10. Fields and Vector Spaces

We will need some background knowledge concerning linear algebra over an arbitrary field. I will assume that you are familiar with the definition of a field, a vector space, and with some basic facts about polynomials over fields; in particular I will also assume the following basic result, which is *Vandermonde's Theorem*.

Proposition 10.1. *Let $f \in k[X]$ be a polynomial of degree $n \geq 0$ with coefficients in a field k. Then f has at most n roots.*

10.1. **A diversion into division rings.** There is a natural definition of the notion of a field, namely a *division ring*, in which one does not require that multiplication is commutative. Much of what will be discussed below applies in this setting but not all. We give an example of a division ring next and briefly mention some things to beware of in this more general setting.

Example 20. The real quaternions, $\mathbb{H}$, are defined to be a 4-dimensional vector space over the real numbers, $\mathbb{R}$.[35] Addition is defined to be the usual addition of vectors.

To define multiplication we introduce some notation: we write a vector (a, b, c, d) as $a + bi + cj + dk$, we define multiplication by a vector $a + 0i + 0j + 0k$ as the usual scalar multiplication, we define the multiplication of basis vectors as

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ ji = -k,\ jk = i,\ kj = -i,\ ki = j,\ ik = -j,$$

and we use distributivity to extend this definition so that multiplication is defined for all pairs of quaternions.

(E10.1) *Check that $\mathbb{H}$ is a division ring.*

(E10.2) *Show that Proposition 10.1 does not hold in $\mathbb{H}$.*

In addition to the failure of Proposition 10.1 demonstrated in (E10.2), division rings are made additionally complicated by the fact that one cannot immediately talk of 'a vector space over a division ring' - one must distinguish between *left* and *right* vector spaces.

Our choice to eschew the generality offered by division rings is justified by our desire to focus on finite fields, and by the following classical result.

Theorem 10.2. (Wedderburn's theorem) *A finite division ring is a field.*

10.2. **Back to fields.** Throughout this section k is a field; we write $k^* := k \backslash \{0\}$.

Lemma 10.3. *Any finite subgroup of the multiplicative group $(k^*, \cdot)$ is cyclic.*

Proof. Let H be a minimal non-cyclic subgroup of $(k^*, \cdot)$. Our knowledge of abelian groups implies that $H \cong C_p \times C_p$ for some prime p. Now every element of H satisfies the polynomial $X^p = 1$ which is a contradiction of Proposition 10.1. □

Of course, if k is finite, then this result implies that $(k^*, \cdot)$ is cyclic. In this case we call those elements of k^* that generate $(k^*, \cdot)$ the *primitive elements*.

(E10.3) *Let k be finite of order n. How many primitive elements does k contain?*

Example 21. Let p be a prime and define $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, the integers modulo p, with the usual addition and multiplication. Then $\mathbb{F}_p$ is a field.

Lemma 10.4. *Let $q = p^a$ where p is a prime and a is a positive integer. Then there exists a finite field of order q.*

Proof. (Sketch) The previous example gives the result for $a = 1$. Now let $f(X) \in \mathbb{F}_p[X]$ be an irreducible monic polynomial of degree $a \geq 2$. Since $\mathbb{F}_p[X]$ is a Principal Ideal Domain we conclude that $I := \langle f(X) \rangle$ is a maximal ideal of $\mathbb{F}_p[X]$ and we conclude that $\mathbb{F}_p[X]/I$ is a field. Since every element of $\mathbb{F}_p[X]/I$ contains a unique (and distinct) polynomial of degree less than a, we conclude that $\mathbb{F}_p[X]/I$ is a field of order p^a.

[35] The real quaternions are denoted $\mathbb{H}$ in honour of William Rowan Hamilton, the Irish mathematician who first described them.

It remains to show that, for every p and every $a > 1$, there exists a monic irreducible polynomial of degree a over $\mathbb{F}_p$. The product of all irreducibles of degree dividing a is equal to $f(x) = X^{p^a} - X$. What is more, since $f'(x) = 1$ over $\mathbb{F}_p$, $f(x)$ has no repeated roots.

Now consider the degree of the product of all irreducibles of degree dividing *and strictly less than* a. It can be no larger than

$$\sum_{d\Big|a, d\neq a} dp^d \leq \sum_{i<a} p^i = \frac{p^a - 1}{p - 1} < p^a = \deg(X^{p^a} - X).$$

Thus $X^{p^a} - X$ has more factors than this, and they are irreducibles of degree a as required. □

Given a monic irreducible $f(X) \in \mathbb{F}_p[X]$, one can do computations in $F := k[X]/\langle f(X)\rangle$ by observing that

$$F := \{c_{a-1}X^{a-1} + c_{a-2}X^{a-2} + \cdots + c_1X + c_0 + \langle f(x)\rangle \mid c_0, \ldots, c_{a-1} \in \mathbb{F}_p\}.$$

(We are using the fact, mentioned in the proof, that every element of $\mathbb{F}_p[X]/I$ contains a unique (and distinct) polynomial of degree less than a.)

Now one represents the element $c_{a-1}X^{a-1} + c_{a-2}X^{a-2} + \cdots + c_1X + c_0 + \langle f(x)\rangle \in F$ by the string

$$c_{a-1}\alpha^{a-1} + c_{a-2}\alpha^{a-2} + \cdots + c_1\alpha + c_0$$

where α is just a convenient symbol. Addition and multiplication on the resulting set of polynomials in α are just the usual addition and multiplication of polynomials, with the extra rule that $f(\alpha) = 0$.

