I. FIELD THEORY

We assume familiarity with the following concepts: ring, field, vector space, K-algebra, group, polynomial, integral domain.

Some Basics

Let F be a field. Then we have a ring homomorphism

$$\varphi: \mathbb{Z} \longrightarrow F \; ; \; \varphi(n) = n \cdot 1 := 1 + \cdots + 1 .$$

We have 2 cases

- If $\ker \varphi = \{0\}$, then we say that the characteristic of F is 0. We have a copy of $\mathbb{Z}$ in F; so we also have a copy of $\mathbb{Q}$ in F (why?). That subfield is called the prime field of F. Most of the times, we'll denote it as $\mathbb{Q}$.

- If $\ker \varphi \neq \{0\}$, than $\ker \varphi = n\mathbb{Z}$ for some $n \in \mathbb{N} - \{0\}$, and F has a copy of $\mathbb{Z}/n\mathbb{Z}$ in it. So $\mathbb{Z}/n\mathbb{Z}$ needs to be an integral domain. Hence n is a prime number; from now on, we'll write p rather than n. In this case we say that the characteristic of F is p and the copy of $\mathbb{F}_p (= \mathbb{Z}/p\mathbb{Z})$ in F is called the prime field of F.

To summarize: The subfield of F generated by 1 is called the prime field of F and it's isomorphic to either $\mathbb{Q}$ or $\mathbb{F}_p$

— o —

Instead of saying F is a subfield of E, we say F is an extension of F, and we talk about the extension E/F. If E/F is an extension, then E is an F-vector space, and its

dimension is called the degree of E over F and it's denoted by $[E:F]$. (This number is either a positive integer of the symbol ∞.)

Proposition: Let $E|F$ and $F|k$ be extensions. Then

$$[E:k] = [E:F] \cdot [F:k].$$

Proof: Let $\{\alpha_i\}_{i\in I}$ be a basis of E over F and let $\{\beta_j\}_{j\in J}$ be a basis of F over k. So $|I| = [E:F]$ and $|J| = [F:k]$

Then $\{\alpha_i\beta_j\}_{i\in I, j\in J}$ is a basis of E over k. (Why?) ∎

Corollary: $E|F$, $F|k$ extension. Then $E|k$ is finite iff both $E|F$ and $F|k$ are finite.

Definition: An extension $E|F$ is finite if $[E:F]$ is a positive integer.

Algebraic Extensions

Let $E|F$ be an extension and $\alpha \in E$. $F[\alpha]$ denotes the subring of E generated by $F\cup\{\alpha\}$; it is sometimes called the subring of E generated over F by α. It's elements are of the form $f(\alpha)$ where $f \in F[x]$. So we have an F-alg. homomorphism:

$$\varphi_\alpha : F[x] \longrightarrow E \;;\; \varphi_\alpha(f) = f(\alpha),$$

whose image is $F[\alpha]$.

If $\ker \varphi_\alpha = \{0\}$, then $F[\alpha] \simeq F[x]$.

If $\ker \varphi_\alpha \neq \{0\}$ then $\ker \varphi_\alpha = \langle f(x)\rangle$ where $f(x) \in F[x]\setminus\{0\}$, because $F[x]$ is a PID.

So we have a copy of $F[x]/\langle f(x)\rangle$ ($\cong F[\alpha]$) in E.
Hence $\langle f(x)\rangle$ is a prime ideal and so $f(x)$ is irreducible.
Note that this $f(x)$ is determined up to a non-zero constant; i.e
if $\ker \varphi_\alpha = \langle f\rangle = \langle g\rangle$ then $g(x) = c\cdot f(x)$ for some $c \in F^\times$.

By dividing the leading coefficient, we may assume that f is monic and such f is unique. That f is called the minimal polynomial of α over F. In this case, we say α is algebraic over F.

Note that $f(\alpha) = 0$; indeed $g(\alpha) = 0$ for every $g \in \ker \varphi_\alpha$.
Actually, α being algebraic over F can be characterized as being a zero of a non-zero polynomial in $F[x]$. The minimal polynomial is the polynomial of smallest degree among non-zero monic polynomials are of whose roots is α.

(Recall: $f(\alpha) = 0 \iff x-\alpha \mid f(x)$ (in some field).)

Definition: An extension $E|F$ is called algebraic if every $\alpha \in E$ is alg. over F.

Proposition: If $E|F$ is finite, then it is algebraic

Proof: Let $[E:F] = n$. & let $\alpha \in E$. Then $1, \alpha, \alpha^2, \dots, \alpha^n$ are linearly dependent over F; this means that α is algebraic over F. ∎

Let $E|F$ be an extension and let $\alpha \in E$. Then $F[x]$ is a subfield of E, so it is an integral domain and we can talk about its field of fractions. That field is a subfield of E generated by F & α, and it is denoted by $F(\alpha)$. It's elements are of the

form $\frac{f(x)}{g(x)}$ where $f, g \in F[x]$ and $g(x) \neq 0$.

Proposition: Let $E|F$ be an extension and let $\alpha \in E$ be algebraic over F. Then $F(\alpha) = F[\alpha]$, $F[\alpha]|F$ is finite, and the degree of the minimal polynomial of α over F is $[F[\alpha] : F]$.

