Proposition 0.1. Let \( R \) be a commutative ring. TFAE:

1. Every ideal in \( R \) is finitely generated.
2. Every chain of ideals \( I_1 \subseteq I_2 \subseteq \cdots \) is stable. That is, there exists \( n \) such that \( I_n = I_{n+1} = \cdots \).
3. Every nonempty set of ideals has a maximal element wrt inclusion.

Proof.

1. (1) \( \implies \) (2). \( I = \bigcup_k I_k \) ideal in \( R \). \( I \) is generated by \( x_1, x_2, \ldots, x_m \). There exists \( n \) such that \( x_1, \ldots, x_m \in I_n \). \( I_n = I \), this implies \( I_n = I_{n+1} = I_{n+2} = \cdots = I \).

2. (2) \( \implies \) (3). Let \( A \) be nonempty set of ideals. Suppose \( A \) has no maximal element. Pick \( I \in A \). Find chain in \( A \)

\[ I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \]

a contradiction.

3. (3) \( \implies \) (1). \( I \subseteq R \) ideal. Suppose \( I \) is not finitely generated. Construct \( x_1, x_2, \ldots \in I \).

\[ x_2 \in I \setminus \langle x_1 \rangle, \ x_3 \in I \setminus \langle x_1, x_2 \rangle. \]

This yields

\[ \langle x_1 \rangle \subseteq \langle x_1, x_2 \rangle \subseteq \langle x_1, x_2, x_3 \rangle \subseteq \cdots \]

Then \( A = \{ \langle x_1, x_2, \ldots, x_i : i \geq 1 \} \) has no maximal element, a contradiction.

\( R \) satisfying (1), (2), (3) is called Noetherian.

Example 0.2.

1. PID is Noetherian \( \mathbb{Z} \), \( \mathbb{Z}[i] \), \( F[X] \).

2. (Later) If \( R \) is Noetherian, then so is \( R[X] \). (Hilbert Basis Theorem)

Theorem 0.3. Every PID is a UFD.

Proof. Primes \( \equiv \) irreducibles. Existence: Let \( A = \{ aR \neq 0 : a \text{ has no factorization} \} \). But if \( A \neq \emptyset \), it has a maximal element \( aR \). \( a \) is not prime. So \( a \) is not irreducible. Write \( a = bc, \ b \in R^\times, \ c \in R^\times \). Then \( aR \subseteq bR \), and \( aR \subseteq cR \). So \( bR, cR \notin A \). So \( b \) and \( c \) have factorizations. Then \( a = bc \) has factorization, contradiction.

Uniqueness: \( a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m \), \( p_i, q_j \) primes. Need \( n = m \) and there exists \( \sigma \in S_n \) such that \( q_i \sim p_{\sigma(i)} \). Induction on \( n \). \( p_n \mid a = q_1 \cdots q_m \), so \( p_n \mid q_i \) for some \( i \). But \( q_i \) is prime, hence irreducible, so \( q_i = p_n u, u \in R^\times \). So \( q_i \sim p_n \). May assume \( i = m \). So \( q_m = p_n u \). Cancelling, \( p_1 \cdots p_{n-1} = q_1 \cdots q_{m-1} u \). Use induction.

\( F[X_1, \ldots, X_n] \) is not PID, but UFD.
1 Localization

A subset $S \subseteq R$ is called multiplicative if $x, y \in S$, then $xy \in S$.

Example 1.1.
1. $a \in R$, $s = \{a^i : i \geq 0, 1\}$.
2. $P \subseteq R$ prime ideal, $S = R \setminus P$. Note $xy \in P$ implies $x \in P$ or $y \in P$, and if $x \notin P$ and $y \notin P$, then $xy \notin P$.
3. $S$ = set of (nonzero) elements that are not zero divisors.

$S \subseteq R$ be nonempty multiplicative subset. $X = R \times S$. Relation on $X$, $\sim$, we say $(r, s) \sim (r', s')$ iff $\exists t \in S, t(rs' - r's) = 0$. $\sim$ is an equivalence relation.

Remark:
1. $(r, s) \sim (r, s)$ Take any $t$.
2. $(r, s) \sim (r', s')$ implies $(r', s') \sim (r, s)$ by symmetry.
3. $(r, s) \sim (r'', s'')$ We have $t(rs' - r's) = 0$ and $trs' = tr's$. Also, $t'(r's' - r''s') = 0$. So $t'r's' = t'r''s'$. Then note $tt's'(rs'' - r''s) = 0$. Why? Observe $tt's' \in S$. Then $tt's'rs'' = tr's's'' = t'r''s'rs$ so that $tt's'(rs'' - r''s) = 0$.

$S^{-1}R$ = set of equivalence classes $= \{r/s : r \in R, s \in S\}$ Then

$$\frac{r}{s} = \frac{r'}{s'} \iff \exists t \in S : t(rs' - r's) = 0.$$ 

We have operations

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}, \quad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}.$$ 

$S^{-1}R$ is a commutative ring. Then $O_{S^{-1}R} = \frac{0}{s}, 1_{S^{-1}R} = \frac{s}{s}$. This is localization of $R$ with respect to $S$.

We have map $f : R \to S^{-1}R : r \mapsto \frac{rs}{s}$ is a ring homomorphism. Note if $r \in S$,

$$f(r) = \frac{rs}{s} \in (S^{-1}R)^\times$$

since $(rs/s) \cdot (s/rs) = 1_{S^{-1}R}$. So $f(S) \subseteq (S^{-1}R)^\times$.

Remark 1 (Properties).
1. $S^{-1}R = 0 \iff 0 \in S$. We have $s/s = 0/s$ if $\exists t \in S$ such that $ts^2 = 0$.
2. If $R$ is a domain and $0 \notin S$, then $S^{-1}R$ is also a domain and $f : R \to S^{-1}R$ is injective.
3. If $R$ is a domain, and $S$ is $R \setminus \{0\}$, then $S^{-1}R$ is a field containing $R$. This field is called the fraction field, or quotient field of $R$.

$R = \mathbb{Z}$, $S = \mathbb{Z} \setminus \{0\}$, invert $S$, get $\mathbb{Q}$. Note $r/s = r'/s'$ in $\mathbb{Q}$ when $rs' = r's$.

2 January 8, 2014

Theorem 2.1. (Universal Property of Localization) Let $S \subseteq R$ be a multiplicative subset in a commutative ring $R$, $g : R \to T$, such that $g(S) \subseteq T^\times$. Then there exists unique ring homomorphism $h : S^{-1}R \to T$ such that the diagram 1 is commutative.

Proof. $f(r) = \frac{rs}{s}$,

$$h(r/s) = h\left(\frac{rs}{s} \cdot \frac{s^2}{s}\right)^{-1} = h(rs/s) \cdot h(s^2/s)^{-1} = h(f(s)h(f(s))^{-1} = g(r)g(s)^{-1}.$$ 

Define $h(r/s) = g(r) \cdot g(s)^{-1}$.

Consider the category, $S \subseteq R$ fixed, with objects $g : R \to T$ with $g(S) \subseteq T^\times$. Morphisms. Then the theorem $\iff f : R \to S^{-1}R$ is an initial object in the category. IF $R$ a domain, $S = R \setminus \{0\}$, $F = S^{-1}R \supset R$ is quotient field of $R$. 

\[ \square \]
2.1 Factorization in polynomial rings

$R$ domain, $R[X]$ domain, $\deg(f) \geq 0$, $\deg(fg) = \deg(f) + \deg(g)$, $R[X]^\times = R^\times$. $R \subseteq S$, then $f \in R[X] \subseteq S[X]$.

**Example 2.2.** 1. $2X \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$ is not irreducible over $\mathbb{Z}$, but irreducible over $\mathbb{Q}$.

2. $x^2 + 1$ is irreducible over $\mathbb{R}$, but not irreducible over $\mathbb{C}$.

\[ a \in R \subseteq R[X], \text{ } a \text{ is irreducible in } R \text{ iff } a \text{ is irreducible in } R[X]. \]

Now suppose $R$ is a UFD, $a_1, a_2, \ldots, a_n \in R$. Write $a_i = u_i \cdot \prod_j c_j^{n_{ij}}$, $u_i \in R^\times$, $m_{ij} \geq 0$, and $c_j$ irreducible. Then

\[ \gcd(a_i) = \left( \prod_j c_j^{n_j} \right) R \]

where $n_j = \min(m_{ij})$, $a_1, \ldots, a_n$ relatively prime if $\gcd(a_i) = R \iff a_i$ have no common irreducible divisor. Now take $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in R[X]$ nonzero. $R \supset \gcd(a_i) = C(f)$ is the content of $f$. We say $f$ is primitive if $C(f) = R$, i.e., the coefficients of $f$ are relatively prime. Every monic polynomial is primitive. Note $C(a) = Ra$, and $C(af) = aC(f)$.

If $C(f) = Ra$, $f = af'$ for $f' \in R[X]$ primitive.

**Lemma 2.3.** (Gauss Lemma) If $f, g \in R[X]$ are primitive, then $fg$ is primitive.

**Proof.** Let $c$ be an irreducible element in $R$. Need: not all coefficients of the product $fg$ are divisible by $c$. Consider $R/(c)$. Note $(c)$ is a prime ideal since $c$ is also prime, so $R/(c)$ is a domain, denote it $\bar{R}$. The map $R \to \bar{R}$ induces a map $R[X] \to \bar{R}[X]$ with $f \mapsto \bar{f}$. Then $fg \mapsto \bar{fg} = \bar{f}\bar{g}$. But $\bar{f} \neq 0$, $\bar{g} \neq 0$ since $f$ and $g$ are primitive. But $\bar{R}[X]$ is a domain, so $\bar{fg} = \bar{f}\bar{g} \neq 0$. \hfill \Box

**Corollary 2.4.** $C(fg) = C(f)C(g)$.

**Proof.** $C(f) = Ra$, $f = af'$, $f'$ primitive, and $C(g) = Rb$, $g = bg'$, $g'$ primitive. Then $fg = ab(f'g')$, $f'g'$ primitive by lemma, so

$$C(fg) = abC(f'g') = abR = C(f)C(g).$$ \hfill \Box

$R \subseteq F$ quotient field of $R$. So $R[X] \subset F[X]$ a PID. Take $f \in F[X]$, $f = g/b$, with $g \in R[X]$, $g = ag'$, $g'$ primitive, then

\[ f = \frac{a}{b}g' = \alpha g' \]

for $\alpha \in F$.

**Lemma 2.5.** Let $p \in R[X]$ be a nonconstant polynomial. Then $p$ is irreducible over $R$ iff $p$ is primitive and irreducible over $F$.

**Proof.** $\Rightarrow$: $C(p) = Ra$, $p = ap'$, where $p'$ is primitive. $p$ irreducible over $R$ implies $a \in R[X]^\times = R^\times$. Then $C(p) = Ra = R$ implies $p$ is primitive. $p = fg$, $f, g \in F[X]$. But $f = af' = \frac{a}{b}f'$, where $f' \in R[X]$ primitive, and $g = bg' = \frac{b}{a}g'$, $g' \in R[X]$ primitive. Then $p = fg = \frac{a}{b}f'g'$. $bd \cdot p = acf'g'$. Then $bdC(p) = C(bdp) = C(acf'g') = acR$. Then $ebd = ac$ for $e \in R$. Then $bdp = ebdf'g'$ so $p = (ef')g'$ over $R$. But $p$ irreducible, so either $f'$ or $g'$ is constant. Thus either $f$ or $g$ is constant in $F^\times$. So $p$ is irreducible over $F$.

$\Leftarrow$: $p = fg$, $f, g \in R[X]$. $p$ irreducible in $F[X]$ implies $f$ or $g$ is a constant polynomial. Suppose $f \in R$. Then $R = C(p) = fC(g)$, so $f \in R^\times$. So $p$ is irreducible in $R[X]$. \hfill \Box

Irreducible polynomials in $R[X]$.

1. Irreducible constants.

2. Primitive polynomials irreducible over $F$. 

3
3 January 10, 2014

Lemma 3.1. Let \( f, g \in R[X] \), \( g \) primitive. If \( g \mid f \) in \( F[X] \), then \( g \mid f \) in \( R[X] \).

Proof. Write \( f = gh \), with \( h \in F[X] \). Write \( h = \frac{g}{h} \) where \( h' \) is primitive. So \( bh = h' \). Then \( bhC(f) = aC(g)h' = aR \) since \( g'h' \) is primitive by Gauss Lemma. So \( a = bh \) for \( c \in R \). Then \( bh = bg \), so \( f = gh' \), where \( ch' \in R[X] \).

Corollary 3.2. Let \( f, g \in R[X] \) be two primitive polynomials. If \( f \sim g \) in \( F[X] \), then \( f \sim g \) in \( R[X] \).

Proof. We have \( g \mid f \) in \( F[X] \). Also, \( f \mid g \) in \( F[X] \). By the lemma, \( g \mid f \) and \( f \mid g \) in \( R[X] \).

Let \( f \in R[X] \) be a primitive polynomial, and \( f = gh \) a nontrivial factorization in \( R[X] \). Then \( \deg(g) < \deg(f) \) and \( \deg(h) < \deg(f) \). If \( g = \text{constant} \), then \( R = C(f) = C(gh) = gC(h) \), which implies \( g \in R^* \), a contradiction.

If \( f \) is not primitive, nonconstant, then \( f = af' \) is a nontrivial factorization with \( a \notin R^* \), and \( f' \) primitive.

Theorem 3.3. If \( R \) is a UFD, then so is \( R[X] \).

Proof. Existence: Take \( f \in R[X] \). Proof by induction on degree \( n = \deg(f) \). Suppose \( n = 0 \), trivial as \( R \) is a UFD. We write \( f = af' \) with \( f' \) primitive, and \( a \in R \). It suffices to factor \( a \) and \( f' \). Since we know how to factor \( a \), we may assume WLOG that \( f \) is primitive. If \( f \) is irreducible, we are done. If not, \( f = gh \) with \( \deg(f) < \deg(g) \), and \( \deg(h) < \deg(f) \). Factor \( g \) and \( h \) by induction.

Uniqueness: \( f = p_1p_2\cdots p_n = q_1q_2\cdots q_m \) with \( p_i, q_j \) all irreducible in \( R[X] \). May assume that \( f \) is nonconstant. So at least one \( p_i \) is nonconstant, say \( p_n \) is nonconstant. But \( p_i, q_j \) primitive and irreducible in \( F[X] \), which is a PID, thus UFD. Thus \( n = m \), So \( \exists \sigma \in S_n \) such that \( q_i \sim p_{\sigma(i)} \) in \( F[X] \). By the corollary, \( q_i \sim p_{\sigma(i)} \) in \( R[X] \).

Corollary 3.4. If \( R \) is a UFD, so is \( R[X_1, \ldots, X_n] \).

Example 3.5. \( 1. \) \( \mathbb{Z}[X_1, \ldots, X_n], \mathbb{F}[X_1, \ldots, X_n] \).

Observe

\[
\text{Fields} \subset \text{ED} \subset \text{PID} \subset \text{UFD}(\mathbb{Z}[X], F[X,Y])
\]

\( R = \mathbb{R}[X,Y]/(X^2 + Y^2 + 1) \) is an example of a PID but not a UFD. Take the matrix

\[
\begin{pmatrix}
-X & Y \\
Y & X
\end{pmatrix}
\]

which is not reducible to the identity, which implies it is not an ED, since a Euclidean function always allows us to do row reduction.

If \( f \in R[X] \), how to factor over \( R \)? Let \( F \) be the quotient field of \( R \). Let \( g \in F[X] \) be a divisor of \( f \). Then \( g' = \alpha g \in R[X] \) primitive for \( \alpha \in F^* \) and \( g' \mid f \) in \( F[X] \). By the lemma, \( g' \mid f \) in \( R[X] \). So \( f = g'h \in R[X] \).

Theorem 3.6. (Eisenstein Criterion) Let \( R \) be a UFD, and \( p \in R \) a prime. Let \( f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in R[X] \) be a polynomial such that

1. \( p \nmid a_n \)
2. \( p \mid a_i \) for \( 0 \leq i \leq n - 1 \).
3. \( p \mid a_0 \) but \( p^2 \nmid a_0 \).

Then \( f \) is irreducible in \( F[X] \).
Proof. Write \( f = cf', \ c \in R \) and \( f' \) primitive. So
\[
f' = a'_nX^n + a'_{n-1}X^{n-1} + \cdots + a'_1X + a'_0
\]
so \( a_i = ca'_i \). But \( p \nmid a_n = ca'_n \), so \( p \nmid c \), and \( p \nmid a'_i \). But \( p \mid a_i \) for \( 0 \leq i \leq n - 1 \), and \( a_i = ca'_i \), so \( p \mid a'_i \). Since \( p^2 \nmid a_0 = ca'_0 \), so \( p^2 \nmid a'_0 \). So \( f \) satisfies the same conditions of the theorem. May assume that \( f \) is primitive.

We prove that \( f \) is irreducible in \( R[X] \). Suppose \( f \) is not irreducible, so \( f = gh, \ g, h \in R[X] \) is a nontrivial factorization, so \( g \) and \( h \) are nonconstant and \( \deg(g), \deg(h) < \deg(f) \). Let \( \overline{R} = R/pR \), for \( pR \) a prime ideal, so \( \overline{R} \) is a domain.

Consider
\[
R[X] \to \overline{R}[X] : f \mapsto \bar{f}
\]
Then
\[
\bar{f} = a_nX^n \neq 0
\]
But \( \deg(g), \deg(h) < n \). So \( \bar{a}_nX^n = \bar{f} = \bar{g}\bar{h} \). This implies \( \bar{g} = \bar{b}X^i \) and \( \bar{h} = \bar{c}X^j \), where \( n = i + j \), and \( 0 < i, j < n \).

Now write \( g = \cdots + e, \) so \( \bar{e} = 0 \), thus \( p \mid e \). Also, \( h = \cdots + s, \) so \( \bar{s} = 0 \), and \( p \mid s \). Then
\[
f = gh = \cdots + es = \cdots + a_0
\]
and \( a_0 = es \) thus \( p^2 \nmid a_0 \), a contradiction. \( \square \)

Example 3.7. 1. \( X^2 - 12 \in \mathbb{Z}[X] \). Take \( p = 3 \).

2. \( XY^3 - Y^3 + X^3Y - XY^2 - X \in \mathbb{Z}[X,Y] \). Take \( R = \mathbb{Z}[X] \), so
\[
f = (X - 1)Y^3 - XY^2 + X^3Y - X
\]
so take \( p = X \). So \( f \) is irreducible in \( \mathbb{Z}(X)[Y] \), and in \( R[Y] = \mathbb{Z}[X,Y] \) since \( f \) is primitive in \( R[Y] \).

3. Take \( p \) prime integer, \( f = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X] \). Write
\[
f = \frac{X^p - 1}{X - 1} = \frac{(X + 1)^p - 1}{Y} = Y^{p-1} + \left( p \right)_{1} Y^{p-2} + \left( p \right)_{2} Y^{p-3} + \cdots + \left( p \right)_{p-1}
\]
but \( p \mid \left( p \right) \) for \( i = 1, \ldots, p - 1 \).

4 Modules

4.1 Definitions

\( R \) a ring, \( A \) is an abelian group and \( A \) is a left \( R \)-module is there is a given map \( R \times A \to A : (r, a) \mapsto ra \).

1. \( x(a + a') = xa + xa' \)
2. \( (x + x')a = xa + xa' \)
3. \( x(x'a) = (xx')a \)
4. \( 1a \equiv a \)

We say \( A \) is a right module if there is given map \( A \times R \to A : (a, r) \mapsto ar \). If \( R \) is commutative, then every left \( R \) module has a structure of a right \( R \)-module by \( ar := ra \).

Example 4.1 (Properties.). 1. \( 0_R \cdot a = 0_A, r \cdot 0_A = 0_A \)

2. \( (-r)a = -(ra) = r(-a) \)

Example 4.2. 1. If \( R \) is a field, then \( R \)-modules are vector spaces over \( R \).
2. If $R = \mathbb{Z}$. If $A$ is an $R$-module, then $1a = a$, $2a = (1 + 1)a = a + a$, $(-1)a = -a$ and $(-2) = -a - a$. Every abelian group admits a unique $\mathbb{Z}$-module structure. So $\mathbb{Z}$-modules are identically abelian groups.

3. Left ideals in $R$ are left $R$-modules.

4. Let $f : R \to S$ be a ring homomorphism and $A$ a left $S$-module. Then $A$ has a left $R$-module structure given by $ra = f(r)a$.

5. A an abelian group, let $R = \text{End}(A)$. Then $A$ is a left $R$-module by $r \cdot a = r(a)$.

If a group $G$ acts on a set $X$, we have a group homomorphism $G \to S(X)$ and conversely. Suppose $A$ is a left $R$-module. If $r \in R$, define $f_r : A \to A : a \mapsto ra$. Thus we get a map $f : R \to \text{End}(A) : r \mapsto f_r$. The remaining properties of a module are equivalent to saying $f$ is a ring homomorphism. Conversely, let $A$ be an abelian group and $f : R \to \text{End}(A)$ a ring homomorphism. Then $A$ is a left $\text{End}(A)$-module, whence $A$ is a left $R$-module.

To give a left module structure on an abelian group $A$ is the same as to give a ring homomorphism from $R \to \text{End}(A)$. If $A$ a right $R$-module structure, is to give $R^\circ \to \text{End}(A)$.

So let $A$ and $B$ be two (left) $R$-modules. A group homomorphism $f : A \to B$ is called an $R$-module homomorphism if $f(ra) = rf(a)$ for all $r$ and $a$. Also, $\text{Hom}_R(A, B)$ is an abelian group.

Then $R\text{-mod}$ is the category of left $R$-modules. Objects are left $R$-modules, and $\text{Mor}(A, B) = \text{Hom}_R(A, B)$.

**Example 4.3.** Fix an abelian group $A$. For any ring $R$, consider diagram

$$R \mapsto \{\text{left $R$-module structures on $A$}\}$$

and

$$S \mapsto \{\text{left $R$-module structures on $A$}\}$$

Then we get a functor $\text{Rings}^o \to \text{Sets}$ with $\alpha_A(R) \cong \text{Hom}_{\text{Rings}}(R, \text{End}(A))$. So $\alpha_A$ is represented by the ring $\text{End}(A)$.