(E10.4) *Show that $X^2 + 1 \in \mathbb{F}_3[X]$ is irreducible, and compute the addition and multiplication tables for $\mathbb{F}_9 := \mathbb{F}_3[x]/\langle X^2 + 1\rangle$.*

(E10.5) *Show that $X^3 + X + 1 \in \mathbb{F}_2[X]$ is irreducible, and compute the addition and multiplication tables for $\mathbb{F}_8 = \mathbb{F}_2[x]/\langle X^3 + X + 1\rangle$.*

Lemma 10.5. *Any finite field k has order p^a where p is a prime and a is a positive integer.*

Proof. Consider the set

$$k_0 := \{1, 1 + 1, 1 + 1 + 1, \ldots\}.$$

This is a closed subring of k of order n, say. Furthermore, $k \cong \mathbb{Z}/n\mathbb{Z}$. Now, since k contains no zero-divisors, neither does k_0 and so $n = p$, a prime. This implies that k_0 is a subfield of k of order p and so k is a vector space over k_0 of dimension a, say. Thus $|K| = p^a$ as required. □

Note that we have shown that k has a unique subfield, k_0, of order p. This is the *prime subfield* of k, and any subfield of k must contain k_0 (as is clear from its definition).

The following theorem summarizes some of what we have proved about finite fields so far. The last phrase "and is unique up to isomorphism" has not been proved, but we will take it as a fact in what follows.

Theorem 10.6. *For every prime p and every positive integer a, there is a finite field of order $q = p^a$. This field is unique up to isomorphism.*

In what follows we will write $\mathbb{F}_q$ for the field of order $q = p^a$. We close this section with a useful result that we prove using Galois theory.

Proposition 10.7. *Let $q = p^a$.*

1. *The automorphism group of $\mathbb{F}_q$ is cyclic of of order a, and is generated by the* Frobenius automorphism, *$\sigma : x \mapsto x^p$.*
2. *For every divisor b of a, there is a unique subfield of $\mathbb{F}_q$ of order p^b, consisting of all solutions of $x^{p^b} = x$, and these are all the subfields of $\mathbb{F}_q$.*

Proof. Write $\mathbb{F}_p$ for the prime subfield of $\mathbb{F}_q$, and observe that the degree of $\mathbb{F}_q$ over $\mathbb{F}_p$ is a. The Frobenius map, σ, is an $\mathbb{F}_p$-automorphism of $\mathbb{F}_q$, and has order a. Thus $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p) \geq a = |\mathbb{F}_q : \mathbb{F}_p|$.

By Galois theory we know that, given a field extension K/F, $\mathrm{Aut}(K/F) \leq |K:F|$ with equality if and only if K/F is a Galois extension. We conclude that $\mathbb{F}_q$ is a Galois extension and that

$$\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p) = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \sigma \rangle \cong C_a,$$

the cyclic group of order a.

The subgroups of $\langle \sigma \rangle$ are $\langle \sigma^{a/b} \rangle$ where b ranges over the divisors of a, and Galois theory implies that the subfields of $\mathbb{F}_q$ are, therefore, the the fixed fields of $\sigma^{a/b}$, as b ranges through the divisors of a. These are precisely the subfields of order p^b consisting of all solutions of $x^{p^b} = x$. □

10.3. **Vector spaces.** Let V and W be vector spaces over some field k. A *semilinear transformation* from V to W is a map $T : V \to W$ such that

(1) $(v_1 + v_2)T = v_1T + v_2T$ for all $v_1, v_2 \in V$;
(2) there exists an automorphism α of k such that

$$(cv)T = c^\alpha(vT)$$

for all $c \in k, v \in V$.

The automorphism α is called the *associated automorphism* of T. If T is not identically zero, then α is uniquely determined by T. If $\alpha = 1$ then T is a *linear transformation* between V and W.

We are mainly interested in the situation where $V = W$ (in which case we talk of 'semilinear transformations on V'). In this case if T is one-to-one and onto, then the inverse map is also a semilinear transformation and we say that T is *invertible*.

We can think of semilinear transformations on V in a different way: first fix a basis B of V. if α is an automorphism of K, then extend the action to V coordinate-wise, by defining

$$(c_1, \ldots, c_n)^\alpha := (c_1^\alpha, \ldots, c_n^\alpha).$$

We call this a *field automorphism of V with respect to B*; note that it is, in particular, a semilinear transformation from V to V.

Lemma 10.8. *Fix a basis B of V. Any semilinear transformation on V is a composition of a linear transformation and a field automorphism of V with respect to B.*

(E10.6) *Prove this.*

Suppose that V has dimension n over k; recall that all vector spaces of dimension n over k are mutually isomorphic (this will justify our next notation). We define

(1) $End(V)$, or $\mathrm{M}_n(k)$, to be the set of all linear transformations on V;
(2) $\mathrm{GL}(V)$, or $\mathrm{GL}_n(k)$ is the set of all invertible linear transformations on V;
(3) $\mathrm{SL}(V)$, of $\mathrm{SL}_n(k)$ is the set of all linear transformations on V of determinant 1;
(4) $\Gamma\mathrm{L}(V)$, or $\Gamma\mathrm{L}_n(k)$ is the set of all invertible semilinear transformations on V.

All of these are groups under the operation of composition. All act naturally on the vector space V (hence our decision to define transformations on the right).

(E10.7) *Prove that $\Gamma\mathrm{L}_n(k) \cong \mathrm{GL}_n(k) \rtimes_\phi \mathrm{Aut}(k)$. You will need to choose an appropriate homomorphism $\phi : \mathrm{Aut}(k) \to \mathrm{Aut}(\mathrm{GL}_n(K))$ to make this work. You may find it convenient to fix a basis for V – so you can express elements of $\mathrm{GL}_n(k)$ as matrices – before you choose ϕ.*