Proof: Let $f(x) \in F[x]$ be the minimal polynomial of α over F; let $n = \deg f$.
If $g(x) \in F[x]$ is such that $g(\alpha) \neq 0$, then $f(x) \nmid g(x)$ in $F[x]$ and hence $k(x)f(x) + l(x)g(x) = 1$ for some $k, l \in F[x]$.
So $l(\alpha)g(\alpha) = 1$. This means that a non-zero element $g(\alpha)$ of $F[\alpha]$ has an inverse in $F[\alpha]$. So $F[\alpha] = F(\alpha)$.
Since $1, \alpha, \dots, \alpha^{n-1}$ are linearly independant over F, we have $[F[\alpha] : F] \geq n$. To show equality let $g(\alpha) \in F[\alpha]$ & divide $g(x)$ by $f(x)$: $g(x) = q(x) \cdot f(x) + r(x)$ where $0 \leq \deg r < n$.
So $g(\alpha) = r(\alpha)$ and $1, \alpha, \dots, \alpha^m$ can be used to write $g(\alpha)$.
Then $[F[\alpha] : F] = n$. ∎

Definition: $E|K$, $E|L$ extensions. $K \cdot L$ denotes the subfield of E generated by K and L, and it's called the compositum of K and L.

- Given $\alpha_1, \dots, \alpha_n \in E$, $K(\alpha_1, \dots, \alpha_n)$ is $K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$ (defined by induction on n).

• $E|F$ is called finitely generated if $E = F(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in E$.

Proposition: An extension $E|F$ is finite iff it is finitely generated and algebraic.

Proof: ($\Rightarrow$) Let $E|F$ be finite. Then it is algebraic. Let $\{\alpha_1, \dots, \alpha_n\}$ be a basis of E over F. Then $E = F\alpha_1 + \cdots + F\alpha_n = F(\alpha_1, \dots, \alpha_n)$; so $E|F$ is finitely generated as well.

($\Leftarrow$) Let $E = F(\alpha_1, \dots, \alpha_n)$. We also know that $\alpha_1, \dots, \alpha_n$ are algebraic over F. Then $F(\alpha_1)|F$ is finite and by induction (for any m) $F(\alpha_1, \dots, \alpha_m)|F(\alpha_1, \dots, \alpha_{m-1})$ is also finite. So $E = F(\alpha_1, \dots, \alpha_n)|F$ is finite. ∎

Proposition: (i) $E \subseteq F \subseteq L$. $L|E$ finite $\Leftrightarrow$ $L|F$ & $F|E$ are finite.

(ii) $k \subseteq E$, $k|F$. $E|k$ is finite $\Leftrightarrow$ $EF|F$ is finite.

(iii) Replace 'finite' with 'algebraic' in (i).

(iv) Replace 'finite' with 'algebraic' in (ii).

Proof: (i) Done already.

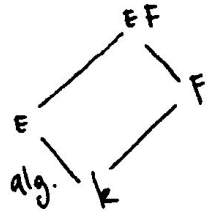
(ii) Let $E = k(\alpha_1, \dots, \alpha_n)$, $\alpha_1, \dots, \alpha_n \in EF$ are algebraic over k. Then $\alpha_1, \dots, \alpha_n$ are algebraic over F as well & $EF = F(\alpha_1, \dots, \alpha_n)$.

(iii) $\Rightarrow$ Clear.

$\Leftarrow$ $\begin{matrix} L \\ | \text{alg.} \\ F \\ | \text{alg.} \\ E \end{matrix}$ Let $\alpha \in L$; we need to show that α is algebraic over E. We know that α is algebraic over L; so $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ with $a_0, a_1, \dots, a_{n-1} \in L$.

Now $E(a_0, \dots, a_{n-1}) \mid E$ is algebraic and finitely generated. Then it is finite. So α is algebraic over E.

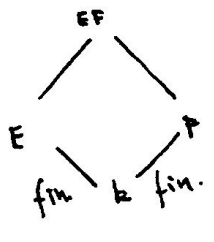
(iii)



We need to show that $EF \mid F$ is algebraic. So let $\alpha \in EF$. Then $\alpha \in F(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in E$. Consider $k(\alpha_1, \dots, \alpha_n) \mid k$. This extension is algebraic and finitely generated. In particular, $\alpha_1, \dots, \alpha_n$ are algebraic over k. So they are algebraic over F. So $F(\alpha_1, \dots, \alpha_n) \mid F$ is algebraic and ~~algebraic~~ finitely generated. So it is finite. So α is algebraic over F. ∎

Corollary: $F \mid k$ and $E \mid k$ are finite/algebraic, E, F contained in L. Then $EF \mid k$ is finite/algebraic.

Proof:



So $EF \mid F$ is finite & and $EF \mid E$ is finite (by (ii)).
So $EF \mid k$ is finite (by (i))
Exact the same proof works for 'algebraic'. ∎

Field Embeddings

Recall that non-constant field homomorphisms are injective; we deal with them and call them embeddings.

Let $E \mid F$ be an extension and $\sigma : F \to L$ be an embedding. An embedding $\tau : E \to L$ said to extend σ if $\tau \mid F = \sigma$.

$$\begin{array}{ccc} E & \xrightarrow{\tau} & L \\ \uparrow & & \uparrow \mathrm{id} \\ F & \xrightarrow{\sigma} & L \end{array}$$

If σ is the identity function on F, then we say τ is over F.