If $R \to S$ is a ring homomorphism, we get a functor $S\text{-mod}$ to $R\text{-mod}$.

Let $A$ be a left $R$-module, and $A$ a subgroup. We say $B \subseteq A$ is a submodule if $rb \in B$ for all $r \in R$, and $b \in B$. Then $B$ is a left $R$-module itself. The intersection of submodules is a submodule. If $\alpha : A \to B$ is a $R$-module homomorphism, then $\ker(\alpha) \subseteq A$, and $\text{im}(\alpha) \subseteq B$.

Let $B \subseteq A$ a submodule, and $A/B$ a factor group. Then $r(a + B) := ra + B$. Then $A/B$ is a module. We the canonical $R$-module homomorphism $\pi : A \to A/B$ which is surjective and $\ker(\pi) = A$.

**Theorem 4.4.** Let $\alpha : A \to B$ be an $R$-module homomorphism. Then

$$A/\ker(\alpha) \cong \text{Im}(\alpha).$$

**Theorem 4.5.** If $A$ and $B$ are $R$-submodules in $M$. Then $(A + B)/B \cong A/(A \cap B)$.

**Theorem 4.6.** If $A \subseteq B \subseteq C$ are $R$-submodules, then

$$\frac{(C/A)/(B/A)}{C/B}$$

Let $M$ be a left $R$-module. Pick $m \in M$, then $Rm = \{rm, r \in R\}$ is the smallest submodule of $M$ containing $m$. If we have a set $\{m_i\}_{i \in I}$, then $\langle m_i \rangle_{i \in I}$, the submodule generated by the $m_i$, is the smallest submodule containing all the $m_i$, is precisely

$$\sum_{i \in I} Rm_i = \{ \sum r_i m_i : r_i \in R \text{ almost all are zero} \}.$$

We say $M$ is finitely generated if there exist $m_1, \ldots, m_s \in M$ such that $M = \langle m_1, \ldots, m_s \rangle$.

Let $\{M_i\}_{i \in I}$ be a family of $R$-modules. To consider products, we must have

$$\text{Hom}_R(N, \prod_{i \in I} M_i) = \prod_{i \in I} \text{Hom}_R(N, M_i)$$
But \( \prod_{i \in I} M_i = \{(m_i)_{i \in I}, m_i \in M_i\} \). And

\[
\text{Hom}_R(\prod_{i \in I} M_i, N) = \prod_{i \in I} \text{Hom}(M_i, N)
\]

WE let \( \prod_{i \in I} M_i = \{(m_i)_{i \in I}, m_i \in M_i\} \) almost all \( m_i \) are zero. Then we may define \( f((m_i)) = \sum f_i(m_i) \in N \). This is the coproduct, the direct sum. Thus \( \prod = \prod \) if \( I \) is finite.

5 January 15, 2014

Let \( R \) be a ring \( \{N_j\}_{j \in J} \) and \( \{M_i\}_{i \in I} \) be familes of \( R \)-modules. Then

\[
f \in \text{Hom}_R\left( \prod_{j \in J} N_j, \prod_{i \in I} M_i \right) = \prod_{i \in I, j \in J} \text{Hom}_R(N_j, M_i).
\]

Then \( f \) is given by a matrix \( f_{ij} \in \text{Hom}_R(N_j, M_i) \). If \( I = \{1, \ldots, n\} \), then

\[
\prod_{I} M_i = M_1 \oplus \cdots \oplus M_n = \prod_{I} M_i.
\]

Let \( M \) be an \( R \)-module, with \( \{M_i\}_{i \in I} \) a family of submodules. We say that \( M \) is an internal direct sum of \( M_i \), \( M = \bigoplus_{I} M_i \) if the natural homomorphism from the external direct sum

\[
\bigoplus_{I} M_i \to M : (m_i)_{i \in I} \mapsto \sum m_i
\]

is an isomorphism. Equivalently, every \( m \in M \) can be uniquely written as

\[
m = \sum m_i, m_i \in M_i
\]

with almost all \( m_i \) zero.

5.1 Exact Sequences

A sequence \( m \xrightarrow{f} N \xrightarrow{g} P \) of homomorphisms of \( R \)-modules is exact if \( \ker(g) = \text{im}(f) \). Short exact sequences are of the form

\[
0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0.
\]

This is exact iff \( f \) is injective, \( \ker(g) = \text{im}(f) \), and \( g \) is surjective.

Category of short exact sequences has objects short exact sequences of \( R \)-modules. The morphisms are if we have

\[
0 \to M \to N \to P \to 0
\]

and

\[
0 \to M' \to N' \to P' \to 0
\]

is a triple \( (\alpha, \beta, \gamma) \) such that \( \alpha : M \to M' \), \( \beta : N \to N' \), and \( \gamma : P \to P' \) make the diagram commute. Then \( (\alpha, \beta, \gamma) \) is an isomorphism iff \( \alpha, \beta, \gamma \) are isomorphisms.

**Example 5.1.** Let \( N \subseteq M \) be a submodule, and then

\[
0 \to N \hookrightarrow M \to M/N \to 0
\]

is a SES.

**Proposition 5.2.** Every SES is isomorphic to the above for some \( N \subseteq M \).
Proof. Take
\[ 0 \rightarrow N \xrightarrow{f} M \xrightarrow{g} P \rightarrow 0 \]
which yields
\[ 0 \rightarrow \text{im}(f) \hookrightarrow M \rightarrow M/\text{im}(f) \rightarrow 0 \]
Then take \( \bar{f} : N \rightarrow \text{im}(f), 1_M : M \rightarrow M \), and by isomorphism theorems, \( P = \text{im}(g) \cong M/\ker(g) = M/\text{im}(f) \) to get an isomorphism from \( P \) to \( M/\text{im}(f) \) making the two sequences isomorphic. \( \square \)

**Example 5.3.** Let \( N \) and \( P \) be \( R \)-modules.
\[ 0 \rightarrow N \rightarrow N \oplus P \rightarrow P \rightarrow 0 \]
where \( n \mapsto (n,0) \), and \( (n,p) \mapsto p \) is the standard split exact sequence. A splitting is a map \( P \rightarrow N \oplus P \) which gives identity on \( P \).

**Proposition 5.4.** Let \( 0 \rightarrow N \xrightarrow{f} M \xrightarrow{g} P \rightarrow 0 \) be a SES. TFAE:

1. There exists \( g' : P \rightarrow M \) such that \( g \circ g' = 1_P \).
2. There exists \( f' : M \rightarrow N \) such that \( f' \circ f = 1_N \).
3. The short exact sequence is isomorphic to the standard SES
\[ 0 \rightarrow N \rightarrow N \oplus P \rightarrow P \rightarrow 0 \]

Proof. (1)–¿ (2) Take \( g' \circ g : M \rightarrow M \). Let
\[ h = 1_m - g' \circ g : M \rightarrow M \]
so
\[ g \circ h = g - g \circ g' \circ g = g - g = 0 \]
So \( h \subseteq \ker(g) = \text{im}(f) \). Then there exists \( f' : M \rightarrow N \) such that \( f \circ f' = h \). Claim that \( f' \circ f = 1_N \). For
\[ f \circ f' \circ f = h \circ f = (1_M - g' \circ g) \circ f = f - g' \circ g \circ f = f = f \circ 1_N \]

For (2)–¿(3) Assuming (2), the morphisms \( 1_N : N \rightarrow N, 1_P : P \rightarrow P \), and \( (f',g) : M \rightarrow N \oplus P \) yield the desired commutative diagram. Then \( (f',g) \) is an isomorphism by five lemma.

(3)–¿(1) Since \( 0 \rightarrow N \rightarrow N \oplus P \rightarrow P \rightarrow 0 \) admits both splitting, so does \( 0 \rightarrow N \xrightarrow{f} M \xrightarrow{g} P \rightarrow 0 \). \( \square \)

**Definition 5.5.** A SES satisfying these three properties is called split.

**Example 5.6.** Let \( R = \mathbb{Z} \). Consider
\[ 0 \rightarrow \mathbb{Z} \xrightarrow{\partial_n} \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 0 \]
is not split if \( n \neq \pm 1 \), since the quotient is torsion, but \( \mathbb{Z} \) is torsion free.

Functors \( F : R \text{-mod} \rightarrow \text{Ab} \). We say that \( F \) is additive if \( F(0) = 0 \) and \( F(g+h) = F(g) + F(h) \). We say \( F \) is a left exact functor if for every SES \( 0 \rightarrow M \rightarrow N \rightarrow P \rightarrow 0 \) in \( R \text{-mod} \), the sequence of abelian groups \( 0 \rightarrow F(M) \rightarrow F(N) \rightarrow F(P) \) is exact. Right exact defined analogously. Then \( F \) is exact if it left and right exact, equivalently, \( F \) takes short exact sequences to short exact sequences.
Example 5.7.  1. If $X \in R$-mod, and $F(M) = \text{Hom}_R(X, M)$. Then $F : R \to \text{Ab}$ is left exact. If

$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$$

then

$$0 \to \text{Hom}_R(X, M) \to \text{Hom}_R(X, N) \to \text{Hom}_R(X, P)$$

is exact. The maps given by $\alpha \to f \circ \alpha$. If $f \circ \alpha = 0$, then $\alpha = 0$ since $f$ is injective. This gives exactness in first term. Suppose $\beta \to g \circ \beta = 0$. Then $\text{Im}(\beta) \subseteq \ker(g) = \text{im}(f)$. So there exists $\gamma : X \to M$ such that $f \circ \gamma = \beta$. So $\ker(g^*) \subseteq \text{Im}(f^*)$.

If $f^*$ and $g^*$ are the new maps between hom spaces,

$$g^*(f^*(\alpha)) = g \circ f \circ \alpha = 0 \implies \text{Im}(f^*) \subseteq \ker(g^*)$$

If the original SES above is not split, the $X = P$, then $1_N$ from $\text{Hom}_R(X, P)$ is not in $\text{im}(g^*)$.

2. $Y \in R$-mod. Then $F(M) = \text{Hom}_R(M, X)$ for $F : R$-mod $\to \text{Ab}$ is left exact. Given

$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$$

, get

$$0 \to \text{Hom}(P, Y) \xrightarrow{g^*} \text{Hom}(N, Y) \xrightarrow{f^*} \text{Hom}(N, X)$$

is exact.

6 Free Modules

Let $R$ be a ring, $M$ a left $R$-module. A subset $X \subseteq M$ is called a basis for $M$ if every element $m \in M$ can be uniquely written in form

$$m = \sum_{x \in X} r_x x$$

with $r_x \in R$, almost all zero. We say $M$ is free if $M$ has a basis.

Example 6.1.  1. If $R$ is a field, every $R$-module is free.

2. $R^n$ is free with $\{e_i\}$ the standard basis.

3. $X$ a set, let $R^{(X)} = \{f : X \to R : f(x) = 0$ for almost all $x \in X\}$. Then $R^{(X)}$ is a free $R$-module with basis given by $x \in X$ and $f_x \in R^{(X)}$ with

$$f_x(x') = \begin{cases} 1 & x' = x \\ 0 & x' \neq x. \end{cases}$$

Then for all $g \in R^{(X)}$, $g = \sum_{x \in X} g(x) \cdot f_x$. Then $\{f_x\}$ is a basis for $R^{(X)}$, $\{f_x\} \leftrightarrow X$. So if $X = \{1, \ldots, n\}$, $R^{(X)} \cong R^n$.

Proposition 6.2. Let $M$ be a free left $R$-module with basis $X$. Then $M$ is isomorphic to $R^{(X)}$.

Proof. Let $R^{(X)} \to M : g \mapsto \sum_{x \in X} g(x) \cdot x$ is an isomorphism of $R$-modules. \hfill $\Box$

So $R^{(X)} \cong \prod_{x \in X} R$ and $R \cong R^1$. There is a ring $R \neq 0$ such that $R \cong R^2$.

Theorem 6.3. Let $M$ be a free left $R$-module with basis $X$. Then for any left module $N$, every map $X \to N$ extends uniquely to an $R$-module homomorphism $M \to N$. 


Proof. Let \( f : X \to N \). We look for \( g : M \to N \) such that \( g|_X = f \). If it exists,
\[
g \left( \sum_{x \in X} r_x x \right) = \sum r_x g(x) = \sum r_x f(x)
\]

Then forgetful funtor \( R\text{-mod} \) to \( \text{Sets} \) and the functor from \( \text{Sets} \) to \( R\text{-mod} \) sending \( X \) to \( R(X) \) is left adjoint to forgetful funtor. So
\[
\text{Map}(X, N) \simeq \text{Hom}_R(R(X), N)
\]
and \( M \simeq R(X) \).

Example 6.4. Let \( R = \mathbb{Z} \). Then \( \mathbb{Z}^{(X)} \simeq \bigsqcup_{x \in X} \mathbb{Z} \) has non nontrivial torsion elements. If \( A \) is an abelian group, and \( A_{\text{tors}} \neq 0 \), then \( A \) is not free \( \mathbb{Z} \)-module. The free object in the category of abelian groups is \( \mathbb{Z}^{(X)} \).

Let \( M \) be a left \( R \)-module, \( I \subset R \) an ideal. Let \( \bar{R} = R/I \). Then \( IR \) is the submodule of \( M \) generated by products \( rm \) with \( r \in I \), and \( m \in M \). Then can form factor modules \( \bar{M} = M/IR \). In fact, \( \bar{M} \) has a structure of an \( \bar{R} \)-module. Define \( \bar{r} \cdot \bar{m} = \bar{rm} \). If \( M \) is free, with basis \( X \), then \( \bar{M} \) is a free \( \bar{R} \)-module with basis \( \bar{X} \) the image of \( X \) under \( M \to \bar{M} \). Moreover, \( X \) and \( \bar{X} \) are in bijection.

If there is a surjective ring homomorphism from \( R \to D \) a nonzero division ring, then \( \text{card}(X) \) is independent of \( X \).

7 Projective and Injective Modules

Proposition 7.1. Let \( R \) be a ring, and \( P \) a left \( R \)-module. TFAE

1. The functor \( \text{Hom}_R(P, -) \) is exact.

2. For every surjection \( g : M \to N \), and every \( f : P \to N \), there exists \( h : P \to M \) such that \( f = gh \).

3. Every short exact sequence \( 0 \to M \to N \to P \to 0 \) is split.

Proof. We already have seen 1 and 2 are equivalent. To see 2-\( \Rightarrow \)3, follows by setting \( f = 1_P \) to yield a splitting. For 3-\( \Rightarrow \)2, refer to notes.

A left \( R \)-module \( P \) satisfying these conditions is called projective.

Example 7.2. Every free module is projective. Let \( P \) be free. Write \( P \simeq R^{(X)} \), use universal properties.

8 January 22, 2014

Theorem 8.1. An \( R \)-module \( P \) is projective iff \( P \) is a direct summand of a free module, \( P \oplus P' \) is free for some \( R \)-module \( P' \).

Proof. Suppose \( P \) is free. Every module is a factor module of a free module. If \( M \) is an \( R \)-module, pick \( X \subset M \) a generating set, then \( f : R^{(X)} \to M \) given by
\[
f \left( \sum_{x \in X} r_x x \right) = \sum r_x x \in M
\]
which is surjective since \( X \) is a generating set.
$P$ is a factor module of a free $R$-module $F$. Let $N = \ker(f)$, which gives
$$0 \to N \to F \xrightarrow{f} P \to 0$$
And since $P$ is projective, the sequence is split, so there exists $g: P \to F$ such that $gf = 1_p$. Thus $F \simeq P \oplus N$.

Conversely, write $F = P \oplus P'$ free. Consider the functor $M \mapsto \text{Hom}_R(P,M)$ from $R$-mod to $\text{Ab}$. This functor is exact since $F$ is free. But $\text{Hom}_R(F,M) = \text{Hom}_R(R,M) \oplus \text{Hom}_R(P',M)$. Then $\text{Hom}_R(P,M)$ is exact, so $P$ is projective.

Example 8.2. Let $R = R_1 \times R_2$, with $R_1$ a left $R$-module by $(x_1,x_2)r_1 = x_1r_1$, likewise $R_2$ is an $R$-module. Then $R_1 \oplus R_2 \simeq R$ as $R$-module, since $R$ is free, $R_1$ and $R_2$ are projective.

Example 8.3. Take $R$ a domain, and let $I$ be an ideal nonzero. So $I$ is an $R$-module. Claim that $I$ is free iff $I$ is principal. If $X \subset I$ is a basis, then $|X| = 1$, so $I = \langle a \rangle$ for some $a$.

Conversely, if $I = \langle a \rangle$ is principal, then $a$ is a basis, so $I$ is free.

If $I$ is projective, but not principal, then $I$ is not free.

Proposition 8.4. Let $Q$ be an $R$-module. TFAE

1. The functor $R \dashrightarrow \text{mod}^\oplus$ to $\text{Ab}$ taking $M \to \text{Hom}_R(M,Q)$ is exact.
2. For a diagram $0 \to X \to Y$, and for any $X \to Q$, there exists an extension $Y \to Q$.
3. Every SES $0 \to Q \to M \to N \to O$ is split

An $R$-module satisfying those conditions is called injective.

Example 8.5. Let $R = \mathbb{Z}$. Every projective $\mathbb{Z}$-module is free. Injective $\mathbb{Z}$-modules are exactly divisible groups.

We say $Q$ is divisible if $nQ = Q$ for every nonzero $n \in \mathbb{Z}$. Equivalently, for all $x \in Q$, and all nonzero $n \in \mathbb{Z}$, there exists $y \in Q$ such that $x = ny$. Some examples are $Q, Q/\mathbb{Z} = \coprod_p Q_p/\mathbb{Z}_p$.

8.1 Modules over a PID

$\mathbb{Z}$ and $F[X]$ will be of interest. Let $R$ be a domain, and $M$ an $R$-module. An element $m \in M$ is called a torsion element if there exists nonzero $r \in R$ such that $rm = 0$.

Write $M_{tor}$ to be the subset of all torsion elements in $M$. It is a submodule, as clearly $0 \in M_{tor}$. If $m_1,m_2 \in M_{tor}$, then there exist $r_1,r_2$ nonzero such that $r_1m_1 = r_2m_2 = 0$. Then $r_1r_2 \neq 0$, and $(r_1r_2)(m_1 + m_2) = 0$. Closure under multiplication obvious.

We say $M$ is torsion free if $M_{tor} = 0$.

Proposition 8.6. $M/M_{tor}$ is torsion free.

Proof. Suppose $m + M_{tor}$ is torsion, so there exists $r \neq 0$ such that $rm + M_{tor} = M_{tor}$, so $rm \in M_{tor}$, so there exists $r'$ such that $r'rm = 0$, so $r'r \neq 0$, thus $m \in M_{tor}$.

So
$$0 \to M_{tor} \to M \to M/M_{tor} \to 0$$
is a SES.

Example 8.7. Free modules are torsion free. Conversely, suppose $I \subset R$ an ideal, and $I$ is torsion free. Then $I$ is free iff $I$ is principal. So the converse is not true if $R$ is not a PID.

If $F$ is free with basis $X$, then rank($F$) = $|X|$. So $F$ is finitely generated iff rank($F$) < $\infty$.

Proposition 8.8. Let $R$ be a PID, and $F$ a finitely generated free $R$-module, $N \subset F$ a submodule. Then $N$ is free and rank($N$) $\leq$ rank($F$). So $N$ is finitely generated.
Proof. Induction on rank(F) = n. If n = 0, F = 0 so N = 0 and N is free of rank 0. Let x₁...,xₙ be a basis of F. Define

\[ f : F \to R : f(\sum r_i x_i) = r_n \]

Then f(N) = I ⊂ R is an ideal. Then F' = ker(f) is free with basis x₁,...,xₙ₋₁. So rank(F') = n − 1.

Consider 0 → F' ∩ N → F/(I∩N) → 0 and ker(f|N) = ker(f) ∩ N = F' ∩ N. And F' ∩ N is a submodule of F', free of rank n − 1. By induction F' ∩ N is free of rank n − 1. Since R is a PID, I is principal, hence free of rank ≤ 1. Thus I is projective, so the sequence is split so N ∼ (F' ∩ N) ⊕ I, hence free. And

\[ \text{rank}(N) = \text{rank}(F' ∩ N) + \text{rank}(I) ≤ (n - 1) + 1 = n. \]

The proposition still holds even for free F of infinite rank. \( \mathbb{Q} \) is a torsion free \( \mathbb{Z} \)-module, but not free.

9 January 2014

Let R be a domain, and F the quotient field. So F = S⁻¹R where S = R \ {0}. If M an R-module,

\[ S⁻¹M = \{ m/s : m ∈ M, s ∈ S \} \]

and we see m/s = m'/s' ⇔ \( \exists t ∈ S \) (ms' − m's) = 0. Then S⁻¹M is an S⁻¹R-module. If R a domain S⁻¹R = F ⊃ R, and S⁻¹M is a vector space over F. Then there is natural map

\[ f : M → S⁻¹M : m ↦ m \frac{1}{1} \]

is a homomorphism of R-modules.

Then ker(f) = \{ m ∈ M : m/1 = 0 in S⁻¹M \} = M_{tors}. Then f is injective ⇔ M is torsion free.

Now suppose M torsion free and finitely generated R-module. Let dim(S⁻¹M) < ∞. Let \{x₁,...,xₙ\} be a basis for S⁻¹M.

Let F be the \( R \)-submodule of S⁻¹M generated by x₁, x₂,...,xₙ. So

\[ P = \{ \sum a_i x_i : a_i ∈ R \} ⊂ S⁻¹M \]

So \{x₁,x₂,...,xₙ\} is a basis of P as an R-module. Thus P is free R-module of finite rank. Let \{m₁,m₂,...,m_k\} generated M as R-module. So

\[ m_i = \sum_{j=1}^{i} a_{ij} x_j, a_{ij} ∈ F \]

There exists \( c ∈ R \) nonzero such that ca_{ij} ∈ R for all i,j. Then cm_i ∈ P for all i. Thus cM ⊂ P. Then M \overset{c}{\to} cM is clearly surjective, and injective since M has no torsion, thus an isomorphism. So M ∼ cM ⊂ P. So every finitely generated torsion free module over a domain is isomorphic to a submodule of a free module.

