for every $x \in V$ there exists $-x \in V$ such that $x + (-x) = 0$;
- **(V5)** $1 \cdot x = x$ for every $x \in V$, where $1 \in F$;
- **(V6)** if $x, y \in V$ and $a \in F$, then $a(x + y) = ax + ay$;
- **(V7)** if $x \in V$ and $a, b \in F$, then $(ab)x = a(bx)$;
- **(V8)** if $x \in V$ and $a, b \in F$, then $(a + b)x = ax + bx$.

Example 9. Let $F = \mathbb{R}$ and $V = \mathbb{R}$. This is a vector space, where vector addition is addition in $\mathbb{R}$ and scalar multiplication is multiplication in $\mathbb{R}$.

Example 10. Let $F = \mathbb{R}$ and $V = \mathbb{R}^2$, the set of all ordered pairs of real numbers. For $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{R}^2$, define vector addition by $x+y = (x_1+y_1, x_2+y_2)$ and scalar multiplication by $ax = (ax_1, ax_2)$. Then V is a vector space over $\mathbb{R}$.

Example 11. Let F be any field, and $n \in \mathbb{N}$. Let F^n denote the set of all ordered n-tuples of elements from F. Define vector addition and scalar multiplication componentwise:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_2, \ldots, x_n + y_n)$$

and

$$a(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n),$$

where $x_1, \ldots, x_n, y_1, \ldots, y_n, a \in F$. Then F^n is a vector space over F.

Example 12. Let P_n denote the set of all polynomial functions with real coefficients of degree less than or equal to n. Then P_n is a vector space over $\mathbb{R}$ under polynomial addition and multiplication by a scalar.

Example 13. The field $\mathbb{Q}[\sqrt{2}]$ is a vector space over $\mathbb{Q}$ in the natural way.

Example 14. Let $\mathcal{F}(\mathbb{R})$ denote the set of all function $f : \mathbb{R} \to \mathbb{R}$. Then $\mathcal{F})(\mathbb{R})$ is a vector space over $\mathbb{R}$ with function addition and scalar multiplication.

Example 15. Let E be a field and let F be a subfield of E. Then E is a vector space over F, with vector addition as field addition in E, and scalar multiplication as multiplication (in E) of an element in F times an element in E.

4. Subspaces

Definition 5. Let V be a vector space over a field F. A *subspace* of V over F is a subset $W \subset V$ such that

(W0) W is nonempty;
(W1) $x, y \in W$ implies $x + y \in W$;
(W2) $x \in W$ and $a \in F$ implies $ax \in W$.

We write $W \leq V$ to mean that W is a subspace of V (where F is understood).

Conditions **(W0)** through **(W2)** are necessary and sufficient for W to itself be a vector space over F. Note that in the presence of **(W1)** and **(W2)**, **(W0)** is equivalent to the statement that the zero vector in W. This is because if W is nonempty by **(W0)**, then $w \in W$ for some $w \in V$, so by **(W2)**, $-w \in W$, and then by **(W1)**, $0 = w + (-w) \in W$.

Proposition 2. *Let V be a vector space over a field F and let $\mathcal{W}$ be a collection of subspaces of V over F. Then $\cap\mathcal{W}$ is a subspace of V over F.*

Proof. We show that $\cap\mathcal{W}$ satisfies properties **(W0)** through **(W2)**.

(W0) Every member of $\mathcal{W}$ is a subspace, and so it contains the zero vector. Thus the zero vector is in the intersection of all the subspaces in $\mathcal{W}$.

(W1) Let $w_1, w_2 \in \cap\mathcal{W}$. Then $w_1, w_2 \in W$ for every $W \in \mathcal{W}$. Thus $w_1 + w_2 \in W$ for every $W \in \mathcal{W}$, because W is a subspace. Therefore $w_1 + w_2 \in \cap\mathcal{W}$.