Proposition: $E|F$ an extension, $\tau: E \to L$ extends $\sigma: F \to L$, $f(x) \in F[x]$ and $\alpha \in E$ is a root of f. Then $\tau(\alpha)$ is a root of $\sigma(f) = f^\sigma$. (If $f = a_0 + a_1 x + \cdots + a_n x^n$, then $f^\sigma = \sigma(a_0) + \cdots + \sigma(a_n) x^n$)

Proof: $f^\sigma(\tau(\alpha)) = \sigma(a_0) + \sigma(a_1)\tau(\alpha) + \cdots + \sigma(a_n)\tau(\alpha)^n$

$= \tau(a_0 + a_1\alpha + \cdots + a_n\alpha^n) = \tau(f(\alpha)) = \tau(0) = 0$. ∎

Corollary: If $\sigma = id_F$ in the proposition above, then τ maps roots of f to roots of f.

Lemma: $E|F$ algebraic extension, $\sigma: E \to E$ is over F. Then σ is an automorphism.

Proof: All we need to show is that σ is surjective. So let $\beta \in E$. We need to find $\alpha \in E$ such that $\sigma(\alpha) = \beta$. Let $f(x) \in F[x]$ be the minimal polynomial of β & let E' be the field generated over F by the roots of f in E. So $E'|F$ is finite & $\sigma|_{E'}$ is an automorphism of E' over F. Thus there is a root α of f in E' mapping to β. ∎

Lemma: Let $E|E_1$, $E|E_2$ be extensions and $\sigma: E \to L$ an embedding. Then $\sigma(E_1 \cdot E_2) = \sigma(E_1) \cdot \sigma(E_2)$.

Proof: ....

Theorem (Kronecker): Let $f \in k[x]$ be nonconstant. Then k has an extension in which f has a root.

Proof: It suffices to prove this when f is irreducible. So $k[x]/\langle f\rangle$ is a field & we have an embedding of k into $k[x]/f$: $k \xrightarrow{\iota} k[x] \xrightarrow{\sigma} k[x]/\langle f\rangle$. This is an injective map because $\langle f\rangle$ doesn't contain any constants.

Let $\zeta = \sigma(x) \in k[x]/\langle f\rangle$. Then $f^\sigma(\zeta) = f^\sigma(x^\sigma) = \sigma(f(x)) = 0$

So ζ is a root of f^σ. Then $\sigma(k) \subseteq k[x]/\langle f\rangle$ is a subfield isomorphic to k. We think it as k and the extension $\sigma(k)(\zeta)$ contains a root of f^σ (which we think as f.) ☐

So we can 'close' k under roots of finitely many polynomials'. We'd like to close it under all roots of all polynomials.

Theorem: Any field k has an extension L that is algebraically closed: If $f \in L[x]$ is non-constant, then f has a root in L.)

Proof: Let $S = \{X_f : f \in k[x]\}$; a new variable for each polynomial in $k[x]$.

Let $R = k[S]$ and $I = \langle f(X_f) : f \in k[x]\rangle$. We claim that $I \neq R$. Otherwise $1 = g_1 f_1(X_{f_1}) + \cdots + g_m f_m(X_{f_m})$ for some $g_1, \ldots, g_m \in R$. Suppose $X_1, \ldots, X_N$ are all the variables involved in the equation above. Take $\in k$ containing roots of $f_1, \ldots, f_m$; say $\alpha_1, \ldots, \alpha_m$. For other variables let x_j be 0. Then

$1 = g_1(\vec{x}) f_1(\alpha_1) + \cdots + g_m(\vec{x}) f_m(\alpha_m) = 0$; a contradiction.

So $I \neq R$ and let $m \supseteq I$ be a maximal ideal containing I.

Then $E_1 := R/m$ is a field, containing a copy of k, and it contains ~~all the~~ roots of each $f \in k[x]$.

Apply the same procedure with E_1 in the place of k to get E_2, and in general E_{i+1} in to place of E_i. This way we get $E = \bigcup_{i=1}^{\infty} E_i$ which is an algebraically closed field containing k.

Corollary: For any field k, there is an algebraic extension $\overline{k}$ of k that is algebraically closed.

Proof: Let E/k be as in the theorem, and let $\overline{k}$ be the union of all $L \subseteq E$ that are algebraic extensions of k. Clearly, $\overline{k}$ is an algebraic extension of k.

Note that if $\alpha \in E$ is algebraic over $\overline{k}$, then α is alg. over k. If $f \in \overline{k}[x] \setminus \overline{k}$ & $\alpha \in E$ ~~then~~ is a root of f then α is algebraic over k. So $k(\alpha) \subseteq \overline{k}$ and $\alpha \in \overline{k}$. ∎

Definition: $\overline{k}$ as in the corollary above is called the algebraic closure of k. (We don't know uniqueness yet.)

Proposition: Let E/k be an extension and $\alpha \in E$ be algebraic over k, let L be an algebraically closed field & $\sigma : k \to L$ an embedding. Then there are as many extensions of σ to $k(\alpha)$ as the number of distinct roots of the minimal polynomial of α (over k).

