Content:

Definition	char (R)
Example	What must a field of order 4 look like?
Proposition	If F is a field, char $F = 0$, then F contains a subfield $\cong \mathbb{Q}$.
	If char $F = p$, then F contains a subfield $\cong \mathbb{Z}_p$.
Proposition	Every finite field has order p^n for some prime p and some positive integer n.
Example	If $p(x) = x^3 + x + 1 \in \mathbb{Z}_5[x]$, then $F = \mathbb{Z}_5[x]/(p(x))$ is a field.
Definition	extension field
Definition	$[E : F]$
Example	If $F = \mathbb{Z}_5[x]/(p(x))$, then $[F: \mathbb{Z}_5] = 3$
Example	$[\mathbb{Q}[i]:\mathbb{Q}] = 2$
Definition	$F[a]$, $F(a)$
Proposition	$F(a) \cong \text{Frac}(F[a])$.
Proposition	If E/F is an extension and $a \in E$, then $F[a] = \varphi_a(F[x])$ where $\varphi_a: F[x] \to F[a]$ is the evaluation homomorphism.

Recall (From lecture notes 11/18/09) char (R) = $n \Leftrightarrow n$ is the smallest positive integer such that $n \bullet 1_R = 0$.
We say char (R) = 0 if no such positive integer exists.

Proposition If F is a field, then char (F) = 0 or char (F) = p for some prime p.

Proof:
If char (F) = 0, we're done.
Assume char (F) = m, m a positive composite integer.
Then $m = kt$ for integer k, t such that $1 < k < m$ and $1 < t < m$.
So we have $(k \bullet 1_F)(t \bullet 1_F) = \underbrace{(1_F + 1_F + \cdots + 1_F)}_{k \text{ summands}} \underbrace{(1_F + 1_F + \cdots + 1_F)}_{t \text{ summands}}$

$= \underbrace{(1_F \bullet 1_F + 1_F \bullet 1_F + \cdots + 1_F \bullet 1_F)}_{kt \text{ summands}} = \underbrace{(1_F + 1_F + \cdots + 1_F)}_{kt \text{ summands}} = m \bullet 1_F = 0$ (*)

Since F has no zero divisors, then $(k \bullet 1_F)(t \bullet 1_F) = 0$ implies $k \bullet 1_F = 0$ or $t \bullet 1_F = 0$. But m is the smallest positive integer such that $m \bullet 1_R = 0$ yet $1 < k < m$ and $1 < t < m$, a contradiction.
$\therefore$ char (F) = p, for some prime integer p.

Example What must a field of order 4 look like?
$F = \{0, 1, a, b\}$. So char (F) = 2 (by above proposition)
$F \cong$ Klein 4 as a group.
$|F^*| = 3$ and (F^*, $\bullet$) is a group.
So $F^* \cong \mathbb{Z}_3$ as a group under $\bullet$.

Note We cannot have a field of order 6. If so, then by Cauchy's Theorem, we must have an element of order 2 and one of order 3. So then char $(F) = 2$, but $2 \bullet a \neq 0$ where $\text{ord}(a) = 3$, a contradiction.

Proposition Let F be a field. If char $(F) = 0$, then F contains a subfield isomorphic to $\mathbb{Q}$. If char $(F) = p$, then F contains a subfield isomorphic to $\mathbb{Z}_p$.

