## Field Theory Basics

Let $R$ be a ring. $M$ is called a maximal ideal of $R$ if $M$ is a proper ideal of $R$ and there is no proper ideal of $R$ that properly contains $M$.

**Lemma 14.1**: Let $R, S$ be rings and $I$ be an ideal in $S$. Let $\phi : R \to S$ be a homomorphism. Then the pre-image $\phi^{-1}(I) = \{r \in R | \phi(r) \in I\}$ is an ideal in $R$.

*Proof*: $\phi^{-1}(I) = \{r \in R|\phi(r) \in I\} \subseteq R$ isn't empty since $0 \in I$ and $\phi(0) = 0$ implies $0 \in \phi^{-1}(I)$. Let $a, b \in \phi^{-1}(I)$. Then $\phi(a), \phi(b) \in I$. Then $\phi(a-b) = \phi(a) + \phi(-b) = \phi(a) - \phi(b) \in I$ since $I$ is an additive subgroup of $S$. Thus $\phi^{-1}(I)$ is an additive subgroup of $R$ by the 1-step subgroup test. Let $r \in R$. $\phi(ar) = \phi(a)\phi(r) \in I$ since $\phi(a) \in I$, $\phi(r) \in S$, and $I$ is an ideal. Similarly, $\phi(ra) \in I$. Thus $ra, ar \in \phi^{-1}(I)$. So $\phi^{-1}(I)$ is an ideal of $R$ $\square$

**Proposition 14.2**: Let $R$ be a commutative ring with unity. $M$ is a maximal ideal of $R$ iff $R/M$ is a field.

*Proof*: Suppose $M$ is a maximal ideal of $R$. Since $M \neq R$ it follows that $1 \notin M$ (otherwise $r = r(1) \in M$ for all $r \in R$ implies $M = R$). So $R/M$ is a non-trivial commutative ring with unity $1 + M$. Let $r + M \in R/M$ be non-zero. So $r \notin M$.

Suppose $r + M$ does not have a multiplicative inverse in $R/M$. Then the set

$$(R/M)(r + M) = \{(a + M)(r + M)|a + M \in R/M\}$$

contains $r + M$, but does not contain $1 + M$.

That makes $(R/M)(r + M)$ a proper and nontrivial subset of $R/M$. It's very easy (ELFY) to show that $(R/M)(r + M)$ is an ideal of $R/M$.

Let $\phi : R \to R/M$ be given by $\phi(r) = r + M$. Clearly $\phi$ is an onto homomorphism (epimorphism). Set $I = \phi^{-1}((R/M)(r + M)) = \{s \in R|\phi(s) \in (R/M)(r + M)\}$. Then by the lemma above $I$ is an ideal in $R$ containing $M$ and $r \notin M$, but $I \neq R$ since $I$ does not contain 1 . That is a contradiction since $M$ is maximal. Hence $r + M$ has a multiplicative inverse. Thus $R/M$ is a field.

Conversely, assume $M \neq R$ is an ideal and $R/M$ is a field.

Let $N$ be an ideal of $R$ such that $M$ is properly contained in $N$. Then there exists $r \in N$ such that $r \notin M$. Then $r + M \neq 0 + M$ in $R/M$. Since $R/M$ is a field, $r + M$ has a multiplicative inverse $s + M \in R/M$ such that $(r + M)(s + M) = (s + M)(r + M) = sr + M = 1 + M$. Then $sr - 1 \in M$. Then $sr - 1 \in N$. Then $1 = sr \in N$ since $r \in N$ and $N$ is an ideal. Thus $x = x(1) \in N$ for all $x \in R$. Thus $R = N$ showing that $M$ is a maximal ideal $\square$

Let $R$ be a ring. An ideal $I$ of $R$ is a <u>prime ideal</u> if for all $a, b \in R$ we have that $ab \in I$ implies $a \in I$ or $b \in I$.

**Proposition 14.3**: Let $R$ be a commutative ring with unity. $P$ is a prime ideal of $R$ iff $R/P$ is an integral domain.