Proof: Let $f \in k[x]$ be the minimal polynomial of α, and let $\beta \in L$ be a root of f^σ in L. We can define $\tau_\beta : k(\alpha) \to L$ by sending $g(\alpha)$ to $g^\sigma(\beta)$. (Why is this independent of g?) Such τ_β is an extension of σ to $k(\alpha)$. For another root β' of f^σ

$\tau_{\beta'} \neq \tau_\beta$. So we have at least number of distinct roots (in L) of f many extensions. Since α should be mapped to a root of f^σ, these are all the possibilities. ∎

Later we'll consider the number of extensions of embeddings to finite extensions.

Theorem: $E|k$ algebraic, $\sigma: k \to L$ embedding, L algebraically closed. Then σ extends to an embedding of E into L. If L is algebraic over σk & E is algebraically closed, then that extension is an isomorphism of E and L.

Proof: Let $S = \{\tau : F \to L \;;\; k \subseteq F \subseteq E,\ \tau|_k = \sigma\}$. Then S is non-empty as $\sigma \in S$ and it can be ordered by "extension". It is closed under chains; so it has a maximal element by Zorn's Lemma. Call this maximal element $\bar{\tau}: F \to L$. We claim that $F = E$. Indeed, if $\alpha \in E \setminus F$, then by the previous proposition τ can be extended to $F(\alpha)$, contradicting the maximality.

For the second part, assume E is algebraically closed and $L|\sigma k$ algebraic. So $\tau E \subseteq L$ is also algebraically closed. If $\alpha \in L$, then α is algebraic over τE; so it is in τE. Thus $L = \tau E$. ∎

Taking σ as id_k, we see that the algebraic closure $\bar{k}$ of k is unique up-to isomorphism. (So we'll start to call $\bar{k}$ as the algebraic closure.)

Normal Extensions

Definition: Let $f \in k[x]$ be non-constant. A splitting field of f is a field extension K of k that is generated over k by all the roots of f in K. That is: $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ where $\alpha_1, \ldots, \alpha_n \in K$ and $K = k(\alpha_1, \ldots, \alpha_n)$. Splitting fields exist since we may take roots in a fixed algebraic closure of k.

Proposition: Let $f \in k[x]$, and E and F are splitting fields of f. Then E and F are isomorphic over k.

Proof: Embed E into $\overline{F}$ over k: $\sigma : E \to \overline{F}$. We claim that σ is an isomorphism of E and F.

Suppose $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n) = c(x-\beta_1)\cdots(x-\beta_n)$ where $\alpha_1, \ldots, \alpha_n \in E$, $\beta_1, \ldots, \beta_n \in F$, and $E = k(\alpha_1, \ldots, \alpha_n)$, $F = k(\beta_1, \ldots, \beta_n)$.

As $\sigma|_k = id_k$, we have $f^\sigma(x) = f(x)$. So $(x-\sigma(\alpha_1))\cdots(x-\sigma(\alpha_n))$ equals $(x-\beta_1)\cdots(x-\beta_n)$. Hence each $\sigma(\alpha_i)$ equals one of β_j's. As a result $\sigma E \subseteq F$. But $F \subseteq \sigma E$ is also clear. Thus $\sigma : E \to F$ is an isomorphism over k. ∎

We may define a splitting field of a family $\{f_i \in k[x] : i \in I\}$ of polynomials in a similar way. (It might be the case that it's an infinite extension.) Existence and uniqueness of splitting fields of families can be shown similarly as well.

Theorem: $K|k$ an algebraic extension; $K \subseteq \overline{k}$. Then TFAE:

(i) K is the splitting field of a family of polynomials in $k[x]$.

(ii) Every embedding of K into $\overline{k}$ over k is an automorphism.

(iii) If $f \in k[x]$ is irreducible and has a root in K, then K contains all the roots of f (in $\overline{k}$).

Proof: (2 ⇒ 3) Let $f \in k[x]$ be irreducible and $\alpha \in K$ be a root of f. (So f is the minimal polynomial of α over k.) Let $\beta \in \bar{k}$ be another root of f (in $\bar{k}$). We would like to show that $\beta \in K$.

We know that there is an embedding of $k(\alpha)$ into $\bar{k}$ by sending α to β, ~~and we can~~ extend that embedding to an embedding of K into $\bar{k}$. By assumption that embedding is an automorphism. So $\beta \in K$.

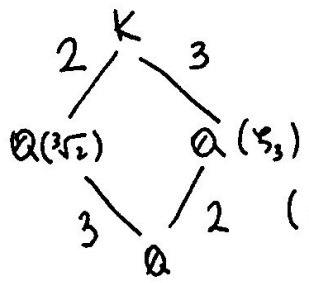
(3 ⇒ 1) The argument above shows that K is the splitting field of the collection of $f(x) \in k[x]$: f has a root in K & f is irreducible in $k[x]$.

(1 ⇒ 2) Let K be the splitting field of $\{f_i \in k[x] : i \in I\}$. An embedding of K into $\bar{k}$ is determined by where roots of f_i are mapped. Since all the roots are in K, any embedding of K into $\bar{k}$ is into K. By an earlier lemma they are actually automorphisms. ∎

Definition: If an algebraic extension K/k satisfies one of the conditions of the theorem above, we say that it is a normal extension.

