Some Consequences of Field Characteristic

Recall that a field F has characteristic zero if

$$na := \underbrace{a + a + \cdots + a}_{n} \neq 0$$

for all $a \in F$ and every natural number $n \geqslant 1$. If $na = 0$ for some nonzero $a \in F$ and $n \geqslant 1$, then the smallest positive n for which this occurs is a prime p, called the characteristic of F. The unique smallest subfield of F is either $\mathbb{Q}$ or $\mathbb{F}_p$, according as $\operatorname{char} F = 0$ or p. This unique smallest subfield of F is called the *prime subfield of F*. Every subfield of F contains the prime subfield.

Theorem 1. Let F be a field of prime characteristic p. Then the map $a \mapsto a^p$ is a one-to-one homomorphism of F.

Proof. Clearly $(ab)^p = a^p b^p$ for all $a, b \in F$, and $1^p = 1$. Also

$$(a+b)^p \;=\; a^p + pa^{p-1}b + \tbinom{p}{2}a^{p-2}b^2 + \cdots + pab^{p-1} + b^p \;=\; a^p + b^p$$

since the binomial coefficients $\binom{p}{k}$ all vanish for $k = 1, 2, \ldots, p-1$. Thus $a \mapsto a^p$ is a homomorphism of rings with identity. Now the kernel of this homomorphism consists of all $a \in F$ such that $a^p = 0$, i.e. $a = 0$; so the homomorphism is one-to-one. □

Theorem 2. If F is a finite field, then $|F| = p^r$ for some prime p and integer $r \geqslant 1$.

Proof. If $|F| < \infty$ then F has no subfield isomorphic to $\mathbb{Q}$, so the prime subfield of F is $\mathbb{F}_p$ for some prime p. Let $r = [F : \mathbb{F}_p]$, so that F has a basis $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ over $\mathbb{F}_p$. Elements of F are uniquely represented in the form

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_r\alpha_r, \quad a_i \in \mathbb{F}_p\,.$$

There are exactly p^r such linear combinations, so $|F| = p^r$. $\square$

If $|F| = p^r$ then the map $a \mapsto a^p$ is in fact an automorphism of F. (It is one-to-one by Theorem 1; but since F is finite, every one-to-one map is also onto.)

For example, the field $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$ has characteristic 2; it is an extension of degree 2 of its prime subfield $\mathbb{F}_2 = \{0, 1\}$. We have seen that the map $a \mapsto a^2$ is an automorphism of $\mathbb{F}_4$. In fact $\mathbb{F}_4$ has just two automorphisms, the identity map and the map $a \mapsto a^2$.

Consider also the field $F_{25} = \mathbb{F}_5[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{F}_5\}$. This field has just two automorphisms, the identity and the map $x \mapsto x^5$ which in fact is just the familiar 'conjugation' map since

$$(a + b\sqrt{2})^5 = a^5 + b^5(\sqrt{2})^5 = a - b\sqrt{2}.$$

(Note that $\sqrt{2}^5 = 4\sqrt{2} = -\sqrt{2}$.)

For every prime p and integer $r \geqslant 1$, it may be shown that there is a field of order $q = p^r$; and it is unique up to isomorphism. This field is denoted $\mathbb{F}_q$. It has exactly r automorphisms, namely $1, \sigma, \sigma^2, \ldots, \sigma^{r-1}$ where $\sigma : x \mapsto x^p$. Note that $\sigma^i : x \mapsto x^{p^i}$.

If F is an infinite field of prime characteristic p, then the monomorphism $\sigma : x \mapsto x^p$ may or may not be onto; for example if $F = \mathbb{F}_p(t)$ or $\mathbb{F}_p((t))$, then σ is not onto; its image is the subfield $\mathbb{F}_p(t^p)$ or $\mathbb{F}_p((t^p))$ respectively, a proper subfield isomorphic to F. This observation leads into the next topic:

Consider a polynomial $f(t) \in F[t]$, and let $\alpha \in E \supseteq F$ where E is an extension field. We say α is a *root of multiplicity* k if $(t - \alpha)^k$ divides $f(t)$ in $E[t]$, but $(t - \alpha)^{k+1}$ does not divide $f(t)$. Every root is either a *simple root* (i.e. a root of multiplicity 1) or a *multiple root* (i.e. a root of multiplicity at least 2). If $f(t) \in F[t]$ is irreducible over F, can $f(t)$ have a multiple root in an extension field E? It depends.

Theorem 3. Suppose $f(t) \in F[t]$ is irreducible over F. If F has characteristic zero, then $f(t)$ has no multiple roots in any extension field $E \supseteq F$.

Proof. Let $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in F[t]$ where $a_i \in F$ with $a_n \neq 0$, $n \geqslant 1$. If f has a multiple root $\alpha \in E \supseteq F$, then $f(t) = (t - \alpha)^2 g(t)$ for some $g(t) \in E[t]$, so $f'(t) = 2(t - \alpha)g(t) + (t - \alpha)^2 g'(t)$ and $f'(\alpha) = 0$. Assuming $\operatorname{char} F = 0$, this gives $f'(t) = a_1 + 2a_2 t + \cdots + n a_n t^{n-1} \in F[t]$ where $n a_n \neq 0$ so $\deg f'(t) = n - 1$ and $\gcd(f(t), f'(t)) = 1$ since $f(t)$ is irreducible. By the Extended Euclidean Algorithm,

$$u(t)f(t) + v(t)f'(t) = 1$$

for some $u(t), v(t) \in F[t]$ so $0 = u(\alpha)f(\alpha) + v(\alpha)f'(\alpha) = 1$, a contradiction. $\square$

The same conclusion holds if E is finite. However, if E is an infinite field of prime characteristic p, then the conclusion fails: consider $E = \mathbb{F}_p(x)$ with subfield $F = \mathbb{F}_p(x^p)$. Then the polynomial $f(t) = t^p - x^p \in F[t]$ is irreducible over F, but factors as $f(t) = (t-x)^p$ over E, by Theorem 1. (You should regard x as a constant here, and t as the variable.) Note that $f'(t) = 0$ in this case so $\gcd(f(t), f'(t)) = f(t)$; for this reason, the proof of Theorem 3 doesn't apply here.