**Proposition 9.1.** Every torsion free finitely-generated R-module is isomorphic to a submodule of a free module of finite rank, where R is a domain.

**Corollary 9.2.** Every torsion free finitely generated module over a PID is free of finite rank.

Note \( \mathbb{Q} \) is torsion free but not free over \( \mathbb{Z} \).

Now let R be a PID, and M a finitely-generated R-module. We have an exact sequence

\[ 0 → M_{tors} → M → M/M_{tors} → 0 \]

where the last term is torsion free and finitely generated. Hence free, thus projective. Thus the sequence splits. So M ∼ M_{tors} ⊕ M/M_{tors}, thus the direct sum of a torsion module and a free module of finite rank. Let P = M/M_{tors}. So

\[ \text{rank}(P) = \text{rank}(M/M_{tors}) = \dim_F(S⁻¹(M/M_{tors})) = \dim_F(S⁻¹M) \]
Let $M$ be torsion and finitely generated over a PID $R$. There exists $c \in R$ nonzero such that $cM = 0$. Let $0 \neq P \subset R$ be a prime ideal. Then $P = Rp$ for some prime $p$, where $p$ is unique up to associate.

Define 

$$M(P) = \{ m \in M : p^n m = 0 \text{ for some } n > 0 \}$$

which is a $R$-submodule of $M$, the $p$-primary part of $M$.

**Lemma 9.3.** Let $a_1, a_2, \ldots, a_n \in R$ be relatively prime elements (no common prime divisor). Then there exist $b_1, \ldots, b_n$ such that $\sum a_ib_i = 1$.

**Proof.** Let $I = \sum a_i R \subset R$ and ideal. Let $I = cR$, and $c \mid a_i$, so $c \in R^\times$. Thus $I = R$. So $1 \in \sum a_i R$ thus $1 = \sum a_ib_i$.

If $R = F[x, y]$, let $a_1 = X$ and $a_2 = Y$, these are relatively prime, but 1 is not in the generated ideal.

**Corollary 9.4.** Let $M$ be an $R$-module, $a_1, \ldots, a_n \in R$ relatively prime, $m \in M : a_im = 0$ for all $i$. So $m = 0$.

**Proof.** Find $b_i \in R : \sum a_ib_i = 1$. Then

$$m = \sum a_ib_im = \sum b_ia_im = 0$$

**Corollary 9.5.** Let $M$ be a finitely generated $R$-module. Then $M(P) = 0$ for almost all prime ideals $P$.

**Proof.** Suppose $M(P) \neq 0$, pick $m \in M(P)$ nonzero. Then $p^n \cdot m = 0$, and $Rp = R$. But $cM = 0$ for some nonzero $c$. Then $cm = 0$, but $m \neq 0$, so by the previous corollary, $p^n$ and $c$ are not coprime, so $p \mid c$. Then $M(P) \neq 0$ implies $p$ is a prime divisor of $c$, so there are finitely many such $P$.

**Theorem 9.6.** (Primary Decomposition) Let $M$ be a finitely generated $R$-module over a PID. Then $M = \prod_{P \subset R} M(P)$.

**Proof.** Choose $c$ so $cM = 0$, with $c \neq 0$. Write $c = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$ with $u$ a unit, and $p_i$ nonassociate primes. So $Rp_i \neq Rp_j$. Consider $a_i = \frac{1}{p_i^{\alpha_i}}$, so that $a_1, a_2, \ldots, a_n$ are relatively prime. By Lemma, there exists $b_1, \ldots, b_n$ such that $\sum a_ib_i = 1$. Pick $m \in M$, then

$$m = \sum a_ib_im = \sum b_i(a_im_i)$$

which implies

$$p_i^{\alpha_i}a_i = c \implies p_i^{\alpha_i}(a_im) = cm = 0$$

so $a_im \in M(P_i)$ and $P_i = Rp_i$.

So $M = \sum M(P_i)$, and $m_1 + m_2 + \cdots + m_n = 0$, where $m_i \in M(P_i)$. Want to show this implies $m_i = 0$ for all $i$. If $P_i = Rp_i$, then $p_j^{\alpha_j}m_j = 0$, and $a_i = \prod_{j \neq i} p_j^{\beta_j}$, and $a_im_j = 0$ for $j \neq i$ as $p_j^{\beta_j} \mid a_i$. Then

$$a_i(m_1 + m_2 + \cdots + m_n) = 0 \implies a_im_i = 0$$

Then $a_im_i = 0$ and $p_i^{\alpha_i}m_i = 0$, but $a_i, p_i^{\alpha_i}$ are relatively prime. By the Corollary, $m_i = 0$.

Let $P \subset R$ be a prime ideal, and $M$ and $R$-module. We say that $M$ is $P$-primary if $M = M(P)$. If $P = Rp$, and if $M$ is finitely generated, $M$ is $P$-primary iff $p^nM = 0$ for some $n > 0$. 


Definition 10.1. If $R$ a ring, a left $R$-module $M$ is cyclic if $M$ is generated by one element.

If $m \in M$ a generator, and $f: R \to M$ with $f(r) = rm$, then $f$ is an epimorphism. Then

$$M \simeq R/I = R/\ker(f)$$

and $\ker(f)$ an ideal in $R$. If $I = 0$, then $M \simeq R$ is free.

Now let $R$ be a PID, take $p \in R$ prime. Consider $R/p^n R$, a $p$-primary cyclic module, note we can write $R/pR$ for a general cyclic module.

Now let $M$ be a left $R$-module, and $I \subseteq R$ be a two sided ideal such that $IM = 0$. Then $M$ has a structure of a left $R/I$-module by $(r + I)m = rm$. If $M$ a left $R$-module, then $IM$ is the submodule of $M$ generated by $rm$ for $r \in I$, and $m \in M$. Then $I(M/IM) = 0$, so $M/IM$ is an $R/I$-module for any $M$.

Let $R$ be a PID, $p \in R$ prime. Then $k = R/pR$ is the residue field at $p$. Let $M$ be an $R$-module, so $M/pM$ is a $k$ vector space, and $p^nM/p^{n+1}M$ is also a $k$-vector space, and

$$pM = \{m \in M : pm = 0\} = \ker(M \to pM).$$

Then $p(M) = 0 \iff pM$ a $k$-vector space.

Lemma 10.2. Let $R$ be a PID, fix a prime $p \in R$. Let $M$ be a $R$-module such that $p^nM = 0$, but $p^{n-1}M \neq 0$, and $\dim_k(pM) = 1$. Then $M \simeq R/p^nR$.

Proof. Choose $m \in M$ such that $p^{n-1}m \neq 0$. I claim that if $rm = 0$, then $p^n | r$. Write $r = ap^k$ where $(a,p) = 1$. Then we want to show $k \geq n$. Suppose not, so $k < n$. Then $rm = 0$ implies $a(p^k m) = 0$, so $p^n m = p^{n-k}(p^k m) = 0$. But $(a,p^{n-k}) = 1$, so $p^k m = 0$, but $p^{n-1}m \neq 0$, so $k \geq n$, a contradiction.

If $f: R \to M$ and $f(r) = rm$, then $\ker(f) = \{r \in R : rm = 0\} = p^n R$ by the claim. So $f$ factors as $\tilde{f}: R/p^n R \to M$. We show that $f$ is surjective. We pick $x \in M$ and pick $k$ least such that $p^k x = 0$. By induction on $k$, $k = 1, \ldots, n$, we show that $x \in \text{im}(f)$.

If $k = 1$, $px = 0$, and $x \in_p M$, then $p(p^{n-1}m) = 0$, but $0 \neq p^{n-1}m \in_p M$, so since $\dim_k(pM) = 1$, we have $p^{n-1}m$ is a basis for $pM$. So

$$x = rp^{n-1}m = f(rp^{n-1}) \in \text{im}(f).$$

For the induction step, $p^k x = 0$, and $p^{k-1}(px) = 0$, by induction, $px \in \text{im}(f)$ and $px = f(r) = rm$. Then $0 = p^n x = p^{n-1}rm$, and now apply the claim, which implies $p^n | p^{n-1}r$, so $p | r$, and thus $r = pa$ for $a \in R$. Then $px = rm = pam$, or $p(x - am) = 0$, so $x - am \in_p M$, so $x - am \in \text{im}(f)$, but $am \in \text{im}(f)$, so $x \in \text{im}(f)$ as well.

So $m$ generates $M$. \hfill \Box

Suppose $M$ is a finitely generated $R$-module, and $p^n M = 0$. Then

$$M \supset pM \supset p^2M \supset \cdots \supset p^nM = 0$$

so we may looks at $p^iM/p^{i+1}M$ is a $k$-vector space. Since the module is finitely generated, this is a finite dimensional vector space. Then $\ell(M)$, the length of $M$ is

$$\ell(M) = \sum_{i=0}^{n-1} \dim_k(p^iM/p^{i+1}M).$$

So every finitely generated module has finite length.

We have the following properties:

1. $\ell(M \oplus N) = \ell(M) + \ell(N)$
2. We have the filtrations

\[ R/p^nR \supset pR/p^nR \supset p^2R/p^nR \supset \cdots \]

and

\[ (p^iR/p^nR)/(p^{i+1}/p^nR) \simeq p^iR/p^{i+1}R \simeq R/pR = k \]

so \( \ell(R/p^nR) = n \).

3. Let \( f : M \to \tilde{M} \) be a surjective \( R \)-module homomorphism, such that \( \ker(f) \neq 0 \). Then \( \ell(\tilde{M}) < \ell(M) \).

**Proof.** We have \( f_i : p^iM/p^{i+1}M \to p^i\tilde{M}/p^{i+1}\tilde{M} \). Let \( N = \ker(f) \neq 0 \). Then there exists unique \( i \) such that

\[ N \subset p^iM \]

but \( N \not\subset p^{i+1}M \). Then \( \ker(f_i) \neq 0 \). \( \square \)

**Proposition 10.3.** Let \( M \) be a finitely generated \( R \)-module such that \( p^nM = 0 \) but \( p^n-1M \neq 0 \). Then there is a surjective \( R \)-module homomorphism \( M \to R/p^nR \).

**Proof.** Induction on \( \ell(M) \). Since \( \dim_k(\varphi, M) \geq 1 \), since \( pM \neq 0 \). If \( \dim(\varphi, M) = 1 \), then by Key Lemma, \( M \simeq R/p^nR \). Suppose that \( \dim(\varphi, M) > 1 \). Choose \( m \in M \) such that \( p^n-1m \neq 0 \), and \( p^n-1m \in_p M \).

This is not a basis, so there exists \( x \in M \) such that \( p^n-1m \) and \( x \) are linearly independent. Then let \( N = (x) \subset M \), which is nonzero since \( x \neq 0 \). Also, \( p^n-1m \notin N \). Let \( \tilde{M} = M/N \). Then \( \ell(\tilde{M}) < \ell(M) \), so \( p^n-1m \in \tilde{M} \neq 0 \) in \( \tilde{M} \). So \( p^n-1M \neq 0 \), but \( p^nM = 0 \). By induction applied to \( \tilde{M} \), there exists a surjective \( R \)-module homomorphism \( \tilde{M} \to R/p^nR \). Take

\[ M \to \tilde{M} \to R/p^nR \]

which is surjective. \( \square \)

**Theorem 10.4.** Let \( R \) be a PID, \( p \in R \) prime, \( M \) a finitely generated, \( p \)-primary \( R \)-module. Then \( M \) is a direct sum of cyclic \( p \)-primary modules, (of form \( R/p^nR \)).

**Proof.** There exists \( n \) such that \( p^nM = 0 \) but \( p^n-1M \neq 0 \). By proposition, there exists a surjective homomorphism \( M \to R/p^nR \), which is a homomorphism of \( R/p^nR \) modules as well, but \( R/p^nR \) is free \( R/p^nR \)-module, so \( f \) is split, and thus \( M \simeq N \oplus R/p^nR \). We conclude by induction on \( \ell(M) \), since \( \ell(N) < \ell(M) \). \( \square \)

**Theorem 10.5.** Let \( R \) be a PID, \( M \) a finitely generated \( R \)-module. Then \( M \) is a direct sum of cyclic modules of the form \( R \) or \( R/p^nR \), where \( p \) is prime.

### 11 January 29, 2014

Suppose \( M \) is a finitely generated torsion \( R \)-module. So \( M \) is a direct sum of modules of form \( R/p^nR \) where \( p \) is prime. Let \( N = R/p^nR \), so

\[ p^{k-1}N/p^kN = \begin{cases} R/pR & k \leq n, \\ 0 & k > n. \end{cases} \]

If \( N = R/q^nR \), and \( p^{k-1}N/p^kN = 0 \), if \( q \not\equiv p \), then \( pR = qR \), and \( pR + qR = R \), \( p^kN = N \).

Let \( \ell_k = \dim_k(p^{k-1}M/p^kM) \), which is the number of \( p \)-primary cyclic summands in \( M \) of form \( R/p^nR \) with \( n \geq k \). So \( \ell_n - \ell_{n-1} \) is the number of cyclic summands in \( M \) isomorphic to \( R/p^nR \), so this is independent of the decomposition.

Recall that if \( M \) is a f.g. \( R \)-module, and \( M = M' \oplus F \) where \( M' \) is torsion, and \( F \) is free. We know \( \text{rank}(F) = \dim_F(S^{-1}M) \), and \( S = R \setminus \{0\} \), and \( F = S^{-1}R \), and \( M' \) is a direct sum of primary cyclic modules.

We have cyclic modules

\[ R/P_1^{\alpha_1}, R/P_1^{\alpha_1+\alpha_2}, \ldots, R/P_1^{\alpha_1+\cdots} \]
with \( \alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_{r_1} \) down to
\[
R/P_1^{\alpha_{k_1}} \oplus R/P_1^{\alpha_{k_2}} \oplus \cdots \oplus R/P_1^{\alpha_{k_{r_1}}}
\]
where the \( p_1, p_2, \ldots \) are distinct primes. The \( \{P_i^{\alpha_i}\} \) are the elementary divisors of \( M \) (or of \( M' = M_{\text{tors}} \)).

**Theorem 11.1.** Let \( M \) and \( M' \) be f.g. \( R \)-modules. Then \( M \simeq M' \) iff \( \text{rank}(M) = \text{rank}(M') \) and the same elementary divisors.

Recall the CRT, that if \( I_1, I_2, \ldots, I_k \subset R \) are pairwise coprime ideals, then
\[
R/I_1 \oplus \cdots \oplus R/I_k = R/I_1 I_2 \cdots I_k
\]
so we may combine the elementary divisors of distinct primes. So
\[
M_{\text{tors}} \simeq R/a_1 R \oplus R/a_2 R \oplus \cdots \oplus R/a_s R
\]
where \( a_r | a_{r-1} | \cdots | a_1 \) so that \( a_r R \supset a_{r-1} R \supset \cdots \supset a_1 R \).

Then the multiset \( \{a_r R, \ldots, a_1 R\} \) are the invariant factors of \( M \).

**Theorem 11.2.** Let \( M \) and \( M' \) be a finitely generated module. Then \( M \simeq M' \) iff \( \text{rank}(M) = \text{rank}(M') \) and \( M \) and \( M' \) have the same invariant factors.

**Example 11.3.** Let \( R = \mathbb{Z} \), and consider \( M = \mathbb{Z}/(12) \oplus \mathbb{Z}/(90) \) and \( M' = \mathbb{Z}/(36) \oplus \mathbb{Z}/(30) \). Note that
\[
\text{ED}(M) = \{(3), (4), (2), (5), (9)\}
\]
and
\[
\text{ED}(M') = \{(4), (9), (2), (3), (5)\}
\]
so \( M \simeq M' \). Also, the invariant factors are \( (4)(5)(9) = (180) \) and \( (2)(3) = (6) \). So
\[
M \simeq M' \simeq \mathbb{Z}/(6) \oplus \mathbb{Z}/(180)
\]
so the invariant factors are \( (6) \) and \( (180) \).

Let \( M \) be a f.g. \( R \)-module. How to find \( \text{IF}(M) \)? Find a surjection \( f: F \rightarrow M \) where \( F \) is free of rank \( n \), and let \( N = \ker(f) \), so that \( M \simeq F/N \). Choose \( \{x_1, \ldots, x_n\} \) to be a basis for \( F \) and \( \{y_1, \ldots, y_m\} \) generate \( N \). Then
\[
y_1 = a_{11} x_1 + \cdots + a_{n1} x_n
\]
up to
\[
y_n = a_{1n} x_1 + \cdots + a_{nm} x_m
\]
with \( a_{ij} \in R \). So write
\[
A = \begin{pmatrix}
     a_{11} & a_{12} & \cdots & a_{1m} \\
     a_{21} & a_{22} & \cdots & a_{2m} \\
     \vdots  & \vdots & \ddots & \vdots \\
     a_{m1} & a_{m2} & \cdots & a_{nn}
\end{pmatrix}
\]
Suppose \( A = \text{diag}(r_1, r_2, \ldots, r_s) \). Assume \( r_1 | r_2 | \cdots | r_s \). If \( y_i = r_i x_i \) for \( 1 \leq i \leq p \), where \( r_p \neq 0 \), but \( r_{p+1} = \cdots = r_s = 0 \). Then
\[
F = Rx_1 \oplus \cdots \oplus Rx_n
\]
Then \( N = Rr_1 x_1 \oplus Rr_2 x_2 \oplus \cdots \oplus Rr_p x_p \) and
\[
M \simeq F/N \simeq R/Rr_1 \oplus \cdots \oplus R/Rr_p \oplus R^{n-p}
\]
so that \( \text{rank}(M) = n - p \), and \( \text{IF}(M) = (R r_1, \ldots, R r_p) \) with \( R r_i = R \) deleted.
11.1 Elementary Transformations

1. You can interchange any number of rows or columns. This only changes names of basis vectors, but not the module.

2. Add to a row (column) a multiple of another row (column).

3. Can multiply a row (column) by \( a \in R^\times \).

Assume \( R \) is a Euclidean domain.

Example 11.4. Find ED and IF of \( \mathbb{Z}^2/\langle(4,2),(2,4)\rangle \). Then

\[
A = \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix}
\]

Get

\[
\begin{pmatrix} 2 & 4 \\ 4 & 2 \end{pmatrix}
\]

Get

\[
\begin{pmatrix} 2 & 4 \\ 0 & -6 \end{pmatrix}
\]

Get

\[
\begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}
\]

So IF(M) = \{\langle 2, 6 \rangle\} and ED(M) = \{\langle 2 \rangle, \langle 2 \rangle, \langle 3 \rangle\}. So

\[
M \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(6) \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(3).
\]

12 January 31, 2014

12.1 Abelian Groups

Let \( R = \mathbb{Z} \). We know \( p\mathbb{Z} \) is prime if \( p \) is prime.

**Theorem 12.1.** (ED Form) Every finitely generated abelian group is isomorphic to the direct sum of cyclic groups \( \mathbb{Z} \) and \( \mathbb{Z}/p^n\mathbb{Z} \) for \( p \) prime.

**Theorem 12.2.** (IF Form) Every finitely generated abelian group is isomorphic to

\[
\mathbb{Z}^k \oplus \mathbb{Z}/(a_1) \oplus \mathbb{Z}/(a_2) \oplus \cdots \oplus \mathbb{Z}/(a_s)
\]

with \( a_1 | a_2 | \cdots | a_s \). Two modules are isomorphic if and only if they have the same rank and invariant factors.

12.2 Rational Canonical Form

Let \( F \) be a field, and \( R = F[X] \). Let \( M \) be an \( R \)-module, and \( F \subset R \) a subring, so \( M \) is an \( F \)-module, hence a vector space over \( F \). Consider \( S: M \to R \) where \( S(m) = X \cdot m \). If \( \alpha \in F \), then \( S(\alpha m) = X(\alpha m) = \alpha X(m) = \alpha S(m) \) and \( S(m_1 + m_2) = X(m_1 + m_2) = Xm_1 + Xm_2 = S(m_1) + S(m_2) \), so \( S \) is a linear operator in the vector space \( M \).

If \( V \) is a vector space over \( F \), then \( S: V \to V \) is a linear operator. Then \( V \) has an \( R \)-module structure. If \( f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \), then

\[
f \cdot v = a_nS^n(v) + \cdots + a_1S(v) + a_0v.
\]

So to give an \( R \)-module is equivalent to giving a vector space with a linear operator. So if \( M \leftrightarrow (V, S) \) and \( N \leftrightarrow (W, T) \), then \( M \oplus N \leftrightarrow (V \oplus W, S \oplus T) \) where \( (S \oplus T)(v, w) = (S(v), T(w)) \).

If \( f: M \to N \) is a \( R \)-module homomorphism, and \( g: V \to W \) a linear map. Then \( g \circ S = T \circ g \).
Example 12.3. Let \( V = F^n \), and let \( A : F^n \to F^n \), so \( A(X) = AX \). Then \((F^n, A)\) is a vector space with a linear operator, thus gives an \( R\)-module. Given \((F^n, B)\), when are

\[
(F^n, A) \simeq (F^n, B)
\]
as \( R\)-modules? If there exists \( C \in GL_n(F) \) such that \( CA = BC \). Equivalently, there exists \( C \) invertible such that \( B = CAC^{-1} \). We say that \( A \) and \( B \) are similar, \( A \sim B \).

Suppose \( S : V \to V \) is a linear operator, \( B = \{ v_1, \ldots, v_n \} \) is a basis for \( V \). So

\[
S(v_1) = \alpha_1 v_1 + \cdots + \alpha_n v_n
\]
up to

\[
S(v_n) = \alpha_1 v_1 + \cdots + \alpha_n v_n
\]
This induces a matrix \( A = (\alpha_{ij})^T \).

Then \( \text{End}_F(V) \simeq M_n(F) \) are isomorphic as algebras by \( S \leftrightarrow [S]_B \).