Example: Let $k = \mathbb{Q}$ and $f(x) = x^3 - 2$. Then f is irreducible in $\mathbb{Q}[x]$. The roots of f in $\mathbb{C}$ (or $\bar{\mathbb{Q}}$) are $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$, $\sqrt[3]{2}\zeta_3^2$ where $\zeta_3 = e^{2\pi i/3}$.

So $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2)$ is the splitting field of f. However, K can be obtained as $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.



(ζ_3 minimal polynomial of ζ_3 is x^2+x+1.)

Note that $K|\mathbb{Q}(\sqrt[3]{2})$ and $K|\mathbb{Q}(\zeta_3)$ are normal, but $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ is not.

$\mathbb{Q}(\zeta_3)|\mathbb{Q}$ is also normal, because the other root of x^2+x+1 is ζ_3^2.

Proposition: ① $E|k$ a normal extension, $F|k$ any extension. Then $EF|F$ is normal

② $E|F$, $F|k$ extensions. If $E|k$ is normal, then $E|F$ is normal.

③ $K_1|k$, $K_2|k$ normal extension, then $K_1\cdot K_2|k$ are normal. and $K_1\cap K_2|k$

Proof: ① We may assume that $\bar{k}\subseteq\bar{F}$ (why?). As $E\subseteq\bar{k}$, we have $E\subseteq\bar{F}$.

Let σ be an embedding of EF into $\bar{F}$ over F. Then $\sigma|_E$ is an embedding of E into $\bar{k}$ (why not $\bar{F}$?) So $\sigma|_E$ is an automorphism of E. Thus $\sigma(EF)=\sigma(E)\sigma(F)=E\cdot F$. Thus $EF|F$ is normal.

② Clear. (E is the splitting field of the same polynomials.)

③ If σ is an embedding of $K_1\cdot K_2$ into $\bar{k}$ over k_1 then $\sigma|_{K_1}$ and $\sigma|_{K_2}$ are automorphisms. Thus $\sigma(K_1K_2)=\sigma(K_1)\cdot\sigma(K_2)$ $=K_1\cdot K_2$.

So $K_1K_2|k$ is normal.

Note that $\sigma(K_1\cap K_2)=\sigma(K_1)\cap\sigma(K_2)$. So easily $K_1\cap K_2|k$ is normal. ∎

Separable Extensions

Let $E|F$ be an algebraic extension & let $\sigma: F \to L$ be an embedding where $\overline{L} = L$. (We may also assume $\overline{\sigma F} = L$)

Let $S(\sigma, E) = \{\tilde{\sigma} : E \to L \text{ over } \sigma\}$.

We know that $S(\sigma, E) \neq \emptyset$ and if $E = F(\alpha)$, then $|S(\sigma, E)|$ is the number of distinct roots of the minimal polynomial of α over F.

Now let $\tau : F \to L'$ be another embedding. Then there is a bijection between $S(\sigma; E)$ and $S(\tau, E)$ as follows: There is an isomorphism $\lambda : L \to L'$ extending $\tau \circ \sigma^{-1} : \sigma(F) \xrightarrow{\sim} \tau(F)$.

Given $\tilde{\sigma} \in S(\sigma, E)$, the embedding $\lambda \circ \tilde{\sigma}$ is an extension of τ to E. So $\lambda \circ \tilde{\sigma} \in S(\tau, E)$. It's easy to see that $\tilde{\sigma} \mapsto \lambda \circ \tilde{\sigma}$ is a bijection using the fact that λ is an isomorphism.

Hence the following definition makes sense:

$$[E:F]_s := |S(\sigma, E)| \cdot \left[\text{We may indeed take } \sigma : F \to \overline{F} \text{ to be the identity.}\right]$$

$[E:F]_s$ is called the **separable degree** of E over F. It can be infinite.

Proposition: Let $E|F$ and $F|k$ be algebraic extensions. Then $[E:F]_s [F:k]_s = [E:k]_s$. Also if $E|k$ is finite, then $[E:k]_s \leq [E:k]$.

Proof: Let $\sigma : k \to L$ be an embedding. (WMA $L = \overline{k} = \overline{E} = \overline{F}$.) First note that each $\tilde{\sigma} \in S(E, \sigma)$ is an extension of $\tilde{\sigma}|_F \in S(F, \sigma)$. Since each $\tau \in S(F, \sigma)$ can be extended to $\tilde{\tau} \in S(E, \tau)$ in $[E:F]_s$ many ways, we get $[E:k]_s = [E:F]_s [F:k]_s$.

For the second part, let $E|k$ be finite and $E = k(\alpha_1, \ldots, \alpha_n)$.

Put $E_0 = k$ and $E_{i+1} = E_i(\alpha_{i+1})$. Then we know that $[E_{i+1} : E_i]_{sep} = \#$ of roots of f_{i+1} in E_{i+1} ($f_{i+1} \in E_i[x]$ min. pol. of α_{i+1}) $\leq [E_{i+1} : E_i]$ ($= \deg \alpha_{i+1}$ over E_i)

So $[E:k]_s = [E_n : E_0]_s = [E_n : E_{n-1}]_s \cdots [E_1 : E_0]_s \leq [E_n : E_{n-1}] \cdots [E_1 : E_0] = [E:k]$. ∎

If we have $E|F$ & $F|k$ finite extensions, then $[E:k]_s = [E:k]$ iff $[E:F]_s = [E:F]$ and $[F:k]_s = [F:k]$.

