2/10

Finite Fields §5.5

Def'n Let K be a field. The characteristic of K is the smallest $n \geq 1$ such that $n \left(= \overbrace{1+1+\cdots+1}^{n \text{ times}}\right) = 0$ in K, or is zero if no such n exists.

E.g. most of the fields we have seen so far, like $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ (and their extensions) have characteristic zero. For an example of a field with "positive characteristic", recall that for a prime number p we have the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, which has characteristic p.

Prop. The characteristic of a field K is 0 or a prime number p.

Pf sketch: Suppose the characteristic of K were $n > 0$ a non-prime number, e.g. $n = 6$. Take any proper divisor of n, e.g. $d = 2$. Then $2 = 1+1$ is a non-zero zero divisor in K, so K cannot be an integral domain (much less a field). $\boxtimes$

Def'n Let K be a field. The intersection of all subfields of K is called the prime subfield of K. It is the "smallest" subfield in K.

Prop. The prime subfield of K is either $\mathbb{Q}$, if K has char. 0, or $\mathbb{F}_p$, if K has positive char. $p > 0$.

Pf: The prime subfield of K is the one generated by $1 \in K$. If K has char. p so that $p \cdot 1 = \overbrace{1+1+\cdots+1}^{p}$ then this will be $\mathbb{F}_p$, otherwise we will get a copy of $\mathbb{Z}$, hence $\mathbb{Q}$, inside K. $\boxtimes$

Corollary If K is a finite field, then it must have positive characteristic.

Pf: Otherwise it would have $\mathbb{Q}$ inside it, which is infinite. $\boxtimes$

Remark Every finite field has positive characteristic, but the converse is not true: there are infinite fields of char. $p>0$. For example, $K = \mathbb{F}_p(x)$, field of rational functions with coefficients in $\mathbb{F}_p$, is infinite of characteristic p. So is $K = \overline{\mathbb{F}_p}$, algebraic closure of $\mathbb{F}_p$ (we may discuss this later).

In fact, we can say a little more about how finite fields look:

Prop. Let K be a finite field. Then the number of elements in K is p^n, where p is the char. of K, for some $n \geq 1$.

Pf: The prime subfield of K is $\mathbb{F}_p$ and K is a finite dimensional v.s. over this $\mathbb{F}_p$, hence has p^n elts where n is its dimension as an $\mathbb{F}_p$-vector space. ☒

In what follows we will show that, for any prime power $q=p^n$, a finite field $\mathbb{F}_q$ exists and is unique! But be warned that while $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is very easy to construct, constructing $\mathbb{F}_q$ for q a prime power which is not a prime is much more involved! In particular...

Note For $n>1$, $\mathbb{F}_{p^n}$ is not the same as $\mathbb{Z}/p^n\mathbb{Z}$. Indeed, for any composite number N, $\mathbb{Z}/N\mathbb{Z}$ is not an integral domain, hence not a field!

To construct finite fields $\mathbb{F}_q$ for $q=p^n$ with $n>1$, we will instead realize them as (algebraic!) extensions of $\mathbb{F}_p$. Hence, our study of field extensions and Galois groups etc. is very useful for this purpose. Sometimes finite fields are called "Galois fields" for this reason...

One of the best tools for studying fields of positive characteristic is the Frobenius endomorphism (or automorphism).

Thm Let K be a field of char. $p>0$. Define the map $\varphi: K \to K$ by $\varphi(x) = x^p$ for all $x \in K$. Then φ is a $\mathbb{F}_p$-linear endomorphism of K (i.e., it preserves $\mathbb{F}_p$ and the field structure of K).
It is called the Frobenius endomorphism. It is always injective.
If K is finite, it is also surjective, called the Frobenius automorphism.

Pf: We need to check that φ preserves the field operations.
That it preserves multiplication (& division) is clear: $\varphi(xy) = (xy)^p = x^p y^p$.
The important thing to check is that it preserves addition.
Recall the Binomial Theorem $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$, where $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ are the binomial coefficients. Notice that for $0<i<p$, $\frac{p!}{i!(p-i)!}$ (an integer) has a factor of p on top that never cancels, hence modulo p we have $\binom{p}{i} = 0$ for those i, which means that $(x+y)^p = x^p + y^p$ (sometimes called the "Freshman's Dream.")
So indeed φ preserves addition. It acts as the identity on $\mathbb{F}_p$, the prime subfield of K, since $\varphi(1) = 1$. It is injective since $\varphi(x) \neq 0$ for any $x \neq 0$ since K has no non-zero zero divisors.
If K is finite, it's bijective since an injective map between two finite sets of the same size is bijective. $\boxtimes$

Remark: The Frobenius endomorphism is not always a bijection. For example, with $K = \mathbb{F}_p(x)$ it fails to be surjective. A field K is called perfect if it either has characteristic zero, or has positive char. $p>0$ and the Frobenius endomorphism is surjective. This is the same as every irreducible polynomial $f(x) \in K[x]$ being separable.
(See also the last problem on your HW...).

2/12

Def'n If K is a finite field, its order is its size, i.e., $\# K$.