Let \( M = R/fR \) with \( f \in R = F[X] \) nonzero a cyclic \( R\)-module. So choose \( f \) monic, and

\[
f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0.
\]
If \( g \in R \), and \( \bar{g} = g + fR \in M \), then \( 0 = \bar{f} = \overline{X^n} + a_{n-1} \overline{X^{n-1}} + \cdots a_1 X + a_0 1 \). So \( M \) is spanned by \( \{1, X, \ldots, X^n\} \), and they form a basis of \( M \). They are linearly dependent, else one gets a polynomial of degree less than that of \( f \), divisible by \( f \), a contradiction. So \( \dim_F(M) = n \). Denote this basis \( B \), and let \( S \) be \( S(m) = X \cdot m \). We compute \([S]_B\), then

\[
\begin{pmatrix}
0 & 0 & \cdots & 0 & -a_0 \\
1 & 0 & \cdots & \vdots & -a_1 \\
0 & 1 & \ddots & \vdots & \\
\vdots & \vdots & \ddots & \vdots & -a_{n-1} \\
0 & 0 & \cdots & 1 & -a_{n-1}
\end{pmatrix}
\]
which is the companion matrix.

Theorem 12.4. (ED for operators) Let \( S : V \to V \) be an operator in a finite dimensional vector space \( V \). Then there is a basis \( B \) for \( V \) such that

\[
[S]_B \text{diag}(C(f_1), C(f_2), \ldots, C(f_k))
\]
where \( f_i = p_i^{m_i} \) where \( p_i \) is a monic irreducible. So \( f_1, \ldots, f_k \) are unique up to permutation.

Theorem 12.5. (IF Form) Let \( S : V \to V \), then there exists a basis \( B \) for \( V \) such that

\[
[S]_B = \text{diag}(C(g_1), \ldots, C(g_s))
\]
where \( g_1 \mid g_2 \mid \cdots \mid g_s \) are monic.

13 February 3, 2014

Theorem 13.1. (ED for matrices) Every matrix \( n \times n \) matrix is similar to a matrix of form \( \text{diag}(C(g_1), C(g_2), \ldots, C(g_k)) \) where \( g_i \) is a power of a monic irreducible. Then \( \{g_1, \ldots, g_k\} \) are the elementary divisors. Two matrices \( A \) and \( B \) are similar iff they have the same elementary divisors.

Theorem 13.2. (IF for matrices) Every \( n \times n \) matrix \( A \) is similar to

\[
\text{diag}(C(f_1), \ldots, C(f_r))
\]
where \( f_1 \mid f_2 \mid \cdots \mid f_r \) are monic, the invariant factors of \( A \). Two \( n \times n \) matrices \( A \) and \( B \) are similar iff \( IF(A) = IF(B) \).
Let $S: V \to V$ be a linear operator, with basis $B = \{v_1, \ldots, v_n\}$ for $V$. Let $A = [S]_B$. Let $P_A(x) = \det(xI_n - A) = x^n + \text{lower terms}$, called the characteristic polynomial of $S$. So $P_S(x)$ is monic of degree $n = \dim V$.

Let $R = F[x]$, and $N \subset R^n$ submodule generated by all $n$ columns of $xI_n - A$.

**Lemma 13.3.** We have $\dim_P(R^n/N) = n$.

**Proof.** Do elementary transformation over $xI_n - A$. Then $R^n/N$ does not change up to isomorphism. So

$$xI_n - A \mapsto \text{diag}(f_1, \ldots, f_n)$$

with $f_i$ monic. But $P_S(x) = f_1 f_2 \cdots f_n$. Then the submodule $N' \subset R^n$ generated by the columns of the new matrix, so

$$R^n/N' = R/f_1 R \oplus \cdots \oplus R/f_n R$$

and

$$\dim(R^n/N) = \dim(R^n/N') = \sum \dim R/f_i R = \sum \deg(f_i) = \deg(P_S(x)) = n. \quad \square$$

If $g: R^n \to V$ given by $g(f_1, \ldots, f_n) = \sum_{i=1}^n f_i(S)(v_i) \in V$. I claim $g$ is an $R$-module homomorphism. Pick $f \in R$, then

$$g(f f_1, \ldots, f f_n) = \sum f(S) f_i(S)(v_i) = f(S) \left( \sum f_i(S)(v_i) \right) = f(S)(g(f_1, \ldots, f_n)).$$

Now applying $g$ to the first column of $xI - A$, we have

$$g(X - a_1, a_2, \ldots, a_n) = S(v_1) - a_1 v_1 - a_2 v_2 - \cdots - a_n v_n = 0.$$ 

So $g$ is zero on every column, so $g(N) = 0$, or $N \subset \ker(g)$. So we may factor through $\tilde{g}: R^n/N \to V$. Also, $g$ is surjective, since $g(e_i) = v_i \in \im(g)$. So $\tilde{g}$ is surjective. Since $\dim(R^n/N) = \dim(V) = n$, hence $\tilde{g}$ is an isomorphism, so we may express $N$ as a factor module of a free module. The columns of $xI - A$ are generators of $N$, say $\{y_1, \ldots, y_n\}$. Take the standard basis for free module $R^n$, say $\{x_1, \ldots, x_n\}$.

Suppose you have $S: V \to V$ or $n \times n$ matrix $A$. In the first case, pick a basis $B$ for $V$, let $A = [S]_B$. Form $xI_A$, and transform to $\text{diag}(f_1, \ldots, f_n)$ by elementary operations, where $f_i$ are monic and $f_1 | f_2 | \cdots | f_n$. Then the invariant factors are the nonconstant $f_i$, which will be 1.

So if $IF(S) = \{f_1, f_2, \ldots, f_r\}$, then $f_1 f_2 \cdots f_r = P_S(x)$, and $\sum \deg(f_i) = n = \dim(V)$.

**Example 13.4.** Let $G = GL_2(\mathbb{Z}/p\mathbb{Z})$, $p$ a prime. Then $|G| = (p^2 - 1)(p^2 - p)$. We want to find number of conjugacy classes in $G$. Two matrices are conjugate if they are similar, iff they have the same invariant factors. So the number of conjugacy classes is the same as the number of possible lists of invariant factors. If $IF(A) = \{f_1, \ldots, f_r\}$, then $f_1 \cdots f_r = P_A$. We have the restrictions that $\sum \deg(f_i) = 2$, and since the constant term of $P_A$ is nonzero (the matrices are invertible), so the $f_i$ have nonzero constant term.

So either $IF(A) = \{f_1\}$ or $IF(A) = \{f_1, f_2\}$ with $f_1 | f_2$. In the first case, $f_1$ is monic of degree 2 with nonzero constant term. So $f_1 = x^2 + ax + b$, where $b \neq 0$, giving $p(p - 1)$ possibilities. In the second, since $f_1 \mid f_2$, $f_1 = f_2$, and they have form $x + c$, with $c \neq 0$. This gives $p - 1$ choices. So the total number of conjugacy classes is $p(p - 1) + (p - 1) = p^2 - 1$.

If $A \sim (C(f_1)) = \begin{pmatrix} 0 & -a \\ 1 & -b \end{pmatrix}$ with $b \neq 0$. If $A \sim \text{diag}(C(f_1), C(f_2)) = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$, with $c \neq 0$. So every matrix is conjugate to one of these matrices. The latter case gives all central elements.

14 February 5, 2014

**Example 14.1.** Classify all $4 \times 4$ matrices $A$ such that $(A - 2I)^2 = 0$. We want to find rational canonical forms satisfying this, equivalent to giving a list of all RCFs of such $A$.

Let $R$ be a PID. Let $M$ be an $R$-module. Then

$$\text{Ann}(M) = \{r \in R : rM = 0\} = Rc$$
is an ideal in \( R \). So \( cM = 0 \) and if \( rM = 0 \), then \( c \mid r \). So \( M = R/Re \), and \( \text{Ann}(M) = Re \). If \( M \) is torsion, write

\[
M = R/Rf_1 \oplus \cdots \oplus R/Rf_s
\]

where \( f_1 \mid \cdots \mid f_s \). Then \( \text{Ann}(M) = Rf_s \).

If \( R = F[x] \), then if \( M \) is an \( R \)-module. Recall that we have an operator \( S : M \to M \) such that \( f(S)(m) = f(S) \cdot m \). So

\[
f(S) \in \text{Ann}(M) \iff f(S) \cdot M = 0 \iff f(S) = 0.
\]

So \( \text{Ann}(M) = Rf_{\min} \) for unique monic \( f_{\min} \), call it the minimal polynomial of \( S \). Then \( f(S) = 0 \) and \( g(S) = 0 \) for some \( g \in R \), then \( f \mid g \).

If \( f_1, \ldots, f_s \) are the invariant factors of \( M \), then \( f_r \) is the minimal polynomial.

Also, since \( P_S = f_1 f_2 \cdots f_s \) is divisible by \( f_{\min} \), which implies \( P_S(S) = 0 \), i.e., we get Cayley-Hamilton theorem.

Returning to the example, we see \( (X - 2)^2 \) annihilates \( A \). So \( f_{\min} \) divides \( (X - 2)^2 \).

Suppose \( IF(A) = \{f_1, \ldots, f_s\} \). We have the conditions that \( f_s \mid (X - 2)^2 \), \( f_1 \mid \cdots \mid f_s \), and \( \sum \deg(f_i) = 4 \).

First case, \( f_s = (X - 2)^2 \). So \( IF(A) = \{(X - 2)^2, (X - 2)^2\} \) or \( IF(A) = \{X - 2, X - 2, (X - 2)^2\} \).

Second case, \( f_s = X - 2 \), then \( IF(A) = \{X - 2, X - 2, X - 2, X - 2\} \).

The corresponding RCFs are

\[
\text{diag}(\begin{pmatrix} 0 & -4 \\ 1 & 4 \end{pmatrix}), \quad \text{diag}(2, 2, \begin{pmatrix} 0 & -4 \\ 1 & 4 \end{pmatrix}), \quad 2I_4.
\]

**Example 14.2.** Let \( S : V \to V \) induce \( V \) with an \( F[X] \)-module structure. TFAE

1. \( V \) is a cyclic \( F[X] \)-module
2. There exists \( v \in V \) such that \( \text{span} S(v), S^2(v), \ldots = V \). It is sufficient to take powers up to \( S^{n-1}(v) \) by Cayley-Hamilton.
3. \( IF(S) = \{f_1\} \).
4. \( ED(S) = \{h_1, \ldots, h_k\} \) where \( h_i \) are pairwise coprime.
5. \( f_{\min} = P_S \).

Remark for (c) above: Suppose \( R/Rf_1 \oplus \cdots \oplus R/Rf_s \simeq R/Rg \). Then \( \text{Ann} = gR = f_s R \), and \( \deg(g) = \sum \deg(f_i) = \deg(f_s) \), so that \( s = 1 \).

**14.1 Jordan Canonical Form**

A vector \( v \in V \) is an eigenvector of the eigenvalue \( \lambda \) if \( S(v) = \lambda v \). (So \( 0 \) is an allowable eigenvector.) Then \( E_\lambda = \{v \in V : S(v) = \lambda v\} \) is the eigenspace of \( \lambda \). Now choose \( B = \{v_1, \ldots, v_n\} \) basis for \( V \) such that all \( v_i \) are eigenvectors. Then \( [S]_B \) is diagonal with eigenvalues along the main diagonal.

We say \( S \) is diagonalizable if there exists a basis \( B \) for \( V \) such that \( [S]_B \) is diagonal, equivalently, there exists a basis for \( V \) of eigenvectors of \( S \).

The roots of \( P_S \) are the eigenvalues of \( S \). We say a monic polynomial \( f \in F[X] \) is split if \( f \) factors as \( f = (X - \lambda_1) \cdots (X - \lambda_n) \) for \( \lambda_i \in F \). So \( S \) diagonalizable implies \( P_S \) is split, but the converse is not true.

Assume that \( P_S \) is split. Then

\[
P_S = (X - \lambda_1)^{k_1} \cdots (X - \lambda_s)^{k_s}
\]

and \( \lambda_1, \ldots, \lambda_s \) are distinct. Then \( ED(S) \) are of form \( (X - \lambda_i)^{m_i} \). So

\[
[S]_B = \text{diag}(C(X - \lambda_1)^{m_1}, \ldots, C(X - \lambda_s)^{m_s}).
\]

Suppose \( V \simeq R/(x - \lambda)^m R \) for \( R = F[X] \). Then \( (S - \lambda I)^m = 0 \). Writing \( T = S - \lambda I \), \( T^m = 0 \). Since \( V \) is cyclic, there exists \( v \in V \) such that \( \{v, Sv, \ldots, S^{m-1}v\} \) is a basis for \( V \). Then \( C = \{v, Tv, \ldots, T^{m-1}v\} \) is a basis for \( V \) as well. Note \( Tv = Sv - \lambda v \), and \( T^2v = S^2v - 4Sv + \lambda^2 v \).
Note
\[ S(T^i(v)) = (T + \lambda I)(T^i(v)) = T^{i+1}(v) + \lambda T^i(v) \]
so \([S]_C\) is the matrix with \(\lambda\) on the main diagonal, and \(\lambda\) on the subdiagonal. This is the Jordan block.

**Theorem 14.3.** Let \(S\) be a linear operator such that \(P_S\) is split. Then there exists a basis \(B\) for \(V\) such that \([S]_B\) is the direct sum of Jordan blocks, unique up to permutation.

### 15 February 7, 2014

#### 15.1 Field Extensions

A field is a nonzero commutative ring such that every nonzero element is invertible. If \(f: F \rightarrow L\) is a homomorphism, \(\ker(f) \subseteq F\) and \(1 \notin \ker(f)\) since \(1 \mapsto 1\), so that \(\ker(f) = (0)\) and \(f\) is injective.

Suppose \(L\) is a field, and \(K \subseteq L\) is a subfield. Then \(L\) is a field extension of \(K\).

Suppose \(f: K \rightarrow L\) such that \(f(x) = x\) is a morphism of fields. Then
\[ K \simeq \text{im}(f) = f(K) \subseteq L \]
and we may view \(L\) as a field extension of \(K\) via \(f\). If \(L/K\), then \(L\) is a vector space over \(K\). We say \(L/K\) is an extension of finite degree if \([L : K] = \dim_K(L) < \infty\).

**Example 15.1.**

1. Always \([F : F] = 1\), and \([K : F] = 1\) implies \(K = F\).

2. \([\mathbb{C} : \mathbb{R}] = 2\) with basis \(\{1, i\}\).

3. \([\mathbb{R} : \mathbb{Q}] = \infty\).

**Proposition 15.2.** Suppose \(L/K/F\). Then \([L : F] = [L : K][K : F]\).

**Proof.** Standard. \(\square\)

**Corollary 15.3.** Then \([L : K] | [L : F]\) and \([K : F] | [L : F]\).

**Corollary 15.4.** Suppose \(F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n\). Then \([F_n : F_0] = \prod_{i=0}^{n-1}[F_{i+1} : F_i]\).

**Lemma 15.5.** Let \(F\) be a field, and \(S \subseteq F\) a subset. Then there exists a unique smallest subfield of \(F\) containing \(S\).

**Proof.** Take \(\bigcap_{S \subseteq F' \subset F} F'\). \(\square\)

Suppose \(L/F\) and \(S \subseteq L\). Let \(F(S)\) be the subfield of \(L\) generated by \(F \cup S\). Then \(F \subset F(S) \subset L\) is the smallest intermediate field containing \(S\). If \(S = \{\alpha_1, \ldots, \alpha_n\}\), then write \(F(S) = F(\alpha_1, \ldots, \alpha_n)\).

**Proposition 15.6.** The field
\[ F(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} : f, g \in F[X_1, \ldots, X_n], g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}. \]

**Proof.** Let \(K\) denote the RHS above. Then \(F \subset K \subset L\), and \(S \subseteq K\), since it contains \(\alpha_i/1\). It is clear that \(K\) is a field, so by minimality, \(F(\alpha_1, \ldots, \alpha_n) \subseteq K\). But certainly \(K \subset F(\alpha_1, \ldots, \alpha_n)\). \(\square\)

Now suppose \(F \subseteq L\), and \(\alpha_1, \alpha_2, \ldots, \alpha_n \in L\). Now
\[ F(\alpha_1, \ldots, \alpha_n) = \{f(\alpha_1, \ldots, \alpha_n) : f \in F[X_1, \ldots, X_n] \} \]
is a subring of \(L\) generated by \(\alpha_i\) over \(F\). Then
\[ F \subset F(\alpha_1, \ldots, \alpha_n) \subseteq F(\alpha_1, \ldots, \alpha_n) \subset L. \]

**Example 15.7.**
1. Consider $\mathbb{C}/\mathbb{R}$ and $S = \{i\}$. Then $\mathbb{R} \subset \mathbb{R}[i] = \mathbb{R}(i) \subset \mathbb{C}$ so $\mathbb{R}[i] = \mathbb{R}(i)$.

2. Let $F(X)$ be the quotient field, and $S = \{X\}$. Then $F \subset F[X] \subseteq F(X)$.

Note that in the first case the first generator is algebraic, in the second case it is not.

Let $K/F$, we say $\alpha \in K$ is algebraic over $F$ if there exists nonzero $f \in F[X]$ such that $f(\alpha) = 0$. Otherwise, it is called transcendental.

Example 15.8.

1. Every $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{R}$. Note $a + bi$ is a root of $x^2 - 2ax + (a^2 + b^2)$.

2. Suppose $L/K/F$, and $\alpha \in L$ is algebraic over $F$, then $\alpha$ is algebraic over $K$.

3. If $\alpha \in K/F$ is transcendental, the ring generated by $\alpha$ over $F$ is isomorphic to $F[\alpha]$ as rings. A field extension $K/F$ is called algebraic if every $\alpha \in K$ is algebraic over $F$. So $\mathbb{C}/\mathbb{R}$ is algebraic.

Theorem 15.9. Let $\alpha \in K/F$ be algebraic over $F$. Then there exists a monic polynomial $m_\alpha \in F[X]$ such that $m_\alpha(\alpha) = 0$ and $m_\alpha$ divides every polynomial $f$ such that $f(\alpha) = 0$. The elements $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ where $n = \deg(m_\alpha)$ is a basis for $F(\alpha)/F$. We have $[F(\alpha) : F] = \deg(m_\alpha)$ and $F(\alpha) = F[\alpha]$.

Proof. Let $\varphi : F[X] \to K$ such that $\varphi(g) = g(\alpha)$. And $\ker(\varphi) \neq 0$ since $\alpha$ is algebraic. So $\ker(\varphi) = F[X]m_\alpha$ for some monic $m_\alpha$. But $\text{im} \varphi = F[\alpha] \simeq F[X]/(m_\alpha)$. Since $m_\alpha$ is irreducible, $(m_\alpha)$ is maximal, so $F[\alpha]$ is a field, so that $F[\alpha] = F(\alpha)$.

The cosets $1, \ldots, \alpha^{n-1}$ form a basis for $F[X]/(m_\alpha) \simeq F(\alpha)$. So $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$ over $F$. \qed

16 February 10, 2014

Suppose $\alpha \in K/F$, and $\alpha$ algebraic over $F$. Then $m_\alpha(x) \in F[X]$. Suppose we find $f \in F[X]$ such that $f(\alpha) = 0$.

Example 16.1.

1. Take $\sqrt{2} \in \mathbb{R}$. Consider $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Then $m_{\sqrt{2}}(X) = X^2 - 2$.

2. Take $p$ prime, and $\xi_p$ the primitive $p$-th root of unity in $\mathbb{C}$. Then $\mathbb{Q}(\xi_p)/\mathbb{Q}$. Then $\xi_p$ is algebraic as a root if $X^p - 1$. But

$$X^p - 1 = (X - 1)(X^{p-1} + \cdots + X + 1)$$

and the second factor is known to be irreducible, hence the minimal polynomial. Then the extension is of degree $p - 1$.

Corollary 16.2. Let $K/F$ be a field extension, and $\alpha \in K$. Then $\alpha$ is algebraic over $F$ iff $F(\alpha)/F$ is of finite degree. This is also equivalent to $F(\alpha) = F[\alpha]$.

Proof. We know $[F(\alpha) : F] = \deg(\alpha) < \infty$. Suppose the extension is finite. Then $\{1, \alpha, \alpha^2, \ldots\}$ is linearly dependent over $F$. Thus there exist $a_i \in F$ not all 0, but almost all 0 such that $\sum a_i \alpha^i = 0$. So $\alpha$ is algebraic. \qed

Corollary 16.3. Every finite field extension if algebraic.

Proof. Let $[K : F] < \infty$, and $\alpha \in K$. But $F(\alpha) \subset K$ so $[F(\alpha) : F] \leq [K : F] < \infty$, so by the previous corollary $\alpha$ is algebraic. \qed
Corollary 16.4. Let $K/F$, and $\alpha_1, \ldots, \alpha_n \in K$ be algebraic over $F$. Then $F(\alpha_1, \ldots, \alpha_n) = F[\alpha_1, \ldots, \alpha_n]$. Moreover, $F(\alpha_1, \ldots, \alpha_n)$ is algebraic over $F$.

Proof. By induction, $n = 1$ is known. We know $\alpha_n$ is algebraic over $F$, hence over $F(\alpha_1, \ldots, \alpha_{n-1})$. But

\[
F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) \\
= F(\alpha_1, \ldots, \alpha_{n-1})[\alpha_{n-1}] \\
= F[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n] \\
= F[\alpha_1, \ldots, \alpha_n] \\
= F(\alpha_1, \ldots, \alpha_n)
\]

Also, $F(\alpha_1, \ldots, \alpha_n)$ is finite over $F(\alpha_1, \ldots, \alpha_{n-1})$, which is finite over $F$ by induction. \hfill \Box

Theorem 16.5. Let $K/F$, then the set of all elements over $K$ algebraic over $F$ is a subfield of $K$.

Proof. If $\alpha, \beta$ are algebraic, then $\alpha + \beta, \alpha\beta, \alpha^{-1} \in F(\alpha, \beta)$, which is algebraic over $F$. \hfill \Box

A class of field extensions is "good" if for every tower of field extensions $L/K/F$, then $L/F$ belongs to the class iff $L/K$ and $K/F$ belong to the class.