Definition: A finite extension $E|k$ is called separable if $[E:k]_s = [E:k]$.

- An element α that is algebraic over k is separable if $k(\alpha)|k$ is separable.
- A polynomial $f(x) \in k[x]$ is separable if it has no multiple roots (in $\bar{k}$).

Note that an algebraic (over k) $\alpha \in E$ is separable iff it's minimal polynomial over k is separable.

Proposition: $E|k$ finite. Then $E|k$ is separable iff each $\alpha \in E$ is separable over k.

Proof: ($\Rightarrow$) Let $\alpha \in E$. $E|k(\alpha)$ & $k(\alpha)|k$ are separable if $E|k$ is separable. As a result $k(\alpha)|k$ is separable, which is what's desired.

($\Leftarrow$) $E = k(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are separable over k. So $E|k$ is separable. ∎

A -possibly infinite- algebraic extension $E|k$ is separable if each $\alpha \in E$ is separable over k. By the proposition above, this means that away for finitely generated $k \subseteq F \subseteq E$, we have $F|k$ is separable.

Proposition: ① $k \subseteq F \subseteq E$ fields. $E|k$ is separable iff $E|F$ and $F|k$ are separable.

② $E|k$ separable, $F|k$ arbitrary. Then $EF|F$ is separable.

Proof: ① Suppose $E|k$ is separable. Let $\alpha \in E$. Then the minimal polynomial f of α over k is separable. If g is the minimal polynomial of α over F, then $g|f$; hence g doesn't have multiple roots either, and $E|F$ is separable. $F|k$ being separable is clear.

Now suppose $E|F$ and $F|k$ are separable. Let $\alpha \in E$ and f be the minimal polynomial of α over F. Let $K|k$ be finite such that $f \in K[x]$. Then $K|k$ is separable. Also $K(\alpha)|K$ is separable. Thus α is separable over k. ∎

② Note that $EF = F(\alpha : \alpha \in E)$ and each $\alpha^{\in E}$ is separable over k, hence over F. We get that $EF|F$ is separable. ∎

Normal Closure

Let $E|k$ be a finite extension; as usual assume $E = \overline{k}$. Consider the intersection of all $E \subseteq K' \subseteq E$ such that $K'|k$ is normal. This is a field extension of E and it is normal over k. This extension $K|k$ is called the normal closure of $E|k$.

We may describe K in terms of embeddings of E over k into $\overline{E}$: let $\sigma_1, \dots, \sigma_n$ be those embeddings. Then $K = \sigma_1(E) \cdots \sigma_n(E)$. (WHY?)

If $E|k$ is separable, then so is $K|k$; because we're adding the missing roots in E, so no new minimal polynomials.

Definition: Let k be a field and fix an algebraic closure $\overline{k}$. The separable closure of k is the compositum of all (finite) separable extensions of k in $\overline{k}$; denoted as k^{sep}. (Clearly, $k^{sep}|k$ is separable.)

Theorem (Primitive Element Theorem). Let $E|k$ be finite separable. Then $E = k(\alpha)$ for some $\alpha \in E$.

Proof: If k is finite, then so is E. As a result $E^\times = \langle \alpha \rangle$, as a group. But then $k(\alpha) = E$. (WHY?)

So suppose k is infinite, and let $\sigma_1, \dots, \sigma_n$ be all the embeddings of E over k in $\overline{k}$. By induction, we may assume $E = k(\alpha, \beta)$.

Consider $P(X) := \prod_{i \neq j} [(\sigma_i \alpha - \sigma_j \alpha) + (\sigma_i \beta - \sigma_j \beta) X]$.

If $P(X) \equiv 0$, then $\sigma_i = \sigma_j$ for some $i \neq j$. So $P(X) \not\equiv 0$ & there is $c \in k$ s.t. $P(c) \neq 0$. This means $\sigma_i(\alpha + c\beta) \neq \sigma_j(\alpha + c\beta)$ for $i \neq j$. (k is infinite!)

Then $k(\alpha + c\beta)$ has at least n different embeddings over k in $\overline{k}$. This means $[k(\alpha + c\beta) : k]_s = [k(\alpha + c\beta) : k] \geq n = [E : k]$.

So $E = k(\alpha + c\beta)$. ∎

One may prove the following: $E|k$ finite.

$E = k(\alpha)$ for some $\alpha \in E$ $\iff$ there are only finitely many intermediate fields: $k \subseteq F \subseteq E$.

If $E = k(\alpha)$, then we say that α is a primitive element of E over k.

Proposition: If k is of characteristic 0, then any algebraic $E|k$ is separable.

Proof: Let $\alpha \in E$ and $f(x)$ be the minimal polynomial of E over k. We'd like to show that f is separable; in other words that it doesn't

have repeated roots.

So let $f(X) = (X-\alpha_1)\cdots(X-\alpha_n)$ where $\alpha_1, \dots, \alpha_n \in \overline{k}$.

