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 $n \; (= \overbrace{1+1+\cdots+1}^{n \text{ times}}) = 0$ 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. $\blacksquare$

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. ☒

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...). ◁