Theorem 16.6. The class of algebraic field extensions is "good."

Proof. Suppose $L/K/F$. If $L/F$ is algebraic, then $K/F$ and $L/K$ is algebraic. So suppose $L/K$ and $K/F$ are algebraic. Take $\alpha \in L$, so there exists nonzero monic polynomial $f \in K[X]$ such that $f(\alpha) = 0$. Write

\[
f = X^n + \beta_1 X^{n-1} + \cdots + \beta_n, \quad \beta_i \in K.
\]

Consider $F(\beta_1, \ldots, \beta_n, \alpha)/F(\beta_1, \ldots, \beta_n)/F$. But $\alpha$ is algebraic over $F(\beta_1, \ldots, \beta_n)$, so $F(\beta_1, \ldots, \beta_n, \alpha)/F$ is finite, so $\alpha$ is algebraic over $F$. \hfill \Box

Proposition 16.7. Let $f \in F[X]$ be a nonconstant polynomial. There is a field extension $K/F$ such that $[K : F] \leq \deg(f)$ and $f$ has a root in $K$.

Proof. Let $p$ be an irreducible divisor of $f$ in $F[X]$. Set $K = F[X]/(p(x))$, which is a field. We can embed $F$ in $K$, so view $K/F$. Then $[K : F] = \deg(p) \leq \deg(f)$. Note that $x + (p(x))$ is a roof of $p$, hence of $f$ in $K$ since

\[
K \ni p([x]) = [p(x)] = [0].
\]

Corollary 16.8. Let $f \in F[X]$ be a nonconstant polynomial. Then there is a field extension $L/F$ such that $[L : F] \leq \deg(f)!$ and $f$ is a product of linear factors over $L$.

Proof. Induction on $n = \deg(f)$. Find $K/F$ with $[K : F] \leq n$ and $\alpha \in K$ such that $f(\alpha) = 0$. Then $f = (x-\alpha)f(x)$, with $g \in K[x]$, and $\deg(g) = n-1$. By induction, there is a field $L/F$ with $[L : K] \leq (n-1)!$ such that $g$ splits over $L$. \hfill \Box

Let $f \in F[X]$ be a nonconstant polynomial. A field extension $K/F$ is called a splitting field of $f$ over $F$ if $f$ is split over $K$, and $K$ is generated by all roots of $f$ over $F$. So

\[
f = a(x-\alpha_1) \cdots (x-\alpha_n)
\]

with $\alpha_i \in K$, and $K = F(\alpha_1, \ldots, \alpha_n)$.

Example 16.9.

1. If $f$ is linear, then $F/F$ is splitting field extension of $f$.

2. If $f = X^3 - 1$ over $\mathbb{Q}$. Then $f = (x-1)(x-\omega)(x-\omega^2)$ where $\omega = \frac{-1+\sqrt{-3}}{2}$. So $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ is splitting field of $f$. 

23
3. If \( f \in F[X] \) is split over \( L/F \), then \( F(\alpha_1, \ldots, \alpha_n)/F \) is a splitting field extension of \( f \) where \( \alpha_1, \ldots, \alpha_n \) are all the roots of \( f \) in \( L \). Every \( f \in F[X] \) of degree \( n > 0 \) has a splitting field of degree \( \leq n! \).

Suppose \( \varphi: F \to F_1 \) is a field homomorphism, and suppose \( K/F \) and \( K_1/F_1 \) are extensions.

A field homomorphism \( \psi: K \to K_1 \) is called an extension of \( \varphi \) if \( \psi|_F = \varphi \).

Special case: When \( F_1 = F \), and \( \varphi = 1_F \) and then \( \psi(a) = a \) for all \( a \in F \). Then \( \psi \) is a field homomorphism over \( F \), and is \( F \)-linear since
\[
\psi(ax) = \psi(a)\psi(x) = a\psi(x).
\]

17 February 12, 2014

Suppose \( \varphi: F \to F_1 \), and \( f = \sum_{i=1}^n a_i x^i \), then define
\[
\varphi(f) = \sum_i \varphi(a_i)X^i \in F_1[X].
\]

**Proposition 17.1.** Let \( K = F(\alpha)/F \) be a finite extension, and \( f = m_\alpha, \varphi: F \to F_1 \) a field homomorphism, and \( K_1/F_1 \) a field extension. If \( \psi: K \to K_1 \) is an extension of \( \varphi \), then \( \psi(\alpha) \) is a root of \( \varphi(f) \). For every root \( \alpha_1 \) in \( K_1 \) of \( \varphi(f) \), there exists a unique extension \( \psi: K \to K_1 \) such that \( \psi(\alpha) = \alpha_1 \).

**Proof.** Since \( f(\alpha) = 0 \), apply \( \psi, \psi(f) = \varphi(f) \). So
\[
0 = \psi(f(\alpha)) = \psi(f)\psi(\alpha) = \varphi(f)(\psi(\alpha)).
\]

For the second claim, write \( K \simeq F[X]/F[X]f \), so \( X \) corresponds to \( \alpha \). We must have \( \rho: F[X] \to K_1 \), and
\[
\rho(x) = \alpha, \text{ and } \rho(g) = g(\alpha_1) \text{ and } \rho(f) = f(\alpha_1).
\]

**Corollary 17.2.** The number of extensions \( \varphi \) is the number of roots of \( \varphi(f) \) in \( K_1 \), which is at most \( \deg(f) \).

**Theorem 17.3.** Let \( f \in F[X] \) be a nonconstant polynomial, \( K/F \) a splitting field of \( f, \varphi: F \to F_1 \) an isomorphism. Let \( K_1/F_1 \) be a splitting field of \( \varphi(f) \in F_1[X] \). Then there exists an isomorphism \( \psi: K \to K_1 \) extending \( \varphi \).

**Proof.** By induction on \( n \). Let \( K = F, K_1 = F_1 \), and take \( \psi = \varphi \). Let \( \alpha \) be a root of \( f \) in \( K \), then \( m_\alpha | f \), so \( \varphi(m_\alpha) | \varphi(f) \), and \( \varphi(m_\alpha) \) is split in \( K \), and \( \alpha_1 \in K_1 \) is a root of \( \varphi(m_\alpha) \) and thus a root of \( \varphi(f) \).

By the proposition, there exists \( \rho: F(\alpha) \to F_1(\alpha_1) \) extending \( \varphi \) such that \( \rho(\alpha) = \alpha_1 \), and thus \( \text{im}(\rho) = F_1(\alpha_1) \). Then \( f = (X - \alpha)f \), and \( g \in F(\alpha)[X] \) and \( \dim(g) = n - 1 \) and \( g \) is split over \( K \), and the roots of \( g \) generate \( K \) over \( F(\alpha) \), so that \( K/F(\alpha) \) is a splitting field of \( g \).

Since \( \varphi(f) = (X - \alpha_1)\rho(g) \) and \( \rho(g) = \varphi(f) \) and \( K_1/F_1(\alpha_1) \) is a splitting field of \( \rho(g) \). By induction, there exists an extension \( \psi: K \to K_1 \) extending \( \rho \).

**Proposition 17.4.** Let \( f \in F[X] \) be a nonconstant polynomial, and \( K/F \) and \( K_1/F_1 \) two splitting fields of \( f \). Then there is an isomorphism \( \psi: K \to K_1 \) over \( F \).

**Proof.** Apply theorem to \( \varphi = 1_F: F \to F \).

17.1 Finite Fields

Let \( \mathbb{Z}/p\mathbb{Z} \) where \( p \) is prime is a field. If \( F \) is a field, \( f: \mathbb{Z} \to F: 1 \mapsto 1 \), then \( \ker(f) = p\mathbb{Z} \subseteq \mathbb{Z} \). So \( \mathbb{Z}/p\mathbb{Z} \hookrightarrow F \), so \( \mathbb{Z}/p\mathbb{Z} \) is a domain, hence \( p \) is prime. We say \( p \) is the characteristic of \( F \).

If \( p > 0 \), then \( p \) is the smallest positive integer such that \( p \cdot 1 = 0 \). If characteristic is 0, then \( n \cdot 1 \neq 0 \) for \( n \neq 0 \). Now let \( F \) be a field, and \( \text{char}(F) = 0 \), and \( \mathbb{Z} \hookrightarrow F \). Then we can invert all \( n \), so \( F \) contains an isomorphic copy of \( \mathbb{Q} \). These are known as the prime subfields.

If \( \text{char}(F) = p \), then \( (x + y)^p = x^p + y^p \). Then it is easily seen that raising to the power of \( p \) is a homomorphism, let \( \Phi: F \to F \) defined by \( \varphi(x) = x^p \) is the Frobenius endomorphism.

A field \( F \) is perfect if either \( \text{char}(F) = 0 \), or \( \text{char}(F) > 0 \) and \( F = F^p \). In particular, \( \mathbb{Z}/p\mathbb{Z} \) is perfect.

If \( f \in F[X], f = a_0X^n + \cdots + a_1X + a_0 \). Then
\[
f' = na_0X^{n-1} + \cdots + a_1 \in F[X]
\]
If \( \text{char}(F) = p > 0 \), then if \( f = X^p \), then \( f' = pX^{p-1} = 0 \).
Lemma 17.5. Let \( f \in F[X], \alpha \in F \) a root of \( f \). Then \( \alpha \) is a simple root iff \( f'(\alpha) \neq 0 \).

Proof. Let \( f = (X - \alpha)h \), then \( f' = h + (X - \alpha)h' \) and \( f'(\alpha) = h(\alpha) \neq 0 \) iff \( \alpha \) is simple.

Corollary 17.6. Let \( f \in F[X] \). If \( (f, f') = 1 \), then every root of \( f \) in \( F \) is simple.

Proof. If \( f(\alpha) = 0 \), then \( (X - \alpha) \mid f \), so \( (X - \alpha) \nmid f' \), and \( f'(\alpha) \neq 0 \), so \( \alpha \) is simple.

Now let \( F \) be a finite field, and \( \text{char}(F) = p > 0 \). Let \( F_0 \subset F \) be the prime subfield, so \( |F : F_0| = n \), with \( \{x_1, \ldots, x_n\} \) a basis, then

\[
F = \left\{ \sum_{i=1}^n a_i x_i : a_i \in F_0 \right\}
\]

so that \( |F| = p^n \).

18 February 19, 2014

Theorem 18.1. Let \( p \) be a prime integer \( n \geq 1 \). Then there exist a unique (up to iso) finite field of \( p^n \) elements.

Proof. Let \( q = p^n \). Consider the polynomial \( x^q - x \) over \( \mathbb{Z}/p\mathbb{Z} = F \). Let \( K \) be a splitting field of \( f \) over \( F \). Note that \( f' = qx^{q-1} - 1 = -1 \). So \( f \) and \( f' \) are coprime. So every root of \( f \) in the field \( K \) is simple. So \( f \) has exactly \( q \) roots in \( K \). Let \( L \) be the set of all roots of \( f \) in \( K \).

If \( x, y \in L \), then \( x^q = x \) and \( y^q = y \), then \( (xy)^q = xy, (x + y)^q = x^q + y^q = x + y \) and \( (x^{-1})^q = x^{-1} \). So \( L \) is a field of \( q \) elements. The polynomial \( f \) is split over \( L \), and \( L \) is generated by the roots of \( f \), so \( L = K \).

We have proved that a splitting field of \( X^q - X \) has \( q \) elements.

Suppose now that \( E \) is a field, and \( |E| = q \), so \( \text{char}(E) = p \). Then \( \mathbb{Z}/p\mathbb{Z} = F \subset E \). Also, \( |E^\times| = q - 1 \), so that if \( x \in E^\times \), \( x^{q-1} = 1 \), in which case \( x^q = x \) for all \( x \in E \). So \( E \) is the field of all roots of \( f = X^q - X \) and \( f \) is split over \( E \), and \( E \) is generated by all roots of \( f \). So \( E \) is a splitting field of \( X^q - X \) over \( F = \mathbb{Z}/p\mathbb{Z} \).

Thus \( E \) is unique up to isomorphism.

Example 18.2. Construct \( \mathbb{F}_4 \). We must have \( [\mathbb{F}_4 : \mathbb{F}_2] = 2 \). Then \( \mathbb{F}_4 = \mathbb{F}_2(\alpha) \) with \( \deg(\alpha) = 2 \).

The polynomial \( 2 + x + 1 \) is irreducible, so

\[
\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1).
\]

Then \( \alpha = x \), and \( \{1, \alpha\} \) is a basis for \( \mathbb{F}_4/\mathbb{F}_2 \), and \( \mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\} \).

Theorem 18.3. Let \( F \) be a field, \( A \subset F^\times \) a finite subgroup. Then \( A \) is cyclic.

Proof. By the structure theorem,

\[
A \cong \mathbb{Z}/(n_1) \oplus \cdots \oplus \mathbb{Z}/(n_r)
\]

where \( n_1 \mid n_2 \mid \cdots \mid n_r \).

Suppose \( r > 1 \). Suppose that \( n_1 \mid n_2 \). So \( \mathbb{Z}/(n_2) \) contains a cyclic group of order \( n_1 \). So \( \mathbb{Z}/(n_1) \oplus \mathbb{Z}/(n_2) \) contains \( \mathbb{Z}/(n_1) \oplus \mathbb{Z}/(n_1) \), and for \( x \) in this group, \( n_1 x = 0 \).

Transferring back with the isomorphism, the set

\[
n_1 \geq |\{a \in A | a^n_1 = 1\}| \geq (n_1)^2
\]

where the first inequality follows since the set is the root of \( x^{n_1} - 1 \). This is a contradiction since \( n_1 > 1 \). Thus \( r = 1 \), so \( A \) is cyclic.

Corollary 18.4. The multiplicative group \( \mathbb{F}_q^\times \) is cyclic of order \( q - 1 \). In particular, \( (\mathbb{Z}/p\mathbb{Z})^\times \) is cyclic if \( p \) is prime.

Corollary 18.5. If \( K/F \) is an extension of finite fields, then \( K \) is generated by one element for some \( \alpha \in K \).

Proof. Take \( \alpha \) a generator of \( K^\times \).

A finite extension \( K/F \) is simple if \( K = F(\alpha) \) for some \( \alpha \in K \).
19 Normal Extensions

Lemma 19.1. Let $E/F$ be a finite field extension and $\sigma: F \to L$ a homomorphism. Then there exists a finite field extension $M/L$ and an extension $\tau: E \to M$ of $\sigma$.

Proof. Write $E = F(\alpha_1, \ldots, \alpha_n)$. Proceed by induction on $n$. Suppose $n = 1$, so $E = F(\alpha)$. Let $f = m_\alpha \in F[x]$, which is irreducible. Now find a finite field extension $M/L$ such that $\sigma(f)$ has a root $\beta$ in $M$. There exists an extension $\tau: E \to M$ of $\sigma$ such that $\tau(\alpha) = \beta$.

For the induction step, we have the tower

$$F \subset F(\alpha_1) \subset E$$

so we may find an extension $\rho: F(\alpha_1) \to K$ extending $\sigma$, and since $E = F(\alpha_1)(\alpha_2, \ldots, \alpha_n)$, and now we may find $\tau: E \to M$ extending $\rho$, hence extending $\sigma$.

Proposition 19.2. Let $E/F$ be a finite field extension. TFAE

1. $E$ is a splitting field of a polynomial over $F$.

2. For any $M/F$, and any homomorphism $\sigma: E \to M$ over $F$, we have $\sigma(E) = E$.

3. Every irreducible polynomial in $F[x]$ that has a root in $E$ is split over $E$.

Proof. Suppose $E$ is a splitting field of a polynomial $f \in F[x]$. So $f$ is split over $E$, and has roots $\alpha_1, \ldots, \alpha_n$, and $E = F(\alpha_1, \ldots, \alpha_n)$. So note $f(\alpha_i) = 0$. Applying $\sigma$, we see

$$0 = \sigma(f(\alpha_i)) = (\sigma f)(\sigma \alpha_i) = f(\sigma(\alpha_i))$$

so $\sigma(\alpha_i)$ is a root of $f$ in $M$. So $\sigma(\alpha_i) = \alpha_j \in E$ for some $j$. So $\sigma(E) \subset E$. Furthermore, $\sigma: E \to E$ is an injective homomorphism, but since $[E:F] < \infty$, so $\sigma$ is surjective by standard linear algebra.

Now suppose 2. Take $f \in F[x]$ irreducible, and $\alpha \in E$, then $f(\alpha) = 0$. Take $K$ a splitting field of $f$ over $E$. Then we have the tower

$$F \subset F(\alpha) \subset E \subset K$$

and $\beta$ a root of $f$ in $K$. We have a homomorphism $\rho: F(\alpha) \to K$ with $\rho(\alpha) = \beta$ extending $id_E$. Now by the lemma, there exists $M/K$ and $\sigma: E \to M$ extending $\rho$. But $\sigma(E) = E$, but $\beta = \rho(\alpha) = \sigma(\alpha) \in E$. So all roots of $f \in K$ are in $E$, so $f$ splits over $E$.

Let $E = F(\alpha_1, \ldots, \alpha_n)$. Then $f_i = m_{\alpha_i}$ is irreducible. Then $f_i(\alpha_i) = 0$, so $f_i$ has a root in $E$. From (3), $f_i$ is split over $E$, so $f = f_1 \ldots f_n$ is split over $E$ and $\alpha_i$ are roots of $f$. Thus $E$ is generated by roots of $f$ over $E$, so $E$ is a splitting field of $f$.

Then $E/F$ is normal if $E/F$ satisfies the above conditions. We have the following normality test. Let $E = F(\alpha_1, \ldots, \alpha_n)$. Let $f_i = m_{\alpha_i}$. Then $E/F$ is normal iff each $f_i$ is split over $E$.

Proof. If $E/F$ is normal, then each $f_i$ is irreducible and has a root in $E$, thus splits over $E$ by (3). Conversely, $E$ is a splitting field of $f = f_1 \ldots f_n$. So $E/F$ is normal by (1).

Example 19.3.

1. Every extension of degree 1 or 2 is normal. If $[E:F] = 2$, pick $\alpha \in E \setminus F$, so $F(\alpha) = E$. Then $F(\alpha) = E$, so $f = m_{\alpha}$ is of degree 2, so $f$ has root over $\alpha$ over $E$, so $f = (x-\alpha)(x-\beta)$ is split over $E$.

2. Consider $Q(\sqrt[3]{2}) \subset \mathbb{R}$. Then $Q(\sqrt[3]{2})/Q$ is not normal. Let $\alpha = \sqrt[3]{2}$, and

$$m_{\alpha} = X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[4]{4})$$

but the last factor is not split over $Q(\sqrt[3]{2})$ as it has no real roots.

Corollary 19.4. Let $L/E/F$ be finite field extensions. If $L/F$ is normal, then so is $L/E$.
Proof. We know $L$ is a splitting field of $f \in F[x]$ over $F$. Then $L$ is a splitting field of $f \in E[x]$.  

Example 19.5.

1. Let $\xi^3 = 1$ be the primitive cubic root. We have the tower

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \xi).$$

The first extension is not normal as noted above. We have

$$X^3 - 2 = (X - \sqrt[3]{2})(X - \sqrt[3]{2}\xi)(X - \sqrt[3]{2}\xi^2)$$

is split, but $m_\xi = X^2 + X + 1$ is split over $L$. Thus the total extension is normal, but the first is not.

2. Consider

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})$$

where each extension is quadratic, hence normal. The minimal polynomial of $\sqrt{2}$ is $X^4 - 2 = (X - \sqrt{2})g$, where $g$ has no real roots. So the whole tower is not normal.

Let $E/F$ be a finite field extension. A normal closure of $E/F$ is a finite field extension $L/F$ such that

1. $L \supset E$
2. $L/F$ is normal
3. For every field $L'$ with $E \subset L' \subset L$, then $L'/F$ is not normal.

Theorem 19.6. Every finite field extension $E/F$ has a normal closure. It is unique up to isomorphism over $E$.

Proof. Write $E = F(\alpha_1, \ldots, \alpha_n)$. Let $f_i = m_{\alpha_i}$, and $f = f_1 \cdots f_n \in F[X] \subset E[X]$. Take $L$ to be a splitting field of $f$ over $E$. I claim that $L$ is a splitting field of $f$ over $E$. We know $f$ is split over $E$. We also know $L$ is generated over $E$ be the roots of $F$, so

$$F(\text{roots of } f) = F(\alpha_1, \ldots, \alpha_n, \text{roots of } f) = E(\text{roots of } f).$$

I know claim $L/F$ is normal. Suppose $E \subset L' \subset L$ and $L'/F$ is normal. Is $L' = L$. Since $f_i$ is irreducible, it has a root $\alpha_i$ in $E \subset L'$, so $f_i$ is split over $L'$, which implies $f$ is split over $L'$. But $L = F(\text{roots of } f)$, and the roots of $f$ are in $L'$. Thus $L = L'$. So $L/F$ is normal closure of $E/F$. Let $L/F$ be a normal closure of $E/F$.

Let $L/F$ be a normal closure of $E/F$. I claim $L$ is a splitting field of $f$ over $E$ hence over $F$. If $f_i$ is irreducible, it has a root $\alpha_i$ in $E \subset L$, which implies $f_i$ is split over $L$, so $f$ is split over $L$. Now

$$E \subset F(\alpha_1, \ldots, \alpha_n) \subset F(\text{roots of } f \text{ in } L) \subset L$$

but the third field is a splitting field of $f$ over $F$, hence normal. So $L/F$ is normal closure, and thus $L = F(\text{roots of } f \text{ in } L)$, which is a splitting field of $f$ over $F$ or $E$.

Since every two splitting fields of $f$ over $E$ are isomorphic over $E$, we are done.  

So if $L$ is a splitting field of $f = f_1 \cdots f_n$ over $E = F(\alpha_1, \ldots, \alpha_n)$, then $L/F$ is a normal closure of $E/F$.

Example 19.7. 1. If $E/F$ is normal, then $E/F$ is a normal closure of $E/F$.

