PERFECT FIELDS

KEITH CONRAD

Characteristic 0 fields have a very handy feature: every irreducible polynomial in characteristic 0 is separable. Fields in characteristic p may or may not have this feature.

Definition 1. A field K is called *perfect* if every irreducible polynomial in $K[X]$ is separable.

Every field of characteristic 0 is perfect. We will see that finite fields are perfect too. The simplest example of a nonperfect field is the rational function field $\mathbf{F}_p(u)$, since $X^p - u$ is irreducible in $\mathbf{F}_p(u)[X]$ but not separable.

Recall that for an irreducible $\pi(X)$, it is inseparable if and only if $\pi'(X) = 0$.

Here is the standard way to check a field is perfect.

Theorem 2. *A field K is perfect if and only if it has characteristic 0, or it has characteristic p and $K^p = K$.*

Proof. When K has characteristic 0, any irreducible $\pi(X)$ in $K[X]$ is separable since $\pi'(X) \neq 0$ (after all, $\deg \pi' = \deg \pi - 1$). It remains to show when K has characteristic p that every irreducible in $K[X]$ is separable if and only if $K^p = K$. To do this we will show the *negations* are equivalent: an inseparable irreducible exists in $K[X]$ if and only if $K^p \neq K$.

If $K^p \neq K$, pick $a \in K - K^p$. Then $X^p - a$ has only one root in a splitting field: if $\alpha^p = a$ then $X^p - a = X^p - \alpha^p = (X - \alpha)^p$ since we are working in characteristic p. The polynomial $X^p - a$ is irreducible in $K[X]$ too: any nontrivial proper monic factor of $X^p - a$ is $(X - \alpha)^m$ where $1 \leq m \leq p - 1$. The coefficient of X^{m-1} in $(X - \alpha)^m$ is $-m\alpha$, so if $X^p - a$ has a nontrivial proper factor in $K[X]$ then $-m\alpha \in K$ for some m from 1 to $p - 1$. Then $m \in \mathbf{F}_p^\times \subset K^\times$, so $\alpha \in K$, which means $a = \alpha^p \in K^p$, a contradiction. Thus $X^p - a$ is irreducible and inseparable in $K[X]$.

Now suppose there is an inseparable irreducible $\pi(X) \in K[X]$. Then $\pi'(X) = 0$, so $\pi(X)$ is a polynomial in X^p, say

$$\pi(X) = a_m X^{pm} + a_{m-1} X^{p(m-1)} + \cdots + a_1 X^p + a_0 \in K[X^p].$$

If $K^p = K$ then we can write $a_i = b_i^p$ for some $b_i \in K$, so

$$\pi(X) = \left(b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0\right)^p.$$

(It was crucial for this conclusion that the coefficients of $\pi(X)$ are pth powers and not only that $\pi(X)$ is a polynomial in X^p.) Since $\pi(X)$ is irreducible we have a contradiction, which shows $K^p \neq K$. □

Corollary 3. *Fields of characteristic 0 and finite fields are perfect.*

Proof. By Theorem 2, fields of characteristic 0 are perfect. It remains to show a finite field K of characteristic p satisfies $K^p = K$. The pth power map $K \to K$ is injective and therefore surjective because K is finite, so we are done. □

The two types of fields listed in Corollary 3 are the most basic examples of perfect fields. Other perfect fields can show up, especially in the middle of technical proofs about fields.

Corollary 3 says any irreducible in $\mathbf{F}_p[X]$ has no repeated root, but the proof was rather indirect. We now give a more elementary proof that any irreducible $\pi(X)$ in $\mathbf{F}_p[X]$ is separable. The idea is to show $\pi(X)$ is a factor of a polynomial which we can directly check has no repeated roots. We may assume $\pi(X) \neq X$, so $X \bmod \pi$ is a unit in $\mathbf{F}_p[X]/(\pi)$. Since $\pi(X)$ is irreducible, $\mathbf{F}_p[X]/(\pi)$ is a field with size p^d, where $d = \deg \pi$. The nonzero elements of $\mathbf{F}_p[X]/(\pi)$ are a group of size $p^d - 1$, so $X^{p^d-1} \equiv 1 \bmod \pi$. Multiplying through by X, we get $X^{p^d} \equiv X \bmod \pi$, so $\pi(X)|(X^{p^d} - X)$ in $\mathbf{F}_p[X]$. The polynomial $X^{p^d} - X$ has no repeated roots (in a splitting field): if $\alpha^{p^d} - \alpha = 0$ then

$$\begin{aligned} X^{p^d} - X &= X^{p^d} - X - (\alpha^{p^d} - \alpha) \\ &= (X^{p^d} - \alpha^{p^d}) - (X - \alpha) \\ &= (X - \alpha)^{p^d} - (X - \alpha) \\ &= (X - \alpha)((X - \alpha)^{p^d-1} - 1). \end{aligned}$$

The second factor $(X-\alpha)^{p^d-1}-1$ has value -1 at $X = \alpha$, so α is a root with multiplicity 1. Since α was taken to be any root of $X^{p^d} - X$, we see that $X^{p^d} - X$ is separable. Therefore its factor $\pi(X)$ is also separable.

Theorem 4. *A field K is perfect if and only if every finite extension of K is a separable extension.*

Proof. Suppose K is perfect: every irreducible in $K[X]$ is separable. If L/K is a finite extension then the minimal polyomial in $K[X]$ of every element of L is irreducible and therefore separable, so L/K is a separable extension.

Now suppose every finite extension of K is a separable extension. To show K is perfect, let $\pi(X) \in K[X]$ be irreducible. Consider the field $L = K(\alpha)$, where $\pi(\alpha) = 0$. This field is a finite extension of K, so a separable extension by hypothesis, so α is separable over K. Since $\pi(X)$ is the minimal polynomial of α in $K[X]$, it is a separable polynomial. □

A lot of results about field theory that are valid in characteristic 0 carry over to perfect fields in characteristic p (but not everything), and the reader should be attentive to this point when reading texts which try to make life easy by always assuming fields have characteristic 0. You should always check if the theorems (and even proofs) go through to general perfect fields.