*Proof*: Assume $P$ is a prime ideal of $R$. Let $a+P, b+P \in R/P$. Suppose $(a+P)(b+P) = 0+P = P$. Well this means that $ab+P = P$ and hence $ab \in P$. But then $a \in P$ or $b \in P$ since $P$ is a prime ideal. But that makes $a+P = 0+P = P$ or $b+P = 0+P = P$. Thus $R/P$ is an integral domain.

Conversely, assume $P$ is an ideal of $R$ and $R/P$ is an integral domain. Suppose $a, b \in R$ and $ab \in P$. Then $ab+P = 0+P = P$. But that implies that $(a+P)(b+P) = 0+P = P$. Therefore either $a+P = 0+P = P$ or $b+P = 0+P = P$. So either $a \in P$ or $b \in P$, which shows that $P$ is a prime ideal $\square$

Putting together the last two propositions we get the following elegant result:

**Corollary 14.4**: Let $R$ be a commutative ring with unity. All maximal ideals of $R$ are prime ideals of $R$.

*Proof*: Assume $M$ is a maximal ideal of $R$. Then $R/M$ is a field. A field is an integral domain, so $R/M$ is an integral domain. Thus $M$ is a a prime ideal $\square$

**Proposition 14.5**: Let $F$ be a field. An ideal $(f) \neq (0)$ in $F[x]$ is maximal if and only if $f$ is irreducible over $F$.

*Proof*: Assume $(f) \neq (0)$ is a maximal ideal in $F[X]$. Then $(f) \neq F[X]$ and thus $\deg(f) \geq 1$. Suppose $f = gh$ is a factorization of $f(x)$ where $g, h \in F[X]$. Since $(f)$ is also a prime ideal we get that either $g \in (f)$ or $h \in (f)$.

But then it is not possible that both $g, h$ are of degree less than $\deg(f)$. Hence $f$ is irreducible over $F$.

Conversely, assume $f \in F[X]$ is irreducible over $F$. In particular, $(f) \neq F[X]$ is an ideal of $F[X]$. Suppose $M$ is an ideal of $F[X]$ and $(f) \subseteq M \subseteq F[X]$.

Since $F[X]$ is a PID we have that $M = (g)$ where $g \in F[X]$. Since $f \in (g)$ we get $f = gh$ for some $h \in F[X]$. But $f$ is irreducible over $F$, so we get that either $g$ or $h$ is of degree 0. If $g$ is of degree 0 then $M = (g) = F[X]$ (see proof of proposition 13.4). If $h$ is of degree 0 then $h \in F$ is invertible and hence $g = h^{-1}f \in (f)$ implies $M = (f)$. Thus $(f)$ is a maximal ideal of $F[X]$ $\square$

**Extension Fields**

Let $E, F$ be fields. We call $E$ an extension field of $F$ if $E \supseteq F$ (that is, $F$ is a subfield of $E$). In particular, this makes $E$ (using the field operations in $E$) a vector space over the field $F$ by the standard vector space axioms.

**Proposition 15.1 (Kronecker's Theorem)**: Let $F$ be a field and $f(x)$ be a non-constant polynomial in $F[X]$. Then there exists an extension field $E$ of $F$ and $\alpha \in E$ such that $f(\alpha) = 0$.

*Proof*: Since we can factor $f(x)$ into a product of irreducible polynomials in $F[X]$ it suffices to show that for an arbitrary irreducible $p(x) \in F[X]$ we can find an extension field $E$ of $F$ and $\alpha \in E$ such that $p(\alpha) = 0$.

So let $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[X]$ be irreducible. Then $(p(x))$ is a maximal ideal of $F[X]$, which makes $F[X]/(p(x))$ a field. Consider the canonical map $\psi : F \to F[X]/(p(x))$ given by $\psi(a) = a + (p(x))$. Clearly $\psi$ is a field homomorphism.