We will see that if K is a finite field of char. p, then the Frobenius automorphism φ generates the Galois group $\mathrm{Aut}_{\mathbb{F}_p}(K)$. First, let's start with the multiplicative group:

Thm Let K be a finite field of order $q = p^n$. Then its multiplicative group $(K \setminus \{0\}, \times)$ is cyclic (of order $q-1$).

Pf: The multiplicative group, whatever it is, is some finite abelian gp, hence by classification has form $\mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}$ where $d_1 \mid d_2 \mid \cdots \mid d_m$. We see that for any $g \in G$ (where G is this gp.) we have $d_m \cdot g = 0$ in additive notation. Multiplicatively, we can say $x^{d_m} - 1 = 0$ for all $x \in K \setminus \{0\}$. But $\# K \setminus \{0\} = q-1$, which is the biggest that d_m could be (if G were cyclic), and a polynomial can have at most as many roots as its degree, so in fact $d_m = q-1$, $m = 1$, and G is cyclic! ▣

Remark: In general, finding a generator of the mult. group of a finite field can be a difficult computational problem. The number of generators is $\Phi(q-1)$ where Φ is "Euler's totient function" $\phi(n) = \# \{k \leq n : \gcd(n,k) = 1\}$.

Thm For any prime power $q = p^n$, a finite field of order q exists, and all such finite fields are isomorphic: it is the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$.

Pf: First we address uniqueness, so let K be a finite field of order p^n. As we just explained $x^{p^n-1} - 1 = 0$ for all $x \in K$, $x \neq 0$. Hence, $x^{p^n} - x = 0$ for all $x \in K$. So indeed the poly.
$f(x) = x^{p^n} - x = \prod_{u \in K} (x-u)$ splits in K. And since the roots of this polynomial are all of K, K is the splitting field.

Now we deal with existence. By looking at the formal derivative of $f(x) = x^{p^n} - x$ (which is $-1 \bmod p$) we can see that in a splitting field of $f(x)$ it has all distinct roots, i.e. is separable. So let K be a splitting field of $f(x)$ and let $E \subseteq K$ be the set of roots of $f(x)$ in K. Then $\# E = p^n$. But also, $E = \{u \in K : \varphi^n(u) = u\}$ where $\varphi : K \to K$ is the Frob. auto., hence E is a subfield (fixed points of an automorphism), and since E contains all roots of $f(x)$, we must have $K = E$. ☒

Remark: Something we have yet to formally address, implicit in the above proof, is that for any field K and any poly. $f(x) \in K[x]$, a splitting field of $f(x)$ exists and it is unique. This can be established in the following way. First:

Lemma: 1) If $f(x) \in K[x]$ is irreducible, then there is a simple algebraic extension $K(u)$ where the min. poly. of u is $f(x)$.

2) If $K(u)$ and $K(v)$ are two simple algebraic extensions s.t. the min. poly.'s of u and v are the same, they are isomorphic.

Pf: For 1): Take $K[X] / \langle f(x) \rangle$ as our field.

For 2): $\varphi : K(u) \to K(v)$ defined by $\varphi(u) = v$ is the iso. ☒

Then, to construct a splitting field of $f(x)$ over K, we inductively factor $f(x)$ into irreducibles and adjoin roots of the irreducible factors of degree 2 or higher until it completely factors. Part 2) of the above lemma can also be used to show that this process results in a unique field independent of what choice of roots we adjoin and in what order. So indeed the field $\mathbb{F}_q$ with $q = p^n$ elts. exists & is unique.

Cor $\mathbb{F}_{p^n}$ as an extension of $\mathbb{F}_p$ is Galois. The Galois group $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ is cyclic of order n, generated by the Frobenius automorphism φ.
For each divisor $d \mid n$, there is a unique subfield $\mathbb{F}_{p^d}$ in $\mathbb{F}_{p^n}$.

Pf: By the above discussion, any subfield $\mathbb{F}_{p^k}$ will be the fixed points of the k^{th} power of φ, hence indeed $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ is generated by φ. (To show $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois, note it is the splitting field of a sep. polynomial)
The last sentence follows from the Fund. Thm. of Galois Theory.

Cor Let $f(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree n, and let $K = \mathbb{F}_p(u)$ where u has minimal polynomial $f(x)$.
Then $K = \mathbb{F}_{p^n}$. Pf: The degree $[K : \mathbb{F}_p] = n$, so we have $\# K = p^n$ and by uniqueness of finite fields this means $K = \mathbb{F}_{p^n}$. ☒

Remark: In practice, to construct $K = \mathbb{F}_{p^n}$ we find an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of deg. n and adjoin a root of it to $\mathbb{F}_p$.
Because to work algorithmically in this K we need to use polynomial long division and the Euclidean gcd algorithm, it is preferable to choose such an $f(x)$ where most coeff's $= 0$.
For example, taking $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ works to construct $\mathbb{F}_{16} = \mathbb{F}_2[x]/\langle x^4+x+1 \rangle$ in this way.
But cannot always choose $f(x) = x^n + x + 1$:
e.g. see exercise 9 of section 5.5 of the textbook.
One choice of irreducible polynomials over finite fields are the "Conway polynomials" but they are slightly complicated to describe ...