2. The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is not normal. The minimal polynomial is $X^3 - 2$, so we must add $\sqrt{2}, \sqrt{2}\xi, \sqrt{2}\xi^2$, but it suffices to add $\xi$ to get the normal closure $\mathbb{Q}(\sqrt{2}, \xi)$.
20 Separable Field Extensions

**Lemma 20.1.** Let \( f \in F[X] \) be a nonconstant polynomial. The following are equivalent,

1. \( f \) and \( f' \) are relatively prime over \( F \).
2. \( f \) has no multiple roots in every extension \( K/F \).
3. There is a field extension \( K/F \) such that \( f \) is split over \( K \) and \( f \) has no multiple roots in \( K \).

**Proof.** Suppose \( f \) and \( f' \) are coprime. If \( \alpha \in K \) is a multiple root of \( f \), then \( f'((\alpha)) = 0 = f((\alpha)) \), so both \( f \) and \( f' \) are divisible by \( X - \alpha \) over \( K \), so \( f \) and \( f' \) are not relatively prime.

Now suppose \( f \) has no multiple roots in every extension. Take \( K \) a splitting field of \( f \).

Now assume (3). We can write \( f = (X - \alpha_1) \cdots (X - \alpha_n) \), and \( f'(\alpha_i) \neq 0 \). so \( X - \alpha_i \) are all irreducible divisors of \( f \) over \( K \). But \( X - \alpha_i \nmid f' \), so \( f \) and \( f' \) are coprime. \( \square \)

**Definition 20.2.** A nonconstant polynomial \( f \in F[X] \) is called separable if \( f \) satisfies the above conditions.

**Corollary 20.3.**

1. A polynomial \( f \in F[x] \) is separable iff \( f \) is separable in \( K[X] \) for a field extension \( K/F \).
2. If \( f \) is separable, \( g \mid f \) is nonconstant, then \( g \) is separable.

**Proof.** We have \((f,f') = 1 \) over \( F \) iff \((f,f') = 1 \) over \( K \). For the second claim, if \( K/F \) is a splitting field of \( f \), then

\[ f = a(x - \alpha_1) \cdots (x - \alpha_n) \]

with \( \alpha_i \) distinct, then \( g \mid f \) implies \( f \) is a product of \( x - \alpha_i \), so \( g \) has no multiple roots. So \( g \) is separable. \( \square \)

**Corollary 20.4.** An irreducible \( f \in F[X] \) is separable iff \( f' \neq 0 \).

**Example 20.5.** Let \( \text{char}(F) = p > 0 \). If \( f = x^p - a \), then \( f' = px^{p-1} = 0 \), so \( f \) is not separable. Over \( K/F \), \( a = b^p \) and \( b \in K \), then \( f = X^p - b^p = (X - b)^p \), so \( b \) is a multiple root of \( f \), thus not separable.

We say \( F \) is perfect if \( \text{char}(F) = 0 \), or \( \text{char}(F) = p \) and \( F = F^p \). Perfect fields are \( \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q \).

**Proposition 20.6.** Let \( f \in F[X] \) be an irreducible polynomial over a perfect field \( F \). Then \( f \) is separable.

**Proof.** Need to show \( f' \neq 0 \). If \( f = aX^n + \text{lower terms} \), then \( f' = naX^{n-1} + \cdots \) is nonzero if \( \text{char}(F) = 0 \). Now let \( \text{char}(F) = p > 0 \), and assume \( f' = 0 \). Then \( f(X) = g(X^p) \), where \( g \in F[X] \). That is,

\[ f(X) = a_nX^{pn} + a_{n-1}X^{p(n-1)} + \cdots + a_0 \]

but if \( F \) is perfect, \( a_i = b_i^p \) for some \( b_i \). Then

\[ f(X) = b_n^pX^{pn} + b_{n-1}^pX^{p(n-1)} + \cdots + b_0^p = (b_nX^n + b_{n-1}X^{n-1} + \cdots b_0)^p \]

a contradiction. \( \square \)

Now let \( K/F \) be a field extension, and \( \alpha \in K \). We say \( \alpha \) is separable over \( F \) if \( m_\alpha \) is separable. If \( F \) is perfect, every \( \alpha \in K \) is separable over \( F \).

**Lemma 20.7.** Let \( L/K/F \), and \( \alpha \in L \) be separable over \( F \). Then \( \alpha \) is separable over \( K \).

**Proof.** Let \( f = m_\alpha \) over \( F \), and \( g \) the minimal polynomial of \( \alpha \) over \( K \), so \( g \mid f \). Since \( f \) is separable, the corollary implies \( g \) is separable, so \( \alpha \) is separable over \( K \). \( \square \)

**Lemma 20.8.** Let \( K/F \) be a finite field extension, and \( \sigma : F \rightarrow L \) a field homomorphism. Then there are at most \(|K:F|\) extensions \( K \rightarrow L \) of \( \sigma \).
Proof. Let \( K = F(\alpha_1, \ldots, \alpha_n) \). Proceed by induction on \( n \). If \( n = 1 \), then \( K = F(\alpha) \), and \( f = m_\alpha \), then the number of extensions is equal to the number of roots of \( \sigma f \) in \( L \), which is at most \( \deg(f) = [K : F] \).

Now consider the tower

\[ F \subset F(\alpha_1) \subset L. \]

Then \( \sigma \) has at most \([F(\alpha_1) : F] \) extensions \( \rho: F(\alpha_1) \to L \). Then by induction, each \( \rho \) has at most \([K : F(\alpha_1)] \) extensions \( \psi: K \to L \). Thus the number of extensions \( K \to L \) of \( \sigma \) is at most \([F(\alpha_1) : F][K : F(\alpha_1)] = [K : F] \).

A finite field extension \( K/F \) is separable if there is a field homomorphism \( \sigma: F \to L \) that has exactly \([K : F] \) extensions \( \rho: K \to L \).

**Proposition 20.9.** Let \( K = F(\alpha)/F \) be a finite field extension. Then \( K/F \) is separable iff \( \alpha \) is separable over \( F \).

**Proof.** Suppose \( \sigma: F \to L \), and \( \sigma \) has \( n \) extensions, where \( n = [F(\alpha) : F] = \deg(m_\alpha) \). So \( \sigma(m_\alpha) \) has exactly \( n \) roots in \( L \). \( m_\alpha \) is split over \( L \), and has no multiple roots in \( L \). So \( m_\alpha \) is separable, so \( \alpha \) is separable.

Conversely, suppose \( \alpha \) is separable, so \( m_\alpha \) is separable. Take \( L \) a splitting field of \( m_\alpha \), and \( \sigma: F \to L \), so \( m_\alpha \) has exactly \( n = \deg(m_\alpha) \) roots in \( L \). Thus \( \sigma \) has \( n = [F(\alpha) : F] \) extensions, so that \( K/F \) is separable.

**Lemma 20.10.** Let \( F \) be an infinite field, and \( L/F \) a field extension. Let \( g \in L[X_1, \ldots, X_n] \) be a nonzero polynomial. Then there exist \( a_1, \ldots, a_n \) such that \( g(a_1, \ldots, a_n) \neq 0 \).

**Proof.** We proceed by induction on \( n \), the number of variables. If \( n = 1 \), \( g \) has only finitely many roots in \( F \). Now suppose \( g = h_m X^m + h_{m-1} X^{m-1} + \cdots + h_0 \) where \( h_i \in L[X_1, \ldots, X_{n-1}] \). So there exists \( h_i \neq 0 \) since \( g \neq 0 \). By induction, \( h_i(a_1, \ldots, a_{n-1}) \neq 0 \) for some \( a_i \in F \). Then

\[ g(a_1, \ldots, a_{n-1}, X) = \cdots + h_i(a_1, \ldots, a_{n-1})X_1^i \in L[X_n] \]

is nonzero. Now use \( n = 1 \) case.

If \( F = \mathbb{F}_q \), then \( f = X^q - X \), and \( f(a) = 0 \) for all \( a \in F \).

**Corollary 20.11.** Let \( g_1, \ldots, g_m \in L[X_1, \ldots, X_n] \) be pairwise distinct polynomials. Then there are \( a_1, \ldots, a_n \in F \) such that \( g_i(a_1, \ldots, a_n) \) are distinct.

**Proof.** Apply lemma to \( \prod_{i<j} (g_i - g_j) \).

**Theorem 20.12.** Let \( K/F \) be separable. Then \( K = F(\alpha) \) for some \( \alpha \in K \).

**Proof.** Case 1: \( F \) is infinite. Let \( \rho_1, \ldots, \rho_m \) be extensions of \( \sigma: F \to L \), with \( m = [K : F] \). Let \( K = F(\alpha_1, \ldots, \alpha_n) \). Set

\[ g_j(X_1, \ldots, X_n) = \sum_{i=1}^{n} \rho_j(\alpha_i)X_i \in L[X_1, \ldots, X_n] \]

for \( j = 1, \ldots, m \). The \( g_j(X_1, \ldots, X_n) \) are distinct polynomials. By the corollary, there exist \( a_1, \ldots, a_n \in F \) such that

\[ g_j(a_1, \ldots, a_n) = \sum_{i=1}^{n} \rho_j(\alpha_i) a_i = \rho_j \left( \sum_{i=1}^{n} \alpha_i a_i \right) \]

are distinct. So \( \alpha = \sum_{i=1}^{n} \alpha_i a_i \) is an element such that \( \rho_1(\alpha), \ldots, \rho_m(\alpha) \) are distinct. Then \( \rho_j|_{F(\alpha)} \) are all distinct, so \( \sigma \) has at least \( m \) extensions to \( F(\alpha) \to L \). So \( m \leq [F(\alpha) : F] \leq [K : F] = m \). So \( K = F(\alpha) \).

(Note: I think this proof as given in class needs to be tweaked slightly so that we can “factor” the \( \rho \) to the left above.)

Case 2: \( F \) is finite. Know since unit group is cyclic.

**Example 20.13.** Let \( \text{char}(F) = p \), and let \( F(X,Y)/F(X^p,Y^p) \), which is an extension of degree \( p^2 \). If \( \alpha \in F(X,Y) \), then \( \deg(\alpha) \leq p \) since \( \alpha \) satisfies \( X^p - \alpha^p \in F(X^p,Y^p) \). So \( F(X,Y)/F(X^p,Y^p) \) cannot be generated by one element.
Proposition 20.14. Let $L/E/F$ be a tower of finite field extensions. Then $L/F$ is separable iff $L/E$ and $E/F$ are separable.

Proof. Suppose $L/F$ is separable. Then there exists $\sigma:F \rightarrow M$ with $[L:F]$ extensions to $\rho:L \rightarrow M$. But there is $\tau:E \rightarrow M$ with the number of $\tau$ extending $\sigma$ is at most $[E:F]$, and the number of $\rho$ extending $\tau$ is at most $[L:E]$. But $[L:F]=[L:E][E:F]$, so we must have equality everywhere. Thus $E/F$ and $L/E$ are separable.

Conversely, suppose $[E:F]=m$. Then there exist $\tau_1,\ldots,\tau_m:E \rightarrow M$ extensions of a given $\sigma:F \rightarrow M$. But $L=E(\alpha)$ for some $\alpha$ separable over $E$. Let $f=m_n \in E[X]$ over $E$, which is separable. Then $f_i:=\tau_i f \in M[X]$ is separable. Let $g=f_1\ldots f_m \in M[X]$. Now let $K/M$ be a splitting field of $g$. Since $[L:E]=n$ every $f_i$ has exactly $n$ roots in $K$. Every $\tau_i$ has exactly $n$ extensions $\rho_i:L \rightarrow K$. Thus we have at least $n \cdot m = [L:F]$ extensions, so $\rho:L \rightarrow K$ of $\sigma:F \rightarrow M \rightarrow K$. Thus $L/F$ is separable. \hfill $\square$

Corollary 20.15. Let $E/F$ be a finite field extension. TFAE

1. $E/F$ is separable.
2. Every $\alpha \in E$ is separable over $F$.
3. $E=F(\alpha_1,\ldots,\alpha_n)$, with $\alpha_i$ separable over $F$.
4. $E=F(\alpha)$, with $\alpha$ separable over $F$.

Proof. (1)--(2). If $\alpha \in E$, then $F \subset F(\alpha) \subset E$, so by Proposition, $F(\alpha)/F$ is separable, thus $\alpha$ is separable over $F$.

(2)--(3) Clear.

(3)--(1) By induction on $n$. We have the tower $F \subset F(\alpha_1,\ldots,\alpha_n-1) = K \subset K(\alpha_n)$. But $\alpha_n$ is separable over $F$, hence separable over $K$. The conclusion now follows from the proposition.

(1)--(4) We know $E=F(\alpha)/F$ is separable, so $\alpha$ is separable.

(4)--(3) Trivial. \hfill $\square$

Corollary 20.16. Every finite field extension of a perfect field is separable.

Proof. If $\alpha \in E/F$, then $m_\alpha$ is irreducible, hence separable. Thus $\alpha$ is separable over $F$, so $E/F$ is separable. \hfill $\square$

21 Galois Field Extensions

Let $E/F$ be a finite field extension. Then

$\text{Gal}(E/F) = \{ \sigma : E \rightarrow E \text{ over } F \}$.

Proposition 21.1. We have $|\text{Gal}(E/F)| \leq [E:F]$ and $|\text{Gal}(E/F)| = [E:F]$ iff $E/F$ is normal and separable.

Proof. Let $\sigma \in \text{Gal}(E/F)$ is $F$ linear, hence extends $1_F$. So $|\text{Gal}(E/F)|$ is at most the number of extensions of $1_F$, which is at most $[E:F]$.

For the second statement, suppose $\sigma : E \rightarrow M$ over $F$. We need to show $\sigma(E) = E$. Let $\{\tau_1,\ldots,\tau_n\} = \text{Gal}(E/F)$, with $n = [E:F]$. Let $\rho_i : E \rightarrow M$ be extensions of $1_F$. There are at most $n = [E:F]$ extensions, so the $\rho_1,\rho_2,\ldots,\rho_n$ are all extensions of $1_F$. So $\sigma = \rho_i$ for some $i$, thus

$\sigma(E) = \rho_i(E) = \tau_i(E) = E$

and $E/F$ is normal.

For separability, $1_F$ has $n$ extensions $\tau_i : E \rightarrow E$. Since $n = [E:F]$, so $E/F$ is separable by definition.

Conversely, suppose $\sigma : F \rightarrow L$, and there are $\tau_1,\ldots,\tau_n : E \rightarrow L$ are extensions of $\sigma$, with $n = [E:F]$. Embed $E$ into $L$ by $\tau_1$. Since $E/F$ is normal, $\tau_i(E) = E$, so $\tau_i : E \rightarrow E$ is an isomorphism over $F$, so $\tau_1,\ldots,\tau_n \in \text{Gal}(E/F)$. Then

$n \leq |\text{Gal}(E/F)| \leq n$. \hfill $\square$
A finite field extension $E/F$ is called a Galois field extension if $|\text{Gal}(E/F)| = [E : F]$, equivalently, $E/F$ is normal and separable.

**Example 21.2.**

1. $|\text{Gal}(\mathbb{C}/\mathbb{R})| = \{1, \tau\}$. So $\mathbb{C}/\mathbb{R}$ is Galois.

2. Suppose $\text{char}(F) \neq 2$, pick $a \in F^\times$ and $a \notin (F^\times)^2$. Then $X^2 - a$ is irreducible. Then $E = (F[X]/(X^2 - a))/F$ is a quadratic field extension. We know $E/F$ is normal, and $(X^2 - a)' = 2X \neq 0$, so $E/F$ is separable, and thus Galois, so $\text{Gal}(E/F) = \{1, \sigma\}$. Then $\sigma$ must permute the roots $\pm \alpha$ of $X^2 - a$, so $\sigma(a + ba) = a - ba$.

3. Now let $\text{char}(F) = 2$. Consider $f = X^2 + X + a$, with $a \in F$. Assume $f$ has no roots in $F$, thus irreducible. Then set $K = (F[X]/(f))/F$ is a quadratic extension. And $f' = 2X + 1 = 1 \neq 0$. Thus $K/F$ is Galois, and $\text{Gal}(K/F) = \{1, \sigma\}$. So $\sigma$ permutes the roots, whose sum is the coefficient of $X$, so $\sigma(\alpha) = \alpha + 1$.

4. Let $q = p^m$, with $p$ a prime. We have $\mathbb{F}_q \subset \mathbb{F}_{q^n}$, with $X^{q^n} - X$ split. Let $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$.

5. Let $E = F(\alpha)/F$ be Galois, with $G = \text{Gal}(E/F)$, and $f = m_\alpha \in F[X]$. Let $\sigma \in G$, then $f(\alpha) = 0$, and $f(\sigma(\alpha)) = 0$, thus $f(\sigma(\alpha)) = 0$, so $\sigma(\alpha)$ is a root of $f$. So $G$ acts simply transitively on the set $X$ of roots of $f$ in $E$. That is, for all $\beta, \gamma \in X$, there exists unique $\sigma \in G$ such that $\sigma(\beta) = \gamma$. So $G \cong \mathbb{Z}/\mathbb{Z}$ as $G$-sets. Isomorphism seen by fixing $\beta$ and having $\sigma \mapsto \sigma(\beta)$.

Consider $\mathbb{Q}(\sqrt{2 + \sqrt{2}})/\mathbb{Q}$. Let $\alpha = \sqrt{2 + \sqrt{2}}$, so $\alpha^2 = 2 + \sqrt{2}$, then $(\alpha^2 - 2)^2 = 2$, so $\alpha^4 - 4\alpha + 2 = 0$. Thus $X^4 - 4X^2 + 2$ is the minimal polynomial as it is 2-Eisenstein, hence irreducible. This polynomial splits, hence the extension is Galois of order 4.

We know there exists unique $\sigma \in F$ such that $\sigma(\sqrt{2 + \sqrt{2}}) = \sqrt{2 - \sqrt{2}}$. Thus $\sigma(2 + \sqrt{2}) = 2 - \sqrt{2}$, so $\sigma(\sqrt{2}) = -\sqrt{2}$. Then

$$\sigma^2(\sqrt{2 + \sqrt{2}}) = \sigma(\sqrt{2 - \sqrt{2}}) = \sigma(\sqrt{2}/\sqrt{2 + \sqrt{2}})$$

which equals

$$\frac{-\sqrt{2}}{\sqrt{2} - \sqrt{2}} = \frac{-\sqrt{2 + \sqrt{2}}}{2}$$

and $\sigma^2$ is not the identity, so $G = \{e, \sigma, \sigma^2, \sigma^3\}$.

Another example.

Consider $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, which is normal as the splitting field of $(X^2 - 2)(X^3 - 2)$, hence a Galois Extension of order 4. So $|G| = 4$. The roots are $\pm \sqrt{2}$ and $\pm \sqrt{3}$. For any $\alpha \in G$, $\sigma(\sqrt{2}) = \pm \sqrt{2}$ and $\sigma(\sqrt{3}) = \pm \sqrt{3}$. This has Klein-4 Galois group.

Lastly, Let $\mathbb{Q}(\sqrt{2}, \xi)$ is an extension of degree 6, and $|G| = 6$. If $\sigma \in G$, then $\sigma(\sqrt{2}) = \sqrt{2}, \sqrt{2}\xi, \sqrt{2} = \xi$, and $\sigma(\xi) = \xi, \xi^2$. Then $G \cong S_3$.

**Theorem 21.3.** (Artin) Let $E$ be any field, and $G$ a finite group of automorphisms of $E$. Set

$$F = E^G = \{x \in E : \sigma(x) = x, \forall \sigma \in G\}.$$  

Then $E/F$ is a Galois extension and $G = \text{Gal}(E/F)$.

**Proof.** Let $|G| = n$. I claim every $\alpha \in E$ is algebraic over $F$ and $[F(\alpha) : F] \leq n$. Let $X = \{\sigma(\alpha) : \sigma \in G\} \subset E$. Let $f = \prod_{x \in X}(X - x) \in E[X]$. Take $\rho \in G$, and let $\rho(f) = \prod_{x \in X}(X - \rho(x))$. Then $G$ acts on $X$, and $\rho : X \to X : x \mapsto \rho(x)$ is a bijection. So $f \in E^G[X] = F[X]$. In fact, $\alpha \in X$, then $\alpha$ is algebraic over $F$. So

$$[F(\alpha) : F] = \deg(m_\alpha) \leq \deg(f) = [X] \leq |G| = n.$$  

Moreover, $f$ is separable, so $\alpha$ is separable.

Second claim: $[E : F] \leq n$. Suppose towards a contradiction $[E : F] > n$. Find $\alpha_1, \ldots, \alpha_{n+1} \in E$ linearly independent over $F$. Then $[F(\alpha_1, \ldots, \alpha_n) : F] > n$, but is finite and separable since every $\alpha_i$ is algebraic and separable. Hence there exists $\alpha \in E$ such that $F(\alpha_1, \ldots, \alpha_n) = F(\alpha)$, and so $[F(\alpha) : F] > n$, a contradiction.

So $E/F$ is separable as every $\alpha \in E$ is separable over $F$ by claim 1. Now $G \subset \text{Gal}(E/F)$, so

$$n \leq |\text{Gal}(E/F)| \leq [E : F] \leq n$$

So $E/F$ is Galois, so $G = \text{Gal}(E/F)$.

31
Example 21.4. 1. Let $E = F_0 = F(X_1, \ldots, X_n)$. Then $S_n$ acts on $E$ by permuting the $X_i$. Then $F = E^G$ is a subfield of symmetric rational functions. By Artin, $S_n = \text{Gal}(E/F)$.

2. Let $G$ be a finite group, so $G \subset S_n$ for some $n$. Let $S_n$ be the galois group of $E/F$. Then $E/E^G/F$ is a tower with $\text{Gal}(E/E^G) = G$.

Inverse Galois Problem: Give a finite group $G$, is there a Galois field extension $E/Q$ with $\text{Gal}(E/Q) \simeq G$?

Theorem 21.5. These maps are bijections inverse to each other.

Proof. Let $K$ be an intermediate field. Let $H = \text{Gal}(E/K)$. Want to show $E^H = K$. If $x \in K$, and $\sigma \in H$, then $\sigma(x) = x$, so $x \in E^H$, thus $K \subset E^H$.