Let's show that $\psi$ is $1{-}1$. Let $a, b \in F$ and suppose $\psi(a) = \psi(b)$. Then $a + (p(x)) = b + (p(x))$. This implies that $a - b \in (p(x))$. So $a - b = p(x)q(x)$ for some $q(x) \in F[X]$. But the degree of $a - b$ is less than 1 and the degree of $p(x)$ is at least 1. The only way to reconcile this is for $q(x) = 0$. Thus $a = b$ showing that $\psi$ is $1 - 1$.

Then $F \cong \psi(F)$. So we can identify $F$ with the subfield $\psi(F) = \{a + (p(x)) | a \in F\}$ of $F[X]/(p(x))$. So we shall view $E = F[X]/(p(x))$ as extension field of $F \cong \psi(F)$ (as it is an extension field of $\psi(F)$).

With this in mind when we write $a \in F$, we can view it as the same as writing $a + (p(x)) \in E$. In particular, this means we can view $p(x)$ as an element of $E[X]$.

Let's find a zero for $p(x)$ in the extension field $E$. Let $\alpha = x + (p(x)) \in E$.

Consider that in $E$ we have

$$p(\alpha) = a_0 + a_1(\alpha) + \cdots + a_n(\alpha)^n = a_0 + a_1(x + (p(x))) + \cdots + a_n(x + (p(x)))^n =$$

$$= a_0 + a_1 x + \cdots + a_n x^n + (p(x)) = p(x) + (p(x)) = (p(x)) = 0.$$

So we have found an extension field $E = F[X]/(p(x))$ of $F \cong \psi(F)$ and $\alpha \in E$ such that $p(\alpha) = 0$ $\square$

Let's see this theorem in action! Consider the polynomial $f(x) = x^2 + 1$ in $\mathbb{R}[X]$. We know that $f(x)$ is irreducible over $\mathbb{R}$. So $(x^2+1)$ is a maximal ideal in $\mathbb{R}[X]$ and thus $\mathbb{R}[X]/(x^2+1)$ is an extension field of $\mathbb{R}$ (where we identity $\mathbb{R}$ with $\{a + (x^2+1) | a \in \mathbb{R}\} \subseteq \mathbb{R}[X]/(x^2+1)$).

Let $\alpha = x + (x^2 + 1) \in \mathbb{R}[X]/(x^2 + 1)$. Then

$$\alpha^2 + 1 = [x + (x^2+1)]^2 + [1 + (x^2+1)] = x^2 + 1 + (x^2+1) = (x^2+1) = 0$$

in $\mathbb{R}[X]/(x^2 + 1)$.

Let $E$ be an extension field of $F$. An element $\alpha \in E$ is algebraic over $F$ if there exists a non-constant polynomial $f \in F[x]$ such that $f(\alpha) = 0$. Otherwise, $\alpha$ is transcendental over $F$. If $\alpha \in E$ is algebraic over $F$ then the degree of $\alpha$ over $F$ is the degree of a polynomial $f \in F[X]$ of minimal degree such that $f(\alpha) = 0$.

ELFY: Let $E$ be an extension field of $F$. Show that if $\alpha \in E$ is algebraic of degree $n$ over $F$ and $f \in F[X]$ is of degree $n$ with $f(\alpha) = 0$ then $f$ is irreducible.

Consider that $\mathbb{R}$ is an extension field of $\mathbb{Q}$. Then we have that $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since for $f(x) = x^2 - 2 \in \mathbb{Q}[X]$ we have $f(\sqrt{2}) = 0$. Furthermore, the degree of $\sqrt{2}$ over $\mathbb{Q}$ is 2 since $\sqrt{2}$ isn't the root of a degree one polynomial in $\mathbb{Q}[X]$.

It is well-known (although very difficult to prove, and we won't) that the real numbers $\pi$ and $e$ are transcendental over $\mathbb{Q}$.

ELFY: Show that $\sqrt{1+\sqrt{2}}$ is algebraic over $\mathbb{Q}$.