Proof:
Define $\varphi: \mathbb{Z} \to F$ where $\varphi(n) = n \bullet 1_F$. Then
$\varphi(m + n) = (m + n) \bullet 1_F = m \bullet 1_F + n \bullet 1_F = \varphi(m) + \varphi(n)$ and
$\varphi(mn) = (mn) \bullet 1_F = (m \bullet 1_F)(n \bullet 1_F) = \varphi(m)\,\varphi(n)$ by (*) in proof of "If F is a field, then char $(F) = 0$ or char $(F) = p$ for some prime p."
$\therefore$ φ is a homomorphism.
By the First Isomorphism Theorem, $\mathbb{Z}/\ker \varphi \cong \varphi(\mathbb{Z})$.
Case 1: If char $(F) = 0$, then $\ker \varphi = \{0\}$. So $\mathbb{Z} \cong \varphi(\mathbb{Z})$.
Recall "$\text{Frac}(\mathbb{Z}) \cong \mathbb{Q}$ by homomorphism $\psi: \text{Frac}(\mathbb{Z}) \to \mathbb{Q}$ where $\psi([a, b]) = ab^{-1}$", Lecture Notes 12/7/09.
Since $\text{Frac}(\mathbb{Z}) \cong \mathbb{Q}$ and $\mathbb{Z} \cong \varphi(\mathbb{Z})$, then $\text{Frac}(\varphi(\mathbb{Z})) \cong \mathbb{Q}$.
But $\text{Frac}(\varphi(\mathbb{Z}))$ is the smallest field containing $\varphi(\mathbb{Z})$ and F is "a" field containing $\varphi(\mathbb{Z})$, so $\text{Frac}(\varphi(\mathbb{Z})) \subseteq F$.
Case 2: If char $(F) = p$, then $\ker \varphi = (p)$. So $\mathbb{Z}_p = \mathbb{Z}/(p) \cong \varphi(\mathbb{Z}) \subseteq F$.

Proposition Every finite field has order p^n for some prime p and some positive integer n.

Proof:
Let F be a finite field. Then char (F) = p (otherwise $|F| \bullet a \neq 0\ \forall\ a \in F$, a contradiction to Cauchy's Theorem)
By the previous proposition, $\mathbb{Z}_p \cong E$ where E is a subfield of F.
And this implies E is a subspace of F, hence F is a vector space over $E \cong \mathbb{Z}_p$. Let $\dim_{\mathbb{Z}_p} F = n$. Then, since $E \cong \mathbb{Z}_p$, vector space homework #9 gives us that $|F| = p^n$.

Example If $p(x) = x^3 + x + 1 \in \mathbb{Z}_5[x]$, then $F = \mathbb{Z}_5[x]/(p(x))$ is a field.

Proof:
$p(x)$ has no roots in $\mathbb{Z}_5[x]$, and is of 3rd degree, hence is irreducible in $\mathbb{Z}_5[x]$. Since $\mathbb{Z}_5[x]$ is a PID then $(p(x))$ is maximal.
Thus, $F = \mathbb{Z}_5[x]/(p(x))$ is a field.

Example (Continued from previous example)
If $p(x) = x^3 + x + 1 \in \mathbb{Z}_5[x]$ and $F = \mathbb{Z}_5[x]/(p(x))$ then $|F| = 125$.

Proof:
Elements in F are of the form $f(x) + (p(x))$ where $f(x) \in F = \mathbb{Z}_5[x]$.
Since $\mathbb{Z}_5$ is a field, then $F = \mathbb{Z}_5[x]$ is an ER, hence we can use the division algorithm. There exist unique $q(x)$ and $r(x) \in \mathbb{Z}_5[x]$ such that $f(x) = p(x)q(x) + r(x)$ where $r(x) = 0$ and $\deg r(x) < \deg p(x)$.
So $f(x) + (p(x)) = p(x)q(x) + r(x) + (p(x)) = r(x) + (p(x))$
since $p(x)q(x) \in (p(x))$.
So any element in F can be expressed as $r(x) + (p(x))$ where $r(x) = a_0 + a_1x + a_2x^2$ for some $a_i \in \mathbb{Z}_5$.
These cosets are unique as
$r_1(x) + (p(x)) = r_2(x) + (p(x)) \Rightarrow r_1(x) - r_2(x) \in (p(x))$, $p(x)$ is of minimal degree in $(p(x))$, and $\deg(r_1(x) - r_2(x)) \leq 2$, hence $r_1(x) - r_2(x) = 0$.
So $|F| = 5^3 = 125$.

Note We have also shown that any element in F can be expressed uniquely as a linear combination of $1 + (p(x))$, $x + (p(x))$, and $x^2 + (p(x))$.
So an isomorphic copy of $\mathbb{Z}_5$ is a subfield of F.

