FIELDS: DEGREE OF AN EXTENSION, SOME FUN WITH FINITE FIELDS.

R. VIRK

1. Degree of a field extension

1.1. Let $K \supset F$ be a field extension. Then K is an F-vector space. The *degree of K over F*, denoted $[K : F]$, is the dimension of K as an F-vector space.

1.2. *Example.* $[\mathbf{C} : \mathbf{C}] = 1$.

1.3. *Example.* $[\mathbf{C} : \mathbf{R}] = 2$.

1.4. *Example.* $[\mathbf{C} : \mathbf{Q}] = \infty$.

1.5. The extension $K \supset F$ is called a *finite extension* if $[K : F]$ is finite. It is called a *quadratic extension* if $[K : F] = 2$ and a *cubic extension* if $[K : F] = 3$.

1.6. Generalizing the terminology for simple extensions, a field extension $K \supset F$ is said to be *algebraic over F* if each element $\alpha \in K$ is algebraic over F.

1.7. **Proposition.** *Let $F(\alpha)$ be a simple algebraic extension over F. Then $[F(\alpha) : F]$ is the degree of the irreducible polynomial of α over F.*

Proof. Exercise! □

The following is almost tautological.

1.8. **Lemma.** *A simple extension $F(\alpha) \supset F$ is algebraic over F if and only if the degree $[F(\alpha) : F]$ is finite.*

Proof. Exercise! □

The following easy result is extremely useful.

1.9. **Proposition.** *Let $F \subset K \subset L$ be fields. Then*

$$[L : F] = [L : K][K : F].$$

Proof. Let $\{\alpha_i\}_{i\in I}$ be a basis for K over F. Let $\{\beta_j\}_{j\in J}$ be a basis for L over K. To demonstrate the result it suffices to show that $\{\alpha_i\beta_j\}_{(i,j)\in I\times J}$ is a basis for L over F. Let $x \in L$, then $x = \sum_{j\in J} b_j\beta_j$ for some $b_j \in K$. Further, for each $j \in J$, $b_j = \sum_{i\in I} a_{ij}\alpha_i$ for some $a_{ij} \in F$. Thus,

$$x = \sum_{j\in J}\sum_{i\in I} a_{ij}\alpha_i\beta_j = \sum_{(i,j)\in I\times J} a_{ij}\alpha_i\beta_j.$$

Hence, $\{\alpha_i\beta_j\}_{(i,j)\in I\times J}$ generates L over F. All that remains to be seen is that the $\alpha_i\beta_j$ are linearly independent over F. Suppose

$$\sum_{(i,j)\in I\times J} c_{ij}\alpha_i\beta_j = 0$$

for some $c_{ij} \in F$. Then

$$\sum_{(i,j)\in I\times J} c_{ij}\alpha_i\beta_j = \sum_{j\in J}\left(\sum_{i\in I} c_{ij}\alpha_i\right)\beta_j = 0.$$

As $\{\beta_j\}_{j\in J}$ is a basis for L over K, we must have that $\sum_{i\in I} c_{ij}\alpha_i = 0$ for all $j \in J$. This forces all the c_{ij} to be 0, since $\{\alpha_i\}_{i\in I}$ is a basis for K over F. □

1.10. **Proposition.** *Let $K \supset F$ be a field extension. Let $L \subseteq K$ denote the subset of all elements in K that are algebraic over F. Then L is a subfield of K.*

Proof. We need to show that if $\alpha, \beta \in K$ are algebraic over F, then $\alpha+\beta, \alpha\beta, -\alpha$ and α^{-1} are also algebraic over F. As β is algebraic over F, it is also algebraic over $F(\alpha)$. By Lemma 1.8, this implies that $[F(\alpha,\beta) : F(\alpha)]$ is finite. As α is algebraic over F, Lemma 1.8 also implies that $[F(\alpha) : F]$ is finite. Now Prop. 1.9 gives that

$$[F(\alpha,\beta) : F] = [F(\alpha,\beta) : F(\alpha)][F(\alpha) : F]$$

is finite. This implies that $[F(\alpha+\beta) : F]$ and $[F(\alpha\beta) : F]$ are finite. So by Lemma 1.8, $\alpha+\beta$ and $\alpha\beta$ are algebraic over F. It is obvious that $F(\alpha) = F(-\alpha) = F(\alpha^{-1})$. In particular,

$$[F(\alpha) : F] = [F(-\alpha) : F] = [F(\alpha^{-1}) : F].$$

Applying Lemma 1.8, we get that α and α^{-1} are algebraic over F. □

1.11. **Proposition.** *Let $F \subset K \subset L$ be fields. If K is algebraic over F and L is algebraic over K, then L is algebraic over F.*

Proof. Exercise! □

2. Counting and finite fields

2.1. I should have probably said this a long time ago, but a field will always mean a field with $1 \neq 0$. If we allowed it, the field with $1 = 0$ would be a cheeky counterexample to many of the results of this section.