Let $E$ be an extension field of a field $F$. Let $\alpha_1, \alpha_2, ..., \alpha_k \in E$. We denote by $F(\alpha_1, \alpha_2, ..., \alpha_k)$ the subfield of $E$ which is the smallest field extension of $F$ that contains $\alpha_1, \alpha_2, ..., \alpha_k$.

A field extension $E$ of $F$ is called a simple extension if $E = F(\alpha)$ for some $\alpha \in E$.

Example: $\mathbb{R}(i) = \mathbb{C}$ since once we have an extension of $\mathbb{R}$ that contains $i$, it must contain $a + bi$ for any $a, b \in \mathbb{R}$. So $\mathbb{C}$ is a simple extension of $\mathbb{R}$.

**Proposition 15.2** : Let $E$ be an extension field of $F$. Let $\alpha \in E$ be algebraic of degree $n$ over $F$. Then

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} | a_0, a_1, ..., a_{n-1} \in F\}.$$

Moreover, every element in $F(\alpha)$ is uniquely expressed in the form $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ where $a_0, a_1, ..., a_{n-1} \in F$.

*Proof*: Let $p(x) \in F[X]$ be an irreducible polynomial satisfying $\deg(p) = n$ and $p(\alpha) = 0$. WLOG assume that $p(x) = x^n - b_{n-1}x^{n-1} + \cdots - b_1 x - b_0$ where $b_0, b_1, ..., b_{n-1} \in F$. Then we have that

$$\alpha^n = b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0.$$

Obviously $K = \{c_0 + c_1\alpha + \cdots + c_m\alpha^m | m \in \{0, 1, ...\} \text{ and } c_0, c_1, ..., c_m \in F\} \subseteq F(\alpha)$.

By using that $\alpha^n = b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0$ (as many times as needed) we have that
$\{c_0+c_1\alpha+\cdots+c_m\alpha^m | m \in \{0, 1, ...\} \text{ and } c_0, c_1, ..., c_m \in F\} = \{a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1} | a_0, a_1, ..., a_{n-1} \in F\}$.

This means that to show that $F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} | a_0, a_1, ..., a_{n-1} \in F\}$ it just suffices to show that $K = \{c_0 + c_1\alpha + \cdots + c_m\alpha^m | m \in \{0, 1, ...\} \text{ and } c_0, c_1, ..., c_m \in F\}$ is a field.

Let $\phi_\alpha : F[X] \to K$ be given by $\phi_\alpha(f(x)) = f(\alpha)$. This is obviously an onto ring homomorphism (called an evaluation homomorphism). We have that $\text{Ker}(\phi_\alpha) = (p(x))$. Well, by the first isomorphism theorem $F[X]/(p(x)) \cong K$ is a field as $(p(x))$ is a maximal ideal.

Now we prove uniqueness. Suppose

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

where $a_0, a_1, ..., a_{n-1}, b_0, b_1, ..., b_{n-1} \in F$.

Then $(a_0 - b_0) + (a_1 - b_1)\alpha + \cdots + (a_{n-1} - b_{n-1})\alpha^{n-1} = 0$. Hence

$$f(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{n-1} - b_{n-1})x^{n-1} \in \text{Ker}(\phi_\alpha) = (p(x)).$$

So $f(x) = p(x)q(x)$ for some $q(x) \in F[X]$. Since the degree of $f(x)$ is less than the degree of $p(x)$ it follows that $q(x) = 0$ and thus $f(x) = 0$. Hence $a_i = b_i$ for all $i \in \{0, 1, ..., n-1\}$ $\square$

This proposition tells us something interesting: For a field extension $E$ of $F$ and an element $\alpha \in E$ that is algebraic of degree $n$ over $F$ we get that the simple extension field $F(\alpha)$ is a vector space of dimension $n$ over the field $F$ with basis $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$. We say that the degree of the simple extension $F(\alpha)$ over $F$ is that dimension $n$.

