VIGRE Algebra QR Review, October 28, 2002

Finite fields

A finite field must have positive characteristic p for some prime integer $p \geq 2$, and so may be viewed as a finite algebraic extension of $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. If L is a finite algebraic extension of a finite field K of degree d, then as an abelian group L is the direct sum of d copies of K, and so $|L| = |K|^d$. In particular, if a finite field K has degree n over its prime field $\mathbb{Z}_p$, it follows that K has p^n elements for some positive integer n. Thus, the number of elements in a finite field is a prime power.

In fact, up to isomorphism, there is a unique finite field with p^n elements for every prime prime power p^n, $n \geq 1$. To see the existence, consider the splitting field of the equation $x^{p^n} - x$ over $\mathbb{Z}_p$. The formal derivative is -1, and so this equation cannot have a multiple root. But the roots are closed under addition and multiplication: if $r^{p^n} = r$ and $s^{p^n} = s$, then $(r+s)^{p^n} = r^{p^n} + s^{p^n} = r + s$, and the proof for multiplication is similar. 0 and 1 are included, as is $1/r$ for $r \neq 0$. Thus, the roots are distinct and form a field, and this field evidently has p^n elements. On the other hand, if a field has p^n elements, its multiplicative group has order $p^n - 1$, and so the nonzero elements satisfy $x^{p^n-1} = 1$, and all elements satisfy $x^{p^n} - x = 0$. Thus, the field must be a splitting field for $x^{p^n} - x$ over $\mathbb{Z}_p$, and uniqueness follows because splitting fields are unique up to isomorphism. The field with $q = p^n$ elements is sometimes called the *Galois field* $\mathrm{GF}(q)$. The notation $\mathbb{F}_q$ is often used for this field as well.

If $p^n = (p^h)^k$, the roots of $x^{p^h} - x$ will be included in those of $x^{p^n} - x$. It follows that $\mathrm{GF}(q)$ may be identified with a subfield of $\mathrm{GF}(q')$ if and only if *q' is a power of q*.

Any ring of prime characteristic $p > 0$ has an endomorphism, the *Frobenius endomorphism*, that maps r to r^p. The Frobenius endomorphism F on any field is injective, since there are no nonzero nilpotents. But an injective map from a finite field to itself is surjective, and so in $\mathrm{GF}(p^n)$ every element has a pth root, i.e., finite fields are perfect.

The multiplicative group of $\mathrm{GF}(p^n)$ has order $p^n - 1$: by a theorem, it is a cyclic group. [It is an abelian group with at most d elements of order dividing d for every integer d dividing $p^n - 1$ (over any field, the equation $x^d - 1 = 0$, like any other equation of degree d, has at most d roots). In a direct sum of finite cyclic groups, if $\mathbb{Z}_d \oplus Z_{dk}$ occurs, then since $\mathbb{Z}_{dk}$ has a subgroup isomorphic with $\mathbb{Z}_d$, there are at least d^2 elements of order d. So if the group is written as a direct sum of finite cyclic groups such that the orders are linearly ordered by divisibility, there can be only one summand.]

Any extension of one finite field by another is automatically normal (the larger field is a splitting field, even over $\mathbb{Z}_p$) and separable, since finite fields are perfect. The Galois group of an extension of finite fields is cyclic. In fact, the automorphism group of the degree n extension $\mathrm{GF}(p^n)$ of $\mathbb{Z}_p$ must have order n (this is actually the group of all automorphisms of $\mathrm{GF}(p^n)$, since any automorphism fixes the elements of $\mathbb{Z}_p$), and one can check that $\mathbf{1}, F, \ldots, F^{n-1}$ are distinct field automorphisms. So they must be all the field automorphisms.

From what has been said, it is now easy to determine the Galois group of $\mathrm{GF}(p^{dn})$ over $\mathrm{GF}(p^d)$: it consists of all automorphisms of $\mathrm{GF}(p^{dn})$ that fix the smaller field, and these are $\mathbf{1}, F^d, F^{2d}, \ldots, F^{d(n-1)}$.

Problems new this week

1. (a) Find the order of the group $\mathrm{GL}(2, \mathbb{F}_p)$ of invertible 2×2 matrices over a field with p elements.

(b) Explicitly describe a Sylow p-subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$.

(c) Show that $\mathrm{GL}(2, \mathbb{F}_p)$ has a normal subgroup of index $p-1$. (Hint: the determinant map!).

(d) Now let U be the subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$ of 2×2 upper triangular matrices. Prove that U is solvable.

2. Let F be a finite field of q elements of char. $p > 0$, and let $a \in F - \{0\}$. Prove that $g(x) = x^q - x - a$ has no roots in F and that its splitting field over F is an extension of degree p. [The examiners gave this hint: There is a root r in some extension field. Prove that $\{r + c : c \in F\}$ is then the complete set of roots of $g(x)$. The easiest solution of this problem does not use this hint.]

3. Let $\mathbb{F}_q$ be the finite field with q elements, and let $G = \mathrm{GL}_2(\mathbb{F}_q)$ be the group of 2×2 invertible matrices with elements in $\mathbb{F}_q$. Let $V = \mathbb{F}_q^2$ be the vector space of 2×1 column vectors over $\mathbb{F}_q$.

(a) Explain how G acts naturally on the set $\mathbb{P}$ of all one-dimensional subspaces of V.

(b) Let $W \subseteq V$ be the subspace spanned by $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Find the stabilizer of $W \in \mathbb{P}$ in G, i.e., the subgroup S of G whose elements fix W.

(c) What is the index of S in G?

4. As a function of q, how many nilpotent 2×2 matrices are there over a finite field with q elements?

5. A finite field F has 81 elements. How many solutions are there to the equation $x^{25} = 1$ in this field?

6. Show that the group $\mathrm{SL}(n, \mathbb{Z})$ of $n \times n$ matrices over the integers with determinant 1 is finitely generated.

7. An 11×11 matrix M over a field F has square 0. Find all the possibilities for the Jordan form of M. Does the number of possible Jordan forms depend on F?