2.2. A field F is called *finite* if the number of elements in F, denoted $|F|$, is finite. The number $|F|$ is often called the *order* of F.

2.3. *Example.* $\mathbf{Z}/p\mathbf{Z}$ for a prime number p.

2.4. For a prime number p, I will write $\mathbf{F}_p$ for the field $\mathbf{Z}/p\mathbf{Z}$.

2.5. *Example.* $\mathbf{F}_3[x]/(x^2+1)$ is a field of order 9.

2.6. *Example.* $\mathbf{Z}[i]/3$ is a field of order 9. This isn't really a new example: $\mathbf{Z}[i]/3$ is isomorphic to $\mathbf{F}_3[x]/(x^2+1)$.

2.7. Let F be a field. The *characteristic* of F, denoted $\mathrm{char}(F)$, is the smallest positive integer $n > 0$ such that

$$\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0.$$

If no such integer exists, then we say that F is of chracteristic 0. This might seem like a funny convention, but it is (somewhat) justified by the following convenient notation.

2.8. Let $n \in \mathbf{Z}$. If n is positive, then we also write n for the element

$$\underbrace{1+1+\cdots+1}_{n \text{ times}}$$

in F. If n is negative, then we also write n for the element

$$-(\underbrace{1+1+\cdots+1}_{-n \text{ times}})$$

in F.

2.9. *Example.* $\mathrm{char}(\mathbf{Q}) = \mathrm{char}(\mathbf{R}) = \mathrm{char}(\mathbf{C}) = 0$.

2.10. *Example.* $\mathrm{char}(\mathbf{F}_p) = p$.

2.11. **Proposition.** *If F is a field of non-zero characteristic, then* $\mathrm{char}(F)$ *must be a prime number.*

Proof. Suppose $\mathrm{char}(F) = mn$ for positive integers m and n. Then $mn = 0$. This implies, without loss of generality, that $m = 0$ in F. So $\mathrm{char}(F) = m$ and $n = 1$, since the characteristic is the smallest positive integer that is zero in F. □

2.12. **Proposition.** *If F is a finite field, then* $\mathrm{char}(F) \neq 0$.

Proof. Set $n = |F|$. Then the elements $0, 1, \ldots, n$ cannot all be distinct in F. That is, $r - s = 0$ in F, for some distinct positive integers r, s. □

2.13. **Proposition.** *If V is a finite dimensional $\mathbf{F}_p$-vector space, then V contains $p^{\dim(V)}$ elements.*

Proof. Let $\{e_1, \ldots, e_n\}$ be a basis for V. Let $v \in V$, then

$$v = a_1 e_1 + \cdots + a_n e_n$$

for some $a_i \in \mathbf{F}_p$ determined *uniquely* by v. There are only p^n possibilities. □

2.14. Let F be a finite field. Then $\mathrm{char}(F)$ must be a prime number, say p. It is easy to see (exercise!) that the subset $\{0, 1, \ldots, p-1\}$ is a sub-field of F. This sub-field is isomorphic to $\mathbf{F}_p$. From this point on I will just say that $\mathbf{F}_p$ is a sub-field of F (pedantically, $\mathbf{F}_p$ only contains an isomorphic copy of $\mathbf{F}_p$, but in this situation nothing is lost by pretending that isomorphic objects are equal). Regardless, the field F is an $\mathbf{F}_p$-vector space. In particular, $|F|$ is some power of p.

2.15. The main points of the discussion above can be summarized as follows: let K be a field of characteristic $p \neq 0$. Then

(i) p must be a prime number;
(ii) $\mathbf{F}_p$ is a subfield of K;
(iii) K is a finite field if and only if $[K : \mathbf{F}_p]$ is finite;
(iv) if K is a finite field, then $|K| = p^{[K:\mathbf{F}_p]}$.

Department of Mathematics, University of California, Davis, CA 95616
E-mail address: virk@math.ucdavis.edu