In this new language, we can say that $\mathbb{C}$ is a degree-2 simple extension of $\mathbb{R}$.

Example making use of vector space concepts: Consider $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ (smallest subfield of $\mathbb{R}$ containing $\sqrt{2}$ and $\sqrt{3}$) as an extension field of $\mathbb{Q}$. Let's show that $1, \sqrt{2}, \sqrt{3}, \sqrt{6} \in F$ are linearly independent over $\mathbb{Q}$:

First we note (ELFY) $\sqrt{2}, \sqrt{3}, \sqrt{6} \notin \mathbb{Q}$ and the product of a non-zero rational and an irrational is irrational.

It's clear that $\sqrt{2}, \sqrt{3}, \sqrt{6} \in F$. Suppose $a, b, c, d \in \mathbb{Q}$ and $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$.

Then $-a - d\sqrt{6} = b\sqrt{2} + c\sqrt{3}$. Squaring both sides gives $a^2 + 2ad\sqrt{6} + 6d^2 = 2b^2 + 2bc\sqrt{6} + 3c^2$. Then $(2ad - 2bc)\sqrt{6} \in \mathbb{Q}$ implies $ad = bc$ since $\sqrt{6} \notin \mathbb{Q}$ and the product of a non-zero rational and an irrational is irrational. Notice that $a$ or $d$ is zero iff $b$ or $c$ is zero.

This gives three cases worth examining:

Case 1: $a = 0$. In this case $b = 0$ or $c = 0$. Suppose $b = 0$. Then $c\sqrt{3} + d\sqrt{6} = 0$ This implies that $c\sqrt{3} = -d\sqrt{6}$. Dividing both sides by $\sqrt{3}$ gives $3c = -d\sqrt{2}$ which implies $d = 0$ since $\sqrt{2} \notin \mathbb{Q}$ and the product of a non-zero rational and an irrational is irrational. Thus $c = 0$, showing that the vectors are linearly independent. A similar argument holds when $c = 0$.

Case 2: $d = 0$. In this case $b = 0$ or $c = 0$. Suppose $b = 0$. Then $a + c\sqrt{3} = 0$ implies as above that $c = 0$ and then $a = 0$, showing that the vectors are linearly independent. A similar argument holds when $c = 0$.

Case 3: $a \neq 0$ and $d \neq 0$. Then $b \neq 0$ and $c \neq 0$. Then

$$0 = 2b^2 + 3c^2 - 6d^2 - a^2 = 2b^2d^2 + 3c^2d^2 - 6d^4 - b^2c^2 = (b^2 - 3d^2)(2d^2 - c^2).$$

We get a contradiction since $c^2 - 2d^2 \neq 0$ and $b^2 - 3d^2 \neq 0$, as otherwise $c = \pm\sqrt{2}d$ or $b = \pm\sqrt{3}d$ is not rational as the product of a non-zero rational and irrational is irrational. This contradiction completes the argument as now it follows that $a = b = c = d = 0$ making $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ linearly independent over $\mathbb{Q}$.

In general, whenever $E$ is a field extension of $F$, and $E$ has finite dimension $n$ as a vector space over $F$, then the degree of E over $F$ is $n$ and we use the notation $[E : F] = n$.

ELFY: Let $E, F, K$ be fields. Show that if $K$ is a field extension of finite degree over $E$ and $E$ is a field extension of finite degree over $F$ then $[K : F] = [K : E][E : F]$. Hint: Play with bases.

A field $F$ is algebraically closed if every non-constant polynomial $f(x) \in F[X]$ has a zero in $F$. Clearly the fields $\mathbb{Q}$ and $\mathbb{R}$ are not algebraically closed, as we have seen.

We just state the following theorem since it is fundamental to this subject, however we don't give a proof. It has a very simple proof using complex analysis (not given here) and some very difficult proofs using just algebra (also not given here).