(W2) Let $w \in \cap\mathcal{W}$. Then $w \in W$ for every $W \in \mathcal{W}$. Thus $-w \in W$ for every $W \in \mathcal{W}$, because W is a subspace. Therefore $-w \in \cap\mathcal{W}$. □

Definition 6. Let V be a vector space over a field F and let $X \subset V$. The *subspace of V over F generated by X*, denoted $\langle X \rangle$, is the intersection of all subspaces of V over F which contain X.

Clearly, $\langle X \rangle$ is the smallest subspace of V over F which contains X, where F is understood from the context. We may write $\langle X \rangle_F$ if the field is ambiguous.

Example 16. The set $\mathbb{Q}[\sqrt{2}]$ is the subspace of $\mathbb{R}$ over $\mathbb{Q}$ generated by the set $\{\sqrt{2}\}$.

Example 17. The set P_n of all polynomials over $\mathbb{R}$ with degree less than or equal to n is the subspace $\mathcal{F}$, the set of all functions $f : \mathbb{R} \to \mathbb{R}$, which is generated by the set $X = \{1, x, x^2, \ldots, x^n\}$.

5. Span

Definition 7. Let V be a vector space over a field F and let $X \subset V$. A *linear combination* from X over F is an expression of the form

$$\sum_{i=1}^{m} a_i x_i \quad \text{where} \quad a_1, \ldots, a_n \in F \text{ and } x_1, \ldots, x_m \in X.$$

Note that a linear combination from X represents an element of V.

Definition 8. Let V be a vector space over a field F and let $X \subset V$. The *span* of X over F is

$$\operatorname{span} X = \{x \in V \mid x \text{ can be expressed as a linear combination from } X\}.$$

If $Y = \operatorname{span} X$, we say that X *spans* Y.

Again, the field F is understood in the notation $\operatorname{span}(X)$. We may write $\operatorname{span}_F(X)$ if the field is ambiguous.

Proposition 3. *Let V be a vector space and let $X \subset V$. Then* $\operatorname{span} X = \langle X \rangle$.

Proof. Since $\langle X \rangle$ is a subspace of V which contains X, it certainly contains all linear combinations of elements from X; that is, $\operatorname{span} X \subset \langle X \rangle$. On the other hand, one sees that $\operatorname{span} X$ is closed under vector addition and scalar multiplication, so it is itself a subspace of V which contains X; thus $\langle X \rangle \subset \operatorname{span} X$. □

Proposition 4. *Let V be a vector space and let $X, Y \subset V$.*
If X spans V and $X \subset Y$, then Y spans V.

Proof. Suppose that X spans V. Then every element of V is a linear combination of elements from X. But since $X \subset Y$, all such linear combinations are also linear combinations from Y. Thus Y spans V. □

6. Linear Independence

Definition 9. Let V be a vector space over a field F, and let $X \subset V$. We say that X is *linearly independent* over F if

$$\sum_{i=1}^{m} a_i x_i = 0 \quad \text{implies} \quad a_i = 0 \text{ for all } i = 1, \ldots, m,$$

where $x_1, \ldots, x_m \in V$ are distinct and $a_1, \ldots, a_m \in F$. Otherwise, we say that X is *linearly dependent*.

A true equation of the form $\sum_{i=1}^{m} a_i x_i = 0$, where $a_i \in F$ and $x_i \in V$ for all i between 1 and m, is called a *dependence relation* among the elements $x_1, \ldots, x_m$. It is a *trivial* dependence relation if all of the a_i's are equal to zero. Otherwise, it is a nontrivial dependence relation. A set is linearly independent if and only if it does not admit a nontrivial dependence relation.

Proposition 5. *Let V be a vector space and let $X, Y \subset V$.*
If Y is independent and $X \subset Y$, then X is independent.

Proof. Any nontrivial dependence relation among the elements of X would be a nontrivial dependence relation among the elements of Y. □

7. Basis

Definition 10. Let V be a vector space over a field F, and let $X \subset V$. We say that X is a *basis* for V over F if

(B1) X spans V over F;
(B2) X is linearly independent over F.