Then the formal derivative of f is $f'(X) = \sum_{i=1}^{n} (X-\alpha_1)\cdots\widehat{(X-\alpha_i)}\cdots(X-\alpha_n)$

If f has a repeated root / say $\alpha_i = \alpha_j$ then $f'(\alpha_i) = 0$. Then $f' \equiv 0$, otherwise $\deg f' < \deg f$ a contradiction. But $f'(X) = nX^{n-1} + \cdots$ and $n > 0$; so $f'(X) \not\equiv 0$. Then f has no repeated roots. ∎

The argument above shows that a polynomial (not necessarily irreducible) is separable if and only if $\gcd(f, f') = 1$.

Finite fields

One finite field we know is $\mathbb{Z}/p\mathbb{Z}$ and we'll denote it as $\mathbb{F}_p$.

If F is a finite field, then it has to be of positive characteristic, say p. Then F is an $\mathbb{F}_p$-vector space of finite dimension, say n. Then $|F| = p^n$. But are there always a field of cardinality p^n?

Fix an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. Then the polynomial $X^{p^n-1} - 1$ is ~~irreducible and~~ separable over $\mathbb{F}_p$, and has precisely $p^n - 1$ many roots in $\overline{\mathbb{F}}_p$. The polynomial $X^{p^n} - X$ has p^n many roots & they are all distinct, and they form a field. So the splitting field of $X^{p^n} - X$ in $\overline{\mathbb{F}}_p$ is a field with p^n elements.

To summarize: there is one and only one field with p^n elements in a fixed algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$; say $\mathbb{F}_{p^n}$. Also $\mathbb{F}_{p^n} / \mathbb{F}_p$ is normal & separable.

Now consider $\mathbb{F}_{p^m}$ & $\mathbb{F}_{p^n}$. When is it the case that $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$? At least, we need $|p^n| = |\mathbb{F}_{p^n}| = (p^m)^{[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]} = p^{m[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]}$.

As a result $m \mid n$. This is also sufficient, because then $X^{p^m} - X \mid X^{p^n} - X$.

It follows that $\alpha^{p^n} = \alpha$ for any $\alpha \in \mathbb{F}_p$.

Consider $\varphi_n : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $\alpha \longmapsto \alpha^p$. Then φ is a field homomorphism, hence it is injective; being an automorphism of a finite field, it is also surjective.

Actually, $\varphi : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$, $\alpha \longmapsto \alpha^p$ is an automorphism, and $\varphi_n = \varphi \restriction_{\mathbb{F}_{p^n}}$.

(We'll drop the n in φ_n from now on.)

This automorphism is called the Frobenius automorphism.

It is easy to see that φ^n is identity on $\mathbb{F}_{p^n}$; moreover $\mathrm{Aut}(\mathbb{F}_{p^n}) = \langle \varphi \rangle \simeq \mathbb{Z}/n\mathbb{Z}$.

Characteristic p

We have seen above that inseparable extension can only happen in positive characteristic. So let p be a prime number and $\mathrm{char}(k) = p$. Also let $\alpha \in \bar{k}$ with minimal polynomial $f(X) \in k[X]$. We know that f is not separable if and only if f and f' have a common root. This means that $f' \equiv 0$. It follows that α is not separable if and only if $f(X) = g(X^p)$ for some $g \in k[X]$.

Let $f(X) = (X-\alpha)^m h(X)$ in $\bar{k}[X]$, where $h(\alpha) \neq 0$. This m is called the multiplicity of α (over k).

We claim that multiplicities of conjugates of α (over k) are also m: Let $f(\beta) = 0$. Then there is an isomorphism $\sigma : k(\alpha) \xrightarrow{\sim} k(\beta)$ over k. Hence $f^\sigma = f$ & mult. of β is also m.

If $\alpha_1, \dots, \alpha_s$ are roots of f, then $\alpha_1^p, \dots, \alpha_s^p$ are roots of g.

If g is separable, then $[k(\alpha^p):k]_s = [k(\alpha^p):k] = \text{degree of } g = \frac{\text{degree of } f}{p}$

So $[k(\alpha):k] = p[k(\alpha^p):k]_s = p[k(\alpha^p):k] = \frac{[k(\alpha):k]}{p}$

On the other hand, the minimal polynomial of α over $k(\alpha^p)$ is $X^p - \alpha^p$. (Why is this irreducible?) Since α is the only root of $X^p - \alpha^p$, we get $[k(\alpha):k(\alpha^p)]_s = 1$. So $[k(\alpha):k]_s = [k(\alpha^p):k]$

As a result, we get $[k(\alpha):k] = p[k(\alpha):k]_s$.

If g is not separable, then $g(X) = h(X^p)$ for some $h \in k[X]$.

Continuing this way, we get that $[k(\alpha):k] = p^\mu [k(\alpha):k]_s$, for some $\mu \in \mathbb{N}$. ($\mu = 0$ case corresponds to α being separable).

It follows that α^{p^μ} is separable. ($f(X) = g(X^{p^\mu})$ for some separable polynomial $g \in k[X]$.)

Consequently, we have $[k(\alpha):k]_s \mid [k(\alpha):k]$. We call p^μ as the degree of inseparability of α over k.

If $E|k$ is finite, then $[E:k] = p^\mu [E:k]_s$ (Again p^μ is called the degree of inseparability of the extension $E|k$ and it is denoted as $[E:k]_i$.)

$[E:k]_i = 1 \iff E|k$ separable.

The other extreme is $[E:k]_i = [E:k]$; i.e $[E:k]_s = 1$. That case is called purely inseparable.