**Proposition 15.3 (The Fundamental Theorem of Algebra** : Every non-constant polynomial $f(x) \in \mathbb{C}[X]$ has a zero in $\mathbb{C}$. In other words, $\mathbb{C}$ is algebraically closed.

Here is another important theorem we just state without proof to save the time:

**Proposition 15.4** : Every field $F$ has an algebraic closure $\bar{F}$, which is an extension field of $F$ that is algebraically closed.

**Finite Fields**

The primary goal of this section will be to show that there exists a finite field of order $p^n$ where $p \in \mathbb{N}$ is a prime and $n \in \mathbb{N}$. We already know that there is (up to isomorphism) exactly one field with $p \in \mathbb{N}$ elements where $p$ is a prime, namely $\mathbb{Z}_p$. We will now denote these fields by $\mathbb{F}_p$ instead of $\mathbb{Z}_p$.

**Proposition 16.1**: Let $F$ be a finite field with $q$ elements. Let $E$ be a field extension of $F$ of degree $n$. Then $E$ has $q^n$ elements.

*Proof*: Let $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ be a basis for $E$ as a vector space over $F$. Then every element $\beta \in E$ can be written uniquely in the form

$$\beta = b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n.$$

Thus this turns into a simple counting problem: How many such expressions above are there? Well, there are $q$ choices for the field element from $F$ chosen as the scalar on $\alpha_i$ for $i = 1, 2, .., n$ so by the multiplication principle there are $q^n$ elements in $E$ $\square$

**Corollary 16.2**: Let $E$ be a finite field of characteristic $p \in \mathbb{N}$ where $p$ is a prime. Then $E$ contains $p^n$ elements where $n \in \mathbb{N}$.

*Proof*: Clearly $E$ contains $< 1 >= \{1, 1+1, 1+1+1, ...\} = \mathbb{F}_p$ as a subfield. Since $E$ is a finite field, it must be of degree $n$ over $F$ for some $n \in \mathbb{N}$. Then by the previous proposition, $E$ has $p^n$ elements $\square$

**Lemma 16.3**: Let $F$ is a finite field with $q$ elements. Then $a^q = a$ for all $a \in F$.

*Proof*: Clearly $0^q = 0$. Since the non-zero elements of $F$ form a multiplicative group of order $q - 1$ we have that $a^{q-1} = 1$ for all non-zero $a \in F$, since the order of any group element divides the order of the group. Thus $a^q = a$ for all $a \in F$ $\square$

This gives us a beautiful result:

**Lemma 16.4**: Let $F$ is a finite field with $q$ elements. Then $x^q - x \in F[X]$ factors into

$$x^q - x = \prod_{a \in F}(x - a).$$

*Proof*: Since $f(x) = x^q - x$ is of degree $q$ it has at most $q$ roots in $F$. By the previous lemma, every element in $F$ is a root of $f(x)$, giving $q$ distinct roots in $F$. By the Root-Factor Correspondence we get that

$$f(x) = \prod_{a \in F}(x - a) \ \square$$

Let $F$ be a field. Define the derivative operator $D : F[X] \to F[X]$ by the rule

$$D(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1.$$

Let's justify the "product rule:"

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ be in $F[X]$.

Then $f(x)g(x) = \displaystyle\sum_{j=0}^{n}\sum_{k=0}^{m} a_j b_k x^{j+k}$ and thus $D(f(x)g(x)) = \displaystyle\sum_{j=0}^{n}\sum_{k=0}^{m} (j+k) a_j b_k x^{j+k-1}$

$D(f(x)) = \displaystyle\sum_{j=0}^{n} j a_j x^{j-1}$ and $D(g(x)) = \displaystyle\sum_{k=0}^{n} k b_k x^{k-1}$ so

$$D(f(x))g(x) + f(x)D(g(x)) = \sum_{j=0}^{n}\sum_{k=0}^{m} j a_j b_k x^{j+k-1} + \sum_{j=0}^{n}\sum_{k=0}^{m} k a_j b_k x^{j+k-1} = D(f(x)g(x)).$$

**Lemma 16.4**: Let $F$ be a field and $f(x) \in F[X]$. Then for any $r \in F$, if $f(x) = g(x)(x-r)^2$ for some $g(x) \in F[X]$ then $D(f(x))(r) = 0$.