Conversely, $E/F$ is Galois, so $E/K$ is Galois. Thus $[E : K] = |H|$. By Artin’s theorem, $E/E^H$ is Galois, so $[E : E^H] = |H|$. It follows that $|E^H : K| = 1$, so $K = E^H$.

Now let $H \subset G$ be a subgroup, and let $K = E^H$. We need to show $\text{Gal}(E/K) = H$. This is just Artin’s theorem.

Some properties:
1. $H_1 \subset H_2 \iff E^{H_1} \supset E^{H_2}$.
2. $E^{(e)} = E$ and $E^G = F$.
3. Consider the tower $E/K/F$. Then $[K : F] = [G : H]$, where $G$ is the galois group of $E/F$, and $H$ is the Galois group of $E/K$.
4. If $H \subset G$, and $\sigma \in G$, then $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$. Note that $x \in E^{\sigma H \sigma^{-1}} \iff \sigma \sigma^{-1} x = x$ for all $h \in H$.
   That is, $h \sigma^{-1}(x) = \sigma^{-1}(x)$ for all $h \in H$, so $\sigma^{-1}(x) \in E^H$, which holds iff $x \in \sigma(E^H)$.
5. $E^H/F$ is normal iff $H$ is normal in $G$. Moreover, $\text{Gal}(E^H/F) \simeq G/H$.

Proof. Suppose $E^H/F$ is normal. Let $\sigma \in G$. Consider the restriction $\sigma : E^H \rightarrow E$, it is an extension of $1_F$, so by normality, $\sigma(E^H) = E^H$. But $\sigma(E^H) = E^{\sigma H \sigma^{-1}}$, so $H = \sigma H \sigma^{-1}$ for all $\sigma$, so $H \leq G$.

Conversely, suppose $H \leq G$. Then $\sigma(E^H) = E^H$. This gives a map

$$f : G \rightarrow \text{Gal}(E^H/F) : \sigma \mapsto \sigma|_{E^H}$$

Then $\ker(f) = \text{Gal}(E/E^H) = H$. This in turn induces

$$\tilde{f} : G/H \rightarrow \text{Gal}(E^H/F)$$

Then

$$\text{Gal}(E^H/F) \geq |G/H| = |G : H| = |E^H : F| \geq \text{Gal}(E^H/F).$$

Then $[E^H : F] = \text{Gal}(E^H/F)$, hence Galois. and $|G/H| = \text{Gal}(E^H/F)$, so $G/H \simeq \text{Gal}(E^H/F)$ with isomorphism $\sigma H \mapsto \sigma|_{E^H}$.

Example 21.6. The extension $\mathbb{Q}(\sqrt{2 + \sqrt{3}})/\mathbb{Q}$ has only $\mathbb{Q}(\sqrt{2})$ as its subfield.

We have $\mathbb{Q}(\sqrt{2} : X)$ is degree 6 over $\mathbb{Q}$ with Galois group $S_3 = \langle \sigma, \tau \rangle$ where $\sigma$ is a 3-cycle, and $\tau$ a transposition. The subgroups are $\{e, \sigma, \sigma^2\}$, $\{e, \tau\}$, $\{e, \sigma \tau\}$, and $\{e, \sigma^2\}$. Suppose $F \subset K, L \subset M$. Suppose $K = F(\alpha_1, \ldots, \alpha_n)$, then $KL = L(\alpha_1, \ldots, \alpha_n)$.

Theorem 21.7. Suppose $K/F$ is Galois. Then $KL/L$ is also Galois, and the restriction homomorphism $f : \text{Gal}(KL/L) \rightarrow \text{Gal}(K/F)$ is injective with image $\text{Gal}(K/K \cap L)$. 32
Proof. We know $K$ is a splitting field of $f \in F[X]$. Thus $KL$ is a splitting field of $f$ over $K$, so $KL/L$ is normal. The $\alpha_i$ can be taken to be the roots of $f$, so the $\alpha_i$ are separable over $F$, hence over $L$, so $KL/L$ is separable, thus Galois.

Now pick $\sigma \in \text{Gal}(KL/L)$ in the kernel of $f$. Since $K/F$ is normal, $\sigma(K) = K$. But $\sigma|_K = 1_K$ and $\sigma|_L = 1_L$, so $\sigma$ is the identity on $L$ and the $\alpha_i$, hence $\sigma = 1_{KL}$.

Now take $\sigma \in \text{Gal}(KL/L)$, so $\sigma$ is trivial on $L$, hence on $K \cap L$. Therefore $\sigma|_K \in \text{Gal}(K/K \cap L)$. Let $H$ be the image of $f$. Want to show $K^H \subset K \cap L$. Take $x \in K^H$, so $\sigma|_K(x) = x$ for any $\sigma \in \text{Gal}(KL/L)$. So $\sigma(x) = x$, so $x \in L$.

We say $K$ and $L$ are disjoint over $F$ if $K \cap L = F$.

**Corollary 21.8.** If $K$ and $L$ are disjoint, then $\text{Gal}(KL/L) \simeq \text{Gal}(K/F)$.

**Theorem 21.9.** Let $K/F$ and $L/F$ be Galois extensions. Then $KL/F$ is Galois, and the restriction homomorphism

$$r : \text{Gal}(KL/F) \to \text{Gal}(K/F) \times \text{Gal}(L/F)$$

is injective. If $K \cap L = F$, then $r$ is an isomorphism.

**Proof.** We know $K$ is a splitting field of $f \in F[x]$ over $F$. Similarly, $L$ is a splitting field of $g \in F[x]$ over $F$. Then $KL$ is a splitting field of $fg$, so $KL/F$ is normal. Then since $KL/L$ is separable, and $L/F$ is separable, thus $KL/F$ is separable, and thus Galois.

Now pick $\sigma \in \text{Gal}(KL/F)$, with $\sigma|_K = 1_K$, and $\sigma|_L = 1_L$. Then $\sigma$ is in the kernel of $\text{Gal}(KL/L) \to \text{Gal}(K/F)$, which is trivial, so $\sigma = e$.

Now suppose $K \cap L = F$, and pick $\rho \in \text{Gal}(K/F)$, $\tau \in \text{Gal}(L/F)$. Pick $\rho' \in \text{Gal}(KL/L) \to \text{Gal}(K/F)$ which maps to $\rho'|_K = \rho$. Also, Let $\tau' \in \text{Gal}(KL/K)$, with $\tau'|_L = \tau$. Then

$$(\rho \tau')(\rho')|_K = (\rho'|_K \tau'|_K) = \rho \cdot 1_K = \rho$$

and

$$(\rho \tau')|_L = \tau.$$

Finally, $r(\rho \tau') = (\rho, \tau)$. So

$$\text{Gal}(KL/F) \simeq \text{Gal}(K/F) \times \text{Gal}(L/F)$$

And the stronger statement is

$$\text{Gal}(KL/F) = \text{Gal}(KL/L) \times \text{Gal}(KL/K).$$

---

**Example 21.10.**

$$\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) = \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}).\mathbb{Q}(\sqrt{2})) \times \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}).\mathbb{Q}(\sqrt{3})) \simeq \mathbb{Z}/(2) \times \mathbb{Z}/(2).$$

Let $F$ be a field. An $F$-algebra is a ring $A$ together with the structure of a vector space over $F$. Now suppose $L/F$ is Galois, and $G = \text{Gal}(L/F)$. Consider the category of $F$-subalgebras of $L \times \cdots \times L$, where we’ve take finitely many copies of $L$.

If $A \subset L^n$, set

$$X^A = \text{Hom}_{F-\text{alg}}(A, L)$$

which is a finite set. Given $\sigma \in G$, $\sigma \circ f \in X^A$. So $X^A$ is a $G$-set. So we want to consider the category of finite $G$-sets. We then get a functor sending $A \to X^A$, and a morphism $A \to B$ to $X^A \to X^B$. In the other direction, suppose you’re given $X$. Let $L^X = \text{Map}(X, L) \simeq L^n$ where $|X| = n$. Denote by $F^X = \text{Map}_G(X, L)$ whose elements are $f$ such that $f(\sigma x) = \sigma f(x)$ which is in $L^X$. So $X \to F^X$, and the morphisms $X \to Y$ goes to $F^Y \to F^X$. These give an equivalence of categories.

We can view $L$ as a $G$ set. Since $F$ has only one map into $L$, it corresponds to one point. Given $F \times \cdots \times F$, we have the possible composites

$$F \times \cdots \times F \xrightarrow{\pi} F \to L$$

33
for a total of $n$ maps, so the corresponding object is the union of $n$ points. In general, the direct product of algebras corresponds to the disjoint union of sets. The tensor product of algebras over $F$ corresponds to a direct product of sets. If the algebra is a field, we get $X$ has a transitive action. So $L^H$ corresponds to $G/H$. Thus the set $X = X_1 \cup \cdots \cup X_s$ with $X_i$ transitive, then corresponds to a direct product $K_1 \times \cdots \times K_s$ where $F \subset K_i \subset L$.

Furthermore, $\text{Aut}(F \times \cdots \times F) = \text{Aut}([n]) = S_n$. Consider $K = L^H$. Then

$$\text{Aut}(K/F) = \text{Gal}(K/F) = \text{Aut}_G(G/H).$$

Then suppose $f : G/H \to G/H$. Then $H = eH \mapsto \sigma H$, so that $\tau H \mapsto \tau \sigma H$. Then

$$\sigma H = f(H) = f(\tau H) = \tau f(H) = \tau \sigma H$$

which holds iff $\sigma^{-1} \tau \sigma \in H, \forall \tau \in H$, iff $\sigma^{-1} H \sigma \subset H$, which holds iff $\sigma \in N_G(H)$.

## 22 Cyclotomic Field Extensions

Fix a field $F$, and $n$ a positive integer such that $\text{char}(F) \nmid n$. Then $f_n = X^n - 1$ is separable over $F$ and $f_n^n = nX^{n-1}$, and $(f_n, f_n^n) = 1$. Let $F_n/F$ be a splitting field of $f_n$. Then $F_n/F$ is the $n$th cyclotomic field extension of $F$.

Denote by $\mu_n \subset F_n$ the subgroup in $F_n^\times$ of all $n$th roots of unity. Then $\mu_n$ is cyclic of order $n$. Then $\xi_n$ is a primitive $n$th root of unity is a generator of $\mu_n$. Then $F_n = F(\xi_n)$, and there are $\varphi(n)$ primitive roots. Write $G_n = \text{Gal}(F_n/F)$. For any $\sigma \in G_n$, then $\sigma(\xi_n) = \xi_n^i$, where $(i, n) = 1$. This induces a map

$$G_n \to (\mathbb{Z}/n\mathbb{Z})^\times : \sigma \mapsto i + n\mathbb{Z}.$$ 

Then $\sigma(\xi) = \xi^i$ for all $\xi \in \mu_n$ since we have a formula on a generator. This map is injective, for if $i = 1 + n\mathbb{Z}$, then $\sigma(\xi_n) = \xi_n$, so $\sigma = e$.

Then we have an embedding $G_n \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$, hence $G_n$ is abelian.

Consider $F = \mathbb{Q}$, $\xi_n \in F_n$, and $F_n = \mathbb{Q}(\xi_n)$. Then $\Phi_n \in \mathbb{Q}[X]$ denotes the minimal polynomial of $\xi_n$ over $\mathbb{Q}$. I claim $\Phi_n$ has integer coefficients. We know $\Phi_n \mid X^n - 1$. Find $\alpha \in \mathbb{Q}^\times$ such that $\alpha \Phi_n \in \mathbb{Z}[X]$ is primitive. Then

$$X^n - 1 = (\alpha \Phi_n) \cdot g$$

So by a previous lemma, $g \in \mathbb{Z}[X]$. So the leading terms are $\pm 1$, but $\Phi_n$ is monic, so $\alpha = \pm 1$. Then $\alpha \Phi_n \in \mathbb{Z}[X]$, hence $\Phi_n \in \mathbb{Z}[X]$.

Let $F_n = \mathbb{Q}(\xi_n)/\mathbb{Q}$. We know $\Phi_n = m_{\xi_n} \in \mathbb{Z}[X]$ is monic, called the $n$th cyclotomic polynomial.

**Lemma 22.1.** Every primitive $n$th root of unity is a root of $\Phi_n$.

**Proof.** If $\xi$ is primitive, then $\xi = \xi_n^i$ for $(i, n) = 1$. I claim that for every prime $p$ such that $p \nmid n$, then $\xi_n^p$ is a root of $\Phi_n$. Then $X^n - 1 = \Phi_n \cdot g$ for some $g \in \mathbb{Z}[X]$. Then $\xi_n^p$ is a root of $X^n - 1$, I claim it is not a root of $g$, hence a root of $\Phi_n$.

Towards a contradiction, suppose $g(\xi_n^p) = 0$. Let $g(X) = g(X^p) \in \mathbb{Z}[X]$, so $g_1(\xi_n) = 0$. This implies $\Phi_n \mid g_1$ over $\mathbb{Z}[X]$ since $\Phi_n$ is primitive. So $g_1 = \Phi_n \cdot h$ for $h \in \mathbb{Z}[X]$.

Now pass to $\mathbb{F}_p$ by mapping $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ by reducing the coefficients modulo $p$. Then $\bar{g_1}(X) = \bar{g}(X^p) = \bar{g}(X)p$. Thus $\bar{g_1} = \bar{g}p$. So $\Phi_n \mid \bar{g_1} = \bar{g}p$. Let $\ell$ be an irreducible divisor of $\Phi_n$ over $\mathbb{F}_p$. Then $\ell \mid \Phi_n$, hence $\ell \mid \bar{g}$, so $\ell \mid \bar{g}$. Since $\ell \mid \Phi_n$, hence $\ell^2 \mid \Phi_n$, hence $\Omega^2 \mid \Phi_n$, where $\Omega$ is a root of unity. So $X^n - 1$ has a multiple root in a splitting field of $\ell$ over $\mathbb{F}_p$. This gives us a contradiction since $X^n - 1$ is separable over $\mathbb{F}_p$, since $p \nmid n$. \qed

**Theorem 22.2.** We have $\text{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$, and

$$\Phi_n(X) = \prod_{\xi \text{ primitive}} (X - \xi)$$

and $\deg(\Phi_n) = \varphi(n)$. 

34
Proof. First, \[
\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| \geq |G| = [\mathbb{Q}(\zeta_n)/\mathbb{Q}] = \deg(\Phi_n) \geq \varphi(n)
\]

To compute \(\Phi_n\), we have
\[
X^n - 1 = \prod_{\xi \in \mu_n(\mathbb{C})} (X - \xi) = \prod_{d | n} \prod_{\xi \text{ primitive}} (X - \xi) = \prod_{d | n} \Phi_d.
\]
This follows for if \(\xi \in \mu_n\), then \(\text{ord}(\xi) = d \mid n\), where \(\xi\) is a primitive \(d\)th root of unity. We conclude
\[
\Phi_n = \frac{X^n - 1}{\prod_{d | n, d \neq n} \Phi_d}.
\]

Example 22.3. 1. Let \(n = p\) be prime. Then
\[
\Phi_p = X^{p-1} + X^{p-2} + \cdots + 1 = \frac{X^p - 1}{X - 1}.
\]

2. Let \(n = p^k\). Then
\[
\Phi_{p^k}(X) = \Phi_p(X^{p^{k-1}}) = X^{p^{k-1}(p-1)} + X^{p^{k-1}(p-2)} + \cdots + 1.
\]

3. \(\Phi_1 = X - 1, \Phi_2 = X + 1, \Phi_3 = X^2 + X + 1, \Phi_4 = X^2 + 1, \Phi_5 = X^4 + X^3 + X^2 + X + 1, \Phi_6 = X^2 - X + 1.
\]
However, \(\Phi_{105}\) is the first cyclotomic polynomial which does not have coefficients \(\{\pm 1\}\) because it is a product of 3 odd primes.

4. Let \(G\) be abelian and finite. There exists \(n\) and a surjection \(f: (\mathbb{Z}/n\mathbb{Z})^* \rightarrow G\). Let \(H = \ker(f)\), so \(G = (\mathbb{Z}/n\mathbb{Z})^*/H\). Then we have the tower \(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^H/\mathbb{Q}\). This is the inverse Galois problem for finite abelian groups. (Added later: I believe the claim about the surjection comes by combining the Structure Theorem from Finitely Generated Abelian Groups with Dirichlet’s Theorem on arithmetic progressions. For instance, writing \(G \simeq \mathbb{Z}/(n_1) \oplus \cdots \oplus \mathbb{Z}/(n_k)\), we can find primes \(p_i\) such that \(p_i \equiv 1 \pmod{n_i}\) for each \(i\) since \((1, n_i) = 1\). Let \(n = p_1 \cdots p_k\), so that
\[
(\mathbb{Z}/(n))^* \simeq (\mathbb{Z}/(p_1))^* \oplus \cdots \oplus (\mathbb{Z}/(p_k))^* \simeq \mathbb{Z}/(p_1 - 1) \oplus \cdots \oplus \mathbb{Z}/(p_k - 1).
\]
Taking projection maps on each component into \(G\) gives this surjection, I think.
Since \(H \triangleleft G\), it follows that \(\mathbb{Q}(\zeta_n)^H/\mathbb{Q}\) is Galois with Galois group isomorphic to \((\mathbb{Z}/n\mathbb{Z})^*/H \simeq G\), as desired.)

23 Algebraically closed fields

Proposition 23.1. Let \(F\) be a field. TFAE

1. Every finite field extension of \(F\) is trivial.

2. Every irreducible polynomial over \(F\) is linear.

3. Every nonconstant polynomial over \(F\) has a root in \(F\).

4. Every nonconstant polynomial over \(F\) is split.

Proof. (1) \(\implies\) (2). Let \(f \in F[X]\) be irreducible. Then \(F[X]/fF[X]\) is a field extension of \(F\) of degree \(\deg(f)\). By hypothesis, \(\deg(f) = 1\).

(2) \(\implies\) (3). \(f\) has an irreducible divisor, which is linear by (2). Thus \(f\) has a root.

(3) \(\implies\) (4). \(f\) has a root \(a \in F\), then \(f = (x - a)g\) is split by induction.

(4) \(\implies\) (1). Let \(L/F\) be a finite field extension. Take \(\alpha \in L\), let \(f = m_\alpha \in F[X]\) be irreducible. By hypothesis, \(f\) is split, so \(\deg(f) = 1\), thus \(\alpha \in F\). So \(L = F\).
A field $F$ satisfying the above conditions is called algebraically closed. Note $\mathbb{R}$ has no odd degree nontrivial extension iff there are no irreducible polynomial over $\mathbb{R}$ of degree greater than 1. (I think this should be greater than 2).

Also, $\mathbb{C}$ has no quadratic extension. We know $X^2 = a \in \mathbb{C}$ has a root in $\mathbb{C}$.

**Theorem 23.2.** The field $\mathbb{C}$ is algebraically closed.

**Proof.** Consider a tower $L/\mathbb{C}/\mathbb{R}$, where $L$ is a finite extension. Replacing $L$ be a normal closure of $L$ over $\mathbb{R}$, we may assume that $L/\mathbb{R}$ is normal, hence Galois. Need to show that $L = \mathbb{C}$. (Note the normal closure still is a finite extension as we need only adjoin the roots of the minimal polynomials of the generators of $L$ over $\mathbb{R}$, of which there are finitely many.)

Let $\text{Gal}(L/\mathbb{R}) = G$. So $H \subset G$ is a Sylow 2-subgroup. Then $[L^H : \mathbb{R}] = [G : H]$ is odd. But $\mathbb{R}$ has no nontrivial odd degree extensions, so $[G : H] = 1$, thus $G = H$, so $G$ is a 2-group. Now let $N = \text{Gal}(L/\mathbb{C})$. Then $N \leq G$, since $[G : N] = 2$. Suppose $|N| > 1$. But $N$ is also a 2-group as a subgroup of $G$. There exists a subgroup $N_0 \subset N$ such that $[N : N_0] = 2$.

Then $[L^{N_0} : \mathbb{C}] = [N : N_0] = 2$, so $L^{N_0}/\mathbb{C}$ is quadratic, a contradiction. Thus $|N| = 1$, so $[L : \mathbb{C}] = 1$, which implies $L = \mathbb{C}$.

Let $F$ be a field. A field extension $L/F$ is called an algebraic closure of $F$ if $L/F$ is algebraic, and $L$ is algebraically closed.

**Example 23.3.** Let $E/F$, with $E$ algebraically closed. Let

$$L = \{x \in E : x \text{ is algebraic over } F\}.$$ 

I claim $L$ is an algebraic closure of $F$. The first property holds clearly. We have the tower $E/L/F$. Let $K$ be a finite extension of $L$. Then there extension $M/E$ such that $K$ extends to $M$. But $E = M$ since $E$ is algebraically closed. Since $K/L$ is finite, and $L/F$ is algebraic, $K/F$ is algebraic, so $K = L$, thus $L$ is algebraically closed.

**Theorem 23.4.** Every field admits an algebraic closure.

**Proof.** Let $P$ be the set of all nonconstant polynomials over $F$. For each $f \in P$, let $X_f$ be a variable. Let $R = F[X_f, f \in P]$. Consider the ideal $I$ generated by $f(X_f)$, $f \in P$. I claim $I \neq R$. For suppose $I = R$, so $1 \in I$. Then

$$1 = \sum_{f \in P_0} f(X_f) \cdot g_f$$

where $P_0 \subset P$ is a finite subset, and $g_f \in R$. Let $L/F$ be a field extension such that all $f \in P_0$ have roots, say $a_f$ is such that $f(a_f) = 0$. Then substituting, we find

$$1 = \sum 0 \cdot g_f = 0$$

a contradiction.

Thus there exists a maximal ideal $M$ such that $I \subset M \subset R$. So $R/M$ is a field, and then

$$F \to R \to R/M := E$$

so $E/F$ is a field extension. But $f(X_f) \in I \subset M$, which implies $f(\bar{X}_f) = 0$ in $E$. So every $f \in P$ has a root in $E$. Repeating this process yields a sequence

$$F \subset E_1 \subset E_2 \subset \cdots$$

where every nonconstant polynomial over $E_i$ has a root in $E_{i+1}$. Then set $E = \bigcup E_i$, which is a field extension over $F$.