Definition Let E/F be an extension. The degree of E/F is denoted $[E : F]$ is the dimension of E over F as a vector space.
i.e. $[E : F] = \dim_F E$.

Example $F = \mathbb{Z}_5[x]/(p(x))$, where $p(x) = x^3 + x + 1$, then $F/\ \mathbb{Z}_5$ is an extension and $[F : \mathbb{Z}_5] = 3$.

Example $\mathbb{Q}[i]/\mathbb{Q}$ is an extension and $[\mathbb{Q}[i] : \mathbb{Q}] = 2$.

Note $[F : \mathbb{Z}_5] = 3$ and $x^3 + x + 1$ has degree 3 is not a coincidence.

Definition Let E/F be an extension and $a \in E$.
(1) $F[a]$ is the smallest ring containing F and a.
(2) $F(a)$ is the smallest field containing F and a.

Note We know $a \in F[a]$ and and $a \in F(a)$.
So if $a \neq 0$, then $a^{-1} \in F(a)$ but might not be in $F[a]$.
So $F[a]$ is bigger than $F(a)$.

Note $F[a] \subseteq F(a)$ since $F(a)$ is also a ring containing F and a.

Proposition $F(a) \cong \text{Frac}(F[a])$.

Proof:
Since $F(a)$ is a field, hence a ring that contains F and a and
$F[a]$ is the smallest ring that contains F and a, then $F[a] \subseteq F(a)$.
Thus, $F(a)$ is a field that contain $F[a]$.
Recall from Lecture Notes 12/7/09,
(1) Frac(R) contains an isomorphic copy of R and
(2) Frac(R) is the smallest field containing [an ismo copy of] R.
Since Frac($F[a]$) is the smallest field containing the ring $F[a]$,
and $F(a)$ is "a" field that contains $F[a]$, then Frac($F[a]$) "$\subseteq$" $F(a)$.
To show the reverse "containment", notice that
$F(a)$ is the smallest field that contains F and a while
Frac($F[a]$) is "a" field that contains F and a.
Thus, $F(a) \cong \text{Frac}(F[a])$.

Proposition Let E/F be an extension and $a \in E$, then $F[a] = \varphi_a(F[x])$ where $\varphi_a: F[x] \to F[a]$ is the evaluation homomorphism.

Proof:
Let $\varphi_a : F[x] \to F[a]$ be defined by $\varphi_a(f(x)) = f(a)$ $\forall f(x) \in F[x]$.
Recall $\varphi_a : F[x] \to F$ is a homomorphism (Lecture Notes 11/18/09).

If $f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$, for some $c_i \in F$, then
$\varphi_a(f(x)) = c_0 + c_1a + \cdots + c_na^n \in \varphi_a(F[x])$.
Thus $\varphi_a(f(x)) \in F[a]$ by closure.

(ie. $c_ia^i \in F[a]$ by definition of $F[a]$, hence $\sum_{i=0}^{n} c_i a^i \in F[a]$ by closure.)

$\therefore$ $\varphi_a(F[x]) \subseteq F[a]$.

To show the reverse containment,
we will show $\varphi_a(F[x])$ is "a" ring that contains F and a,
hence $F[a]$, the smallest ring containing F and a,
is contained in $\varphi_a(F[x])$.
Let $x \in F[x]$. Then $\varphi_a(x) = a$ and $\varphi_a(x) \in \varphi_a(F[x])$, so $a \in \varphi_a(F[x])$.
Let $b \in F$, then $b = bx^0 \in F[x]$, and $\varphi_a(bx^0) = b$.
So then $\varphi_a(bx^0) \in \varphi_a(F[x])$, hence $b \in \varphi_a(F[x])$. Thus $F \subseteq \varphi_a(F[x])$.

And so we have $F[a] \subseteq \varphi_a(F[x])$.

$\therefore$ $F[a] = \varphi_a(F[x])$ as desired.