*Proof*: Suppose $r \in F$ and $f(x) = g(x)(x-r)^2$ for some $g(x) \in F[X]$. Then we have that $f(x) = g(x)(x^2 - 2rx + r^2)$. By the product rule, $D(f(x)) = D(g(x))(x-r)^2 + 2g(x)(x-r)$. Hence $D(f(x))(r) = 0$ $\square$

**Proposition 16.5**: Let $p \in \mathbb{N}$ be a prime and $n \in \mathbb{N}$. There exists a field $\mathbb{F}_{p^n}$ with $p^n$ elements.

*Proof*: Let $\bar{F}$ be the algebraic closure of $\mathbb{F}_p$. Obviously the characteristic of $\bar{F}$ is still $p$. Consider that for $q = p^n$ the polynomial $f(x) = x^q - x$ completely factors into linear factors in $\bar{F}[X]$. We see that $D(f(x)) = qx^{q-1} - 1 = -1$ in $\bar{F}[X]$, so $f(x) = x^q - x$ does not have any repeated roots in $\bar{F}$ by the previous lemma.

So $S = \{a \in \bar{F} | a^q - a = 0\}$ has $q$ distinct elements. Let's show that $S$ is a field:

Clearly $0, 1 \in S$.

For $a, b \in S$ we have that $(a-b)^q = a^q - b^q = a - b \in S$ by using the binomial theorem since $q = p^n$ and the characteristic of $\bar{F}$ is $p$. So $(S, +)$ is an abelian group (as it is a subgroup of the abelian group $(\bar{F}, +)$).

For non-zero $a, b \in S$ we have that $(ab^{-1})^q = a^q b^{-q} = ab^{-1} \in S$. So $(S^*, \cdot)$ forms a multiplicative group (as it is a subgroup of $(\bar{F}^*, \cdot)$).

So $S$ is a field with $q = p^n$ elements $\square$

It turns out that (up to isomorphism) $S$ is the unique field with $p^n$ elements, but we will not devote the time required to prove this.

Standard notation: $\mathbb{F}_q$ is the field (up to isomorphism) with $q = p^n$ elements (where $p \in \mathbb{N}$ is prime and $n \in \mathbb{N}$).

Let's play with $\mathbb{F}_9$. First, let's construct this field as a quotient of $\mathbb{F}_3[X]$. Consider the polynomial $f(x) = x^2 + 2x + 2 \in \mathbb{F}_3[X]$. $f(0) = 2$, $f(1) = 2$, and $f(2) = 1$. Hence $f(x)$ is irreducible in $\mathbb{F}_3[X]$. Thus $I = (f(x))$ is a maximal ideal and $\mathbb{F}_3[X]/I$ is a field with 9 elements:

$$\mathbb{F}_9 \cong \{0+I, 1+I, 2+I, x+I, x+1+I, x+2+I, 2x+I, 2x+1+I, 2x+2+I\}.$$

ELFY: Make addition and multiplication tables for $\mathbb{F}_9$.

Let's take advantage of $x^2 + I = x + 1 + I$:

Consider that $\mathbb{F}_9^* \cong \{1+I, 2+I, x+I, x+1+I, x+2+I, 2x+I, 2x+1+I, 2x+2+I\}$ and

$$(x+I)^2 = x^2 + I = x + 1 + I,$$

$$(x+I)^3 = x^2 + x + I = 2x + 1 + I,$$

$$(x+I)^4 = 2x^2 + x + I = 2 + I,$$

$$(x+I)^5 = 2x + I,$$

$$(x+I)^6 = 2x^2 + I = 2x + 2 + I,$$

$$(x+I)^7 = 2x^2 + 2x + I = x + 2 + I,$$

and

$$(x+I)^8 = x^2 + 2x + I = 1 + I.$$

So the non-zero elements of this field is generated as a multiplicative group by $x + I$.