Claim: $E$ is algebraically closed. Take $f \in E[X]$. It has finitely many coefficients, so there is $E_i$ such that $f \in E_i[X]$. Then $f$ has a root in $E_{i+1} \subset E$. □
Every two algebraic closures of $F$ are isomorphic over $F$ (but not canonically). Suppose $F_{\text{alg}}/F$ and $E/F$ is a finite extension. Now let $M/F_{\text{alg}}$ be a finite extension. There exists an embedding $E \to M$, but $F_{\text{alg}} = M$ since $F$ has no nontrivial finite extension, so we may view $E$ as an intermediate subfield of $F_{\text{alg}}/F$.

We may consider

$$F_{\text{sep}} = \{ \alpha \in F_{\text{alg}} : \alpha \text{ separable over } F \}$$

There is a correspondence between the fields between $F$ and $F_{\text{sep}}$ and closed subgroups of $\text{Gal}(F_{\text{sep}}/F)$. We have a tower $\mathbb{Q}_{\text{sep}}/E/Q$. If $G = \text{Gal}(E/Q)$, then we get a surjection $\text{Gal}(\mathbb{Q}_{\text{sep}}/\mathbb{Q}) \to G$.

For finite fields,

$$\text{Gal}( (\mathbb{F}_q)_{\text{sep}} / \mathbb{F}_q) = \lim_{n \to \infty} \mathbb{Z}/n\mathbb{Z} \subset \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$$

We have a map $\mathbb{Z}/(mn) \to \mathbb{Z}/(n) : a_{mn} + mn\mathbb{Z} \mapsto a_n + n\mathbb{Z}$. The limit consists of cosets $\{(a_n + n\mathbb{Z} : a_{nm} \equiv a_n \mod n)\}$.

## 24 Galois Group of a Polynomial

Let $f \in F[X]$ be nonconstant and separable. Let $L/F$ be a splitting field of $f$, which is Galois. Then we define the Galois group of $f$ to be $\text{Gal}(L/F)$.

Let $\alpha_1, \ldots, \alpha_n$ be roots of $f$ in $L$, so $L = F(\alpha_1, \ldots, \alpha_n)$. Then $\sigma \in \text{Gal}(f) = G$ permutes $\alpha_i$. So $G$ acts on $\{\alpha_1, \ldots, \alpha_n\}$ transitively. This gives an injective map $G \to S_n$, so any automorphism acting trivially on the roots is the identity on $L$.

**Example 24.1.**

1. Let $f = X^n - 1$ over $\mathbb{Q}$. Then

$$\text{Gal}(f) = \text{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$$

2. Let $L = F_0(X_1, \ldots, X_n)$, and $F = L^{S_n}$. Then $\text{Gal}(L/F) \simeq S_n$. We have the generic polynomial

$$f(X) = \prod_{i=1}^n (X - X_i) \in F[X].$$

So $L/F$ is a splitting field of $f$, and $\text{Gal}(f) = S_n$.

**Proposition 24.2.** Let $L/F$ be a Galois extension, $G = \text{Gal}(L/F)$, and $\alpha \in L$. Then

$$\deg(\alpha) = |\{\sigma(\alpha), \sigma \in G\}|.$$

**Proof.** Let $S = \{\sigma(\alpha), \sigma \in G\} \subset L$. Then let $f(X) = \prod_{\beta \in S} (X - \beta)$. Then

$$(\sigma f)(X) = \prod_{\beta \in S} (X - \sigma(\beta)) = f$$

for all $\sigma \in G$, so $f \in F[X]$, and $f(\alpha) = 0$. Then $\deg(f) = |S|$. What is $[F(\alpha) : F]$? We can map $F(\alpha) \to L$ by sending $\alpha \mapsto \beta$ by some $\sigma \in G$, which exists by definition of $S$. Then the identity of $F$ has at least $|S|$ extensions $F(\alpha) \to L$. Then we find

$$|S| \leq [F(\alpha) : F] \leq \deg(f) = |S|$$

In particular, $f$ is the minimal polynomial of $\alpha$. 

**Example 24.3.**
1. Let \( \alpha = \sqrt{3} + \sqrt{2} \). We can compute that \( \deg(\alpha) \) is at most 6. Consider the Galois extension \( \mathbb{Q}(\sqrt{3}, \sqrt{2}, \xi_3) \). This is Galois since \( \mathbb{Q}(\sqrt{3}) \) and \( \mathbb{Q}(\sqrt{2}, \xi_3) \) are Galois, hence their composite is Galois. But these fields are disjoint over \( \mathbb{Q} \), since the only quadratic subfield of \( \mathbb{Q}(\sqrt{2}, \xi_3) \) is \( \mathbb{Q}(\sqrt{3}) \) which is not isomorphic nor equal to \( \mathbb{Q}(\sqrt{3}) \). Since they are disjoint, we have the Galois group is isomorphic to the product of the Galois groups, 
\[
G \simeq \mathbb{Z}/(2) \times S_3
\]
If \( \sigma \in G \), \( \sigma(\alpha) = \pm \sqrt{3} + \xi_i \sqrt{2} \) for \( i = 0, 1, 2 \). So \( |\sigma(\alpha)| = 6 = \deg(\alpha) \).
Also, \( \mathbb{Q}(\alpha) \) is not normal, since the roots of the minimal polynomial of \( \alpha \) generate the normal closure, which then must contain \( \pm \sqrt{3} \), so \( \mathbb{Q}(\sqrt{3}, \sqrt{2}, \xi_3) \) is the normal closure.

25 Radical Extensions

Let \( \text{char}(F) = 0 \). For \( n \geq 1 \), let \( K = F(\alpha)/F \) be a finite field extension. If \( \alpha^n \in F \), we say that \( K/F \) is \( n \)-radical.

**Lemma 25.1.** Let \( K/F \) be an \( n \)-radical extension, and \( \xi_n \in F \). Then \( K/F \) is Galois and \( \text{Gal}(K/F) \) is cyclic.

**Proof.** Let \( \alpha \in K \) and \( K = F(\alpha) \), with \( \alpha^n = a \in F \). Then \( f = X^n - a \) is split over \( K \) with roots \( \xi_i \alpha \) for \( i = 0, 1, \ldots, n-1 \). Thus \( K/F \) is splitting field of \( f \), hence normal, hence Galois.

Let \( \mu_n \) denote the group of all \( n \)-th roots of unity. We have a map
\[
f : G = \text{Gal}(K/F) \to \mu_n : \sigma \mapsto \frac{\sigma(\alpha)}{\alpha} = \xi_i.
\]
for some \( i \) since \( \sigma(\alpha) = \xi_i \alpha \).

I claim \( f \) is a homomorphism. Note
\[
f(\sigma \tau) = \frac{\sigma \tau(\alpha)}{\alpha} = \frac{\sigma \tau(\alpha)}{\sigma(\alpha)} \cdot \frac{\sigma(\alpha)}{\alpha} = \sigma \left( \frac{\tau(\alpha)}{\alpha} \right) \cdot \left( \frac{\sigma(\alpha)}{\alpha} \right).
\]
But \( \tau(\alpha)/\alpha \in \mu_n \subset F \), thus is fixed, so the above is then equal to
\[
\frac{\tau(\alpha)}{\alpha} \cdot \frac{\sigma(\alpha)}{\alpha} = f(\tau) f(\sigma).
\]
I now claim \( f \) is injective. Suppose \( f(\sigma) = 1 = \frac{\sigma(\alpha)}{\alpha} \). Thus \( \sigma(\alpha) = \alpha \) which implies \( \sigma = e \), so that \( G \) is cyclic as it is isomorphic to a subgroup of the cyclic group \( \mu_n \).

Let \( L/F \) be Galois, and \( G = \text{Gal}(L/F) \). Then \( G \subset \text{End}_F(L) \), which is a vector space over \( L \).

**Lemma 25.2.** The set \( G \) is linearly independent over \( L \).

**Proof.** Suppose
\[
\sum_{\sigma \in G} x_\sigma \cdot \sigma = 0.
\]
Here \( x_\sigma \in L \). Suppose the number of \( x_\sigma \) is the smallest. Choose \( \tau \) such that \( x_\tau \neq 0 \). Now
\[
\sum_{\sigma \in G} x_\sigma \cdot \sigma(y) = 0
\]
for all \( y \in L \). Then for any \( z \),
\[
0 = \sum_{\sigma \in G} x_\sigma \cdot \sigma(yz) = \sum_{\sigma \in G} x_\sigma \cdot \sigma(y) \sigma(z).
\]
Also,
\[
0 = \sum_{\sigma \in G} x_\sigma \sigma(y) \tau(z).
\]
Subtracting yields
\[ 0 = \sum_{\sigma \in G} x_{\sigma}(y)(\sigma(z) - \tau(z)) \]
for all \( y, z \in L \). Then
\[ 0 = \sum_{\sigma \in G} x_{\sigma}(\sigma(z) - \tau(z)) \cdot \sigma. \]

But the \( \tau \)-coefficient is zero. By assumption, there is also a \( \rho \) such that \( x_{\rho} \neq 0 \). Then the \( \rho \)-coefficient above is \( x_{\rho}(\rho(z) - \tau(z)) \). Since \( x_{\rho} \neq 0 \), then \( \rho(z) - \tau(z) \neq 0 \) for some \( z \), contrary to minimality.

**Proposition 25.3.** (Hilbert Theorem 90). Let \( L/F \) be a cyclic extension of degree \( n \). If \( \xi_n \in F \), then \( L/F \) is \( n \)-radical.

**Proof.** By assumption \( G = \langle \sigma \rangle \) is the Galois group. Consider the sum
\[ \sum_{i=0}^{n-1} \xi_n^{-i} \sigma^i(x) \neq 0 \]
for some \( x \in L \). Such \( x \) exists since the \( \sigma^i \) are independent by the previous lemma. Then
\[ \sigma(\alpha) = \sum_{i=0}^{n-1} \xi_n^{-i} \sigma^{i+1}(x) = \sum_{j=0}^{n-1} \xi_n^{-j+1} \sigma^j(x) = \xi_n \alpha \]
by substituting \( j = i + 1 \). (I think there is the implicit assumption that \( \alpha = \sum_{i=0}^{n-1} \xi_n^{-i} \sigma^i(x) \), which was omitted during lecture.) Then \( \sigma(\alpha) = \xi_n \alpha \), and \( \sigma^i(\alpha) = \xi_n^i \alpha \) are distinct for \( i = 0, 1, \ldots, n - 1 \). Then \( 1_F \) has at least \( n \) extensions \( \sigma^i : F(\alpha) \to L \), which implies \( [F(\alpha) : F] \geq n \). But \( [F(\alpha) : F] \leq [L : F] = n \), so that \( L = F(\alpha) \).

Then \( \sigma^i(\alpha^n) = \sigma^i(\alpha)^n = (\xi_n^i \alpha)^n = \alpha^n \). Then \( \alpha^n \in L^G = F \), and the extension is \( n \)-radical.

**Example 25.4.** Then \( F(\xi_n)/F \) is \( n \)-radical since \( (\xi_n)^n = 1 \in F \). This does not contradict the proposition since \( \xi_n \) are not in the ground field for \( F = \mathbb{Q} \).

A field extension \( L/F \) is called radical if there exists a tower
\[ F = F_0 \subset F_1 \subset \cdots \subset F_m = L \]
where \( F_{i+1}/F_i \) is \( n_i \)-radical for some \( n_i \) for \( 0 \leq i \leq m - 1 \). For example, if we have
\[ 5\sqrt[3]{\sqrt{2} + 5\sqrt{8} - 1} = \alpha \]
then adjoin \( \sqrt{2} \), then \( \sqrt{8} \), then \( \sqrt[3]{\sqrt{2} + 5\sqrt{8}} \), and finally \( \alpha \).

**Example 25.5.** Let \( F(\alpha_1, \ldots, \alpha_n)/F \) with \( \alpha_i^n \in F \) is radical.

We have the following properties:

1. Consider \( L/K/F \). If \( K/F \) and \( L/K \) are radical, then so is \( L/F \).

2. If \( L/F \) is radical, then so is \( KL/K \). For if \( \alpha^n \in F \subset K \), then \( F(\alpha)/F \) is radical, so \( KL = KF(\alpha) = K(\alpha) \) is radical over \( K \).

**Lemma 25.6.** Let \( K/F \) be a radical extension. Then there exists a normal radical extension \( L/F \) such that \( L \supseteq K \).
Proof. By definition, we have sequence

\[ F = F_0 \subset F_1 \subset \cdots \subset F_m = K \]

and every \( F_{i+1}/F_i \) is \( n_i \)-radical. By induction on \( m \). If \( m = 0 \), clear.

Suppose it holds for \( m - 1 \). Suppose \( K = F_m/F_{m-1} \). By induction, we can embed \( F_{m-1} \) into \( L \) where \( L/F \) is normal and radical. So \( L \) is a splitting field of some \( g \in F[X] \). Also, \( F_m/F_{m-1} \) is \( n \)-radical, so \( F_m = F_{m-1}(\alpha) \) where \( \alpha^n \in F_{m-1} \). Let \( f = m_\alpha \in F_{m-1}[X] \). Let \( G = \text{Gal}(L/F) \).

Set \( h = \prod_{\sigma \in G} \sigma(f) \in F[X] \), and \( h(\alpha) = 0 \). Let \( E \) be a splitting field of \( gh \) over \( F \) (over \( L \)). Then \( F_m = F_{m-1}(\alpha) \) which implies \( E/L \) is generated over \( L \) by all conjugates of \( \alpha \), i.e., \( E/F = L(\sigma\alpha)_{\sigma \in G} \). But \( \alpha^n \in F_{m-1} \in L \) implies \( (\sigma\alpha)^n \in L \). So \( E/L \) is radical, thus \( E/F \) is radical and normal.

However, \( f = m_\alpha \) is split in \( E \), so it has a root in \( E \), so there is a map \( K = F_{m-1}(\alpha) \to E \) over \( F_{m-1} \). So \( K \) is embedded into \( E \), which is radical and normal, as desired.

A nonconstant polynomial \( f \in F[X] \) is solvable by radicals if \( f \) is split in a radical extension of \( F \).

**Theorem 25.7.** A nonconstant polynomial \( f \in F[X] \) is solvable by radicals iff \( \text{Gal}(f) \) is solvable.

Suppose \( G \) is solvable with subnormal series

\[ G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}. \]

We have a tower of fields

\[ L^{G_n}/\cdots/L^{G_1}/L^{G_0}. \]

But \( L^{G_{i+1}}/L^{G_i} \) has Galois group \( G_i/G_{i+1} \), which is cyclic (equivalently abelian.)

We say \( f \) is solvable by radicals iff \( \text{Gal}(f) \) is solvable.

**Proof.** Suppose \( f \) is solvable. There exists \( E/F \) radical such that \( f \) is split over \( E \). Let \( L \subset E \) be a splitting field of \( f \). We may assume that \( E/F \) is normal. Also, \( E/F \) is a tower of \( n_i \)-radical extensions. Let \( n = \prod n_i \).

Set \( F' = F(\xi_n) \). Then set \( E' = E(\xi_n) = EF' \). Then \( E'/F' \) is radical, and \( \xi_n \in F' \), so that \( E'/F' \) is a tower of cyclic extensions since every \( n_i \)-radical field extension is cyclic.

Then \( \text{Gal}(E'/F') \) is solvable. Then \( \text{Gal}(F'/F) \) is abelian, hence solvable. So

\[ \text{Gal}(F'/F) \simeq \text{Gal}(E'/F')/\text{Gal}(E'/F') \]

where \( \text{Gal}(F'/F) \) and \( \text{Gal}(E'/F') \) are solvable. Then \( \text{Gal}(E'/F) \) is solvable. Then \( \text{Gal}(f) = \text{Gal}(L/F) \) is a factor group of \( \text{Gal}(E'/F) \) by \( \text{Gal}(E'/L) \), hence solvable.

Conversely, suppose \( G = \text{Gal}(f) \) is solvable. Let \( n = |G| \), and \( L/F \) be a splitting field of \( f \). Set \( F' = F(\xi_n) \) and \( L' = L(\xi_n) = LF' \). Then \( \text{Gal}(L'/F') \) embeds into \( G \), hence is solvable. So \( L'/F' \) is a tower of cyclic extensions. Each cyclic extension is \( n_i \)-radical for some \( n_i \). Then

\[ n_1 \mid [L':F'] \mid [L:F] = |G| = n \]

so \( L'/F' \) is radical. Thus \( L'/F \) is radical. So \( f \) is solvable by radicals.

**Example 25.8.**

1. Take any \( f \in F[X] \) of degree \( n \) with \( \text{Gal}(f) \simeq S_n \). We know \( S_n \) is not solvable if \( n \geq 5 \).

2. Let \( p \) be prime, \( f \in Q[x] \) be irreducible of degree \( p \). Suppose that \( f \) has exactly two nonreal roots.

I claim \( \text{Gal}(f) \simeq S_p \), hence not solvable if \( p \geq 5 \). Let \( L/F \) be a splitting field of \( f \), with \( \alpha \in L \). This implies \( p \mid [L:F] = |G| \), and \( G = \text{Gal}(L/F) = \text{Gal}(f) \) is embedded in \( S_p \). The \( G \) contains an element of order \( p \), hence \( G \) contains a \( p \)-cyclic.

Let \( \tau \in G \) be complex conjugation, a transposition. Then \( S_p \) is generated by \( \sigma \) and \( \tau \), hence \( G = S_p \). For example, take \( f = X^5 - 4X + 2 \).
26 Kummer Theory

Let $F$ be a field, and $n$ not divisible by $\text{char}(F)$. Let $a_1, \ldots, a_m \in F^\times$, and $\xi_n \in F$. Let $L$ be a splitting field of $(X^n - a_1) \cdots (X^n - a_m)$. Let $\alpha_i^n = a_i$, so that

$$L = F(a_1, \ldots, a_m) = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_m}).$$

What is $\text{Gal}(L/F) = G$?

Let $A \subset F^\times$ be generated by $a_1, \ldots, a_m$ and $(F^\times)^n$. Then $A/(F^\times)^n \subset F^\times/(F^\times)^n$ be a finite subgroup. We have a map

$$G \times (A/(F^\times)^n) \to \mu_n \subset F^\times : (\sigma, \bar{a}) \to \frac{\sigma(\alpha)}{\alpha} = (\sigma, \bar{a}).$$

Note $a_i \in (L^\times)^n$ implies $A \subset (L^\times)^n$, so $a = \alpha^n$ for some $\alpha \in L^\times$.

Also, if $a = \beta^n$ then $\beta = \xi \cdot \alpha$, where $\xi \in \mu_n \subset F^\times$. Then

$$\frac{\sigma(\beta)}{\beta} = \frac{\sigma(\xi) \sigma(\alpha)}{\xi} = 1.$$

but $\sigma(\xi)/\xi = 1$. Then

$$\left(\frac{\sigma(\alpha)}{\alpha}\right)^n = \frac{\sigma(\alpha^n)}{\alpha^n} = \frac{\sigma(\alpha)}{\alpha} = 1.$$

Then

$$\langle \sigma \tau, \bar{a} \rangle = \langle \sigma, \bar{a} \rangle \cdot \langle \tau, \bar{a} \rangle$$

and

$$\langle \sigma, \overline{ab} \rangle = \langle \sigma, \bar{a} \rangle \langle \sigma, \bar{b} \rangle.$$

Then

$$i : G \to \text{Hom}(A/(F^\times)^n, \mu_n) : \sigma \mapsto (\bar{a} \mapsto \langle \sigma, \bar{a} \rangle).$$

I claim $i$ is injective. Is $\sigma \in \ker(i)$, then $\langle \sigma, \bar{a} \rangle = 1$ for all $a \in A$. Then

$$\langle \sigma, \bar{a_i} \rangle = \frac{\sigma(\alpha_i)}{\alpha_i} = 1$$

for all $i$ so that $\sigma(\alpha_i) = \alpha_i$ for all $i$, so $\sigma = e$. Thus $G$ is abelian.

I now claim that if $C$ is finite abelian, and $C^n$, then

$$\text{Hom}(C, \mu_n) \simeq C.$$ 

Suppose $C$ be cyclic, with $|C| = k \mid n$. The elements of

$$\text{Hom}(C, \mu_n) = \{ \xi \in \mu_n : \xi^k = 1 \} = \mu_k \simeq C$$

since generators must map to elements with order dividing $k$.

**Theorem 26.1.** The map $i : G \to \text{Hom}(A/(F^\times)^n, \mu_n)$ is an isomorphism. In particular, $G \simeq A/(F^\times)^n$.

**Proof.** We have

$$A/(F^\times)^n \to \text{Hom}(G, \mu_n) : \bar{a} \mapsto (\sigma \mapsto \langle \sigma, \bar{a} \rangle)$$

is injective. But

$$|A/(F^\times)^n| \leq |\text{Hom}(G, \mu_n)| = |G|.$$

Since $i$ is injective,

$$|G| \leq |\text{Hom}(A/(F^\times)^n, \mu_n)| = |A/(F^\times)^n|$$

so $i$ is an isomorphism. \qed
Example 26.2. Let $p_1, \ldots, p_n$ be distinct primes. Consider $\text{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}) = G$? In this case $n = 2$. Note

$$Q^\times \simeq \mu_n \times \text{free abelian group generated by primes}$$

Then $Q^\times/(Q^\times)^2$ is a vector space over $\mathbb{F}_2$ with basis $-1$ and $\overline{p}$ for $p$ primes. Then $A/(Q^\times)^2$ subspace in $Q^\times/(Q^\times)^2$ spanned by $\overline{p}_1, \ldots, \overline{p}_m$. So that

$$A/(Q^\times)^2 \simeq \mathbb{Z}/(2) \cdots \mathbb{Z}/(2)$$

where we have $m$ factors on the RHS. This is the Galois group. So choosing $\epsilon_i = \pm 1$ for $i = 1, \ldots, m$ there exists $\sigma \in G$ with $\sigma(\sqrt{p_i}) = \epsilon_i \sqrt{p_i}$.