Note that if α is purely inseparable over k (i.e $[k(\alpha):k]_i = [k(\alpha):k]$) (11) if and only if its minimal polynomial over k is of the form $X^{p^n} - a$. ($a \in k$)

Proposition: ① $k \subseteq F \subseteq E$ fields. Then $E|k$ is purely inseparable if and only if $E|F$ and $F|k$ are purely inseparable.

② If $E|k$ is purely inseparable and $F|k$ any extension, then $EF|F$ is purely inseparable.

Proof: ...

Let's give the following definition to be used later.

Definition: A field k of characteristic p is called perfect if $k^p = k$. (This is to say that the Frobenius map is surjective.)

— ∘ —

Galois Correspondence

Definition: An algebraic extension $E|k$ is called Galois if it is both normal and separable.

- If $E|k$ is Galois, then we define the Galois group of the extension to be $Gal(K/k) := \{\sigma : K \to K : \text{automorphism over } k\}$.

Assuming $\bar{k} = \bar{K}$, normality gives us: $Gal(K/k) = \{\sigma : K \to \bar{K} \overset{\text{emb.}}{\text{over}} k\}$.

- An intermediate field of an extension $E|k$ is a field $L \subseteq E$ containing k.

· If $G \leq \mathrm{Aut}(k)$, then $K^G := \{\alpha \in K : \sigma(\alpha) = \alpha \text{ for every } \sigma \in G\}$ is called the fixed field of G.

Note that if $G = \mathrm{Gal}(K/k)$ for some Galois extension K/k, then $K^G = k$. (why? $K^G \supseteq k$ is not clear.) More generally if $H \leq G$, then K^H is an intermediate field of K/k.

Conversely, if F is an intermediate field of K/k, then K/F is Galois and $\mathrm{Gal}(K/F) \leq \mathrm{Gal}(K/k)$.

We are aiming to show that this gives a correspondence between intermediate fields of K/k and subgroups of $\mathrm{Gal}(K/k)$, provided that K/k is finite Galois.

Let's prove the injectivity of one side:

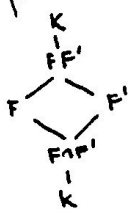
Proposition: K/k a Galois extension. If F, F' are intermediate fields of K/k such that $\mathrm{Gal}(K/F) = \mathrm{Gal}(K/F')$, then $F = F'$. (Note that we know that K/F and K/F' are Galois.)

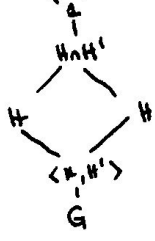
Proof: Let $G_1 = \mathrm{Gal}(K/F) = \mathrm{Gal}(K/F')$. Then $F = K^{G_1} = F'$. ∎

It follows that if F, F' are intermediate fields of K/k with $H = \mathrm{Gal}(K/F)$ and $H' = \mathrm{Gal}(K/F')$, then $\mathrm{Gal}(K/FF') = H \cap H'$. (WHY?)

Also, $\mathrm{Gal}(K/F \cap F') = \langle H, H' \rangle$ (= subgroup of G generated by H and H').

It follows that $F \subseteq F'$ iff $H' \subseteq H$.





& order reversing.

If E/k is finite and separable, then the normal closure K is Galois over k (K finite). There are only finitely many subgroups of $\mathrm{Gal}(K/k)$; so there are only finitely many subfields of E containing k.

5th Lecture

Theorem (Artin): Let $G \leq \mathrm{Aut}(K)$ be finite; say $|G| = n$, and let $k = K^G$. Then K/k is finite Galois with Galois group G.

First, a lemma.

Lemma: E/k separable. Suppose that each $\alpha \in E$ is of degree $\leq n$ over k. Then E/k is finite of degree at most n.

Proof: Take $\alpha \in E$ that has maximal degree over k; say $[k(\alpha):k] = m \leq n$. Suppose $k(\alpha) \neq E$, then take $\beta \in E \setminus k(\alpha)$. By primitive element theorem $k(\alpha,\beta)$ is $k(\gamma)$ for a single γ. Then $[k(\gamma):k] = [k(\alpha,\beta):k] > m$, which contradicts with maximality of m. So $E = k(\alpha)$ and $[E:k] = m \leq n$. ∎

Proof of Artin's Theorem: Let $\alpha \in K$. We'll show that $k(\alpha)/k$ is Galois of degree at most n. This will finish the proof using the lemma above.

Let $\sigma_1, \dots, \sigma_m \in G$ be maximal such that $\{\sigma_1\alpha, \dots, \sigma_m\alpha\}$ has m elements.

Note that if $\tau \in G$, then $\{\tau\sigma_1\alpha, \dots, \tau\sigma_m\alpha\} = \{\sigma_1\alpha, \dots, \sigma_m\alpha\}$ (why?)

In particular, $\alpha = \sigma_i\alpha$ for some i, and α is a root of $f(X) = \prod_{i=1}^{m}(X - \sigma_i\alpha)$. We have $f^\tau = f$ for any $\tau \in G$; hence $f(X) \in K^G[X]$. Clearly, f is separable over k and splits into linear polynomials in K. Hence K/k is Galois and each $\alpha \in K$ has degree at most n, as desired. ∎

(How about $G