Note: A similar construction occurs with $g(x) = x^2 + x + 2$. Why?

**Proposition 16.6**: Let $q = p^n$ where $p \in \mathbb{N}$ be a prime and $n \in \mathbb{N}$. The multiplicative group $\mathbb{F}_q^*$ is cyclic.

*Proof*: We may assume $q \geq 4$ as otherwise $q - 1 \leq 3$ (all groups of orders 1, 2, or 3 are cyclic). Set $h = q - 1$ and let

$$h = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

be a prime factor decomposition of $h$.

Let $i \in \{1, 2, ..., k\}$. The polynomial $x^{h/p_i} - 1$ has at most $h/p_i$ roots in $\mathbb{F}_q$. Since $h/p_i < h$ it follows that there are non-zero elements of $\mathbb{F}_q$ which are not roots of $x^{h/p_i} - 1$. Let $a_i \in \mathbb{F}_q^*$ be such a non-root. Set

$$b_i = a_i^{h/(p_i^{n_i})}.$$

Then $b_i^{p_i^{n_i}} = a_i^h = 1$, but $b_i^{p_i^{n_i - 1}} = a^{h/p_i} \neq 1$.

So on one hand the order of $b_i$ divides $p_i^{n_i}$. On the other hand the order of $b_i$ is greater than $p_i^{n_i - 1}$. That means $b_i$ must be of order $p_i^{n_i}$.

Let $b = b_1 b_2 \cdots b_k$. We claim that the order of $b$ is $h$ and thus generates $\mathbb{F}_q^*$ which is hence a cyclic group.

Let's prove the claim. To yield a contradiction, suppose the order of $b$ is actually less than $h$, making it a proper divisor of $h$.

Then the order of $b$ would have to be a divisor of at least one $h/p_i$ where $i \in \{1, 2, .., k\}$. WLOG assume the order of $b$ divides $h/p_1$.

Then

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \cdots b_k^{h/p_1}.$$

For $i = 2, 3, ..., k$ we have that $p_i^{n_i}$ divides $h/p_1$ and thus $b_i^{h/p_1} = 1$. Therefore,

$$1 = b_1^{h/p_1}.$$

So the order of $b_1$ divides $h/p_1$, but that contradicts the fact that the order of $b_i$ is $p_1^{n_1}$.

So $b$ generates $\mathbb{F}_q^*$ showing that it is a cyclic group $\square$

Generators of $\mathbb{F}_q^*$ are called primitive elements of $\mathbb{F}_q$.

One last bit of fun with finite fields:

Let $p \in \mathbb{N}$ be prime and $m, n \in \mathbb{N}$. Consider $GL_m(\mathbb{F}_q)$, the general linear group of $m \times m$ matrices over $\mathbb{F}_q$, where $q = p^n$. How many elements are there in this finite group?

It's a pretty neat counting problem: The first column can be any non-zero vector in the vector space $\mathbb{F}_q^m$. Well, clearly there are $q^m - 1$ such vectors. The second column can be any vector not contained in the span of the first column. There are $q$ vectors in the span of the first column, so that gives $q^m - q$ such vectors. The third column can be any vector not contained in the span of the first two columns. There are $q^2$ vectors in the span of the first two columns, so that gives $q^m - q^2$ such vectors.

Continue in this way until we arrive at $q^m - q^{m-1}$ possible vectors for the last column (requiring they aren't in the span on the previous $m - 1$ columns).

Hence by the multiplication principle, we get

$$|GL_m(\mathbb{F}_q)| = \prod_{i=0}^{m-1} q^m - q^i.$$

ELFY: How many elements are there in the group $GL_2(\mathbb{F}_2)$? Would it be easy to write them all down? How about $GL_3(\mathbb{F}_2)$ or $GL_2(\mathbb{F}_4)$?