Lemma 1. *Let V be a vector space and let $X \subset V$ be a spanning set.*
If $v \in V \setminus X$, then $Y = X \cup \{v\}$ is dependent.

Proof. If $v = 0$, then $1 \cdot v = 0$ is a nontrivial dependence relation from Y, so Y is dependent; thus we may assume that $v \neq 0$. Since X spans, we may write $v = \sum_{i=1}^{m} a_i x_i$ for some $a_i \in \mathbb{R}$ and $x_i \in X$. Not all of the a_i's are zero, because $v \neq 0$. Let $x_{m+1} = v$ and $a_{m+1} = -1$; then $\sum_{i=1}^{m+1} a_i x_i = 0$ is a nontrivial dependence relation from Y. Thus Y is dependent. □

Lemma 2. *Let V be a vector space and let $X = \{x_1, \ldots, x_n\}$ be a dependent set. Then there exists $k \in \{1, \ldots, n\}$ such that x_k is a linear combination from $\{x_1, \ldots, x_{k-1}\}$.*

Proof. Since X is dependent, there is a nontrivial dependence relation

$$\sum_{i=1}^{n} a_i x_i = 0,$$

where not all a_i's equal zero. Let k be the largest integer between 1 and n such that $a_k \neq 0$. Then

$$x_k = \frac{1}{a_k} \sum_{i=1}^{k-1} a_i x_i$$

is a linear combination of the preceding elements. □

Theorem 1. *Let V be a vector space over a field F, and let $X, Y \subset V$ be finite subsets of V. If X is linearly independent over F and Y spans V over F, then*

$$|X| \leq |Y|.$$

Proof. Let $|Y| = n$ and $Y = \{y_1, \ldots, y_n\}$.

By way of contradiction (BWOC), suppose that $|X| > n$ and let

$$Z = \{z_1, \ldots, z_{n+1}\} \subset X;$$

then Z is independent by Proposition 5. Label the elements of Y and Z so that all of those contained in $Y \cap Z$ are in the front, with $y_i = z_i$ for all $i \leq j$:

$$Y = \{z_1, \ldots, z_j, y_{j+1}, \ldots, y_n\}.$$

By Lemma 1, the set

$$\{z_1, \ldots, z_{j+1}, y_{j+1}, y_{k+2}, \ldots, y_n\}$$

is dependent. By Lemma 2, one of these vectors is dependent on the preceding ones, and since the $z_i's$ are linearly independent, there exists $k \in \{j+1, \ldots, n\}$ such that y_k is a linear combination of $\{z_1, \ldots, z_{j+1}, y_{j+1}, \ldots, y_{k-1}\}$. Thus if we remove y_k from the set, it will still span:

$$\text{span}\{z_1, \ldots, z_{i+1}, y_{i+1}, \ldots, y_{k-1}, y_{k+1}, \ldots, y_n\} = V.$$

Continuing in this way, adding the next z and removing a y, we see that after $n - j$ replacements we have

$$\text{span}\{z_1, \ldots, z_n\} = V.$$

Thus the set $Z = \{z_1, \ldots, z_n\} \cup \{z_{n+1}\}$ is dependent by Lemma 1, producing a contradiction. □

Corollary 1. *Let V be a vector space over a field F, and let $X, Y \subset V$ be finite bases of V over F. Then*

$$|X| = |Y|.$$

Proof. Since X and Y are basis, each spans and is independent. Since X is independent and Y spans, we have $|X| \leq |Y|$. But also, Y is independent and X spans, so $|Y| \leq |x|$. The result follows. □

If we know that V is spanned by a finite set, we can use Lemma 2 to throw out one superfluous vector at a time, until we arrive at a spanning set which is also independent. This is a basis for V. Thus, in this case, V has a basis.

Definition 11. Let V be a vector space over a field F. The *dimension* of V over F is the cardinality of any basis for V over F.

Department of Mathematics and CSci, Southern Arkansas University
E-mail address: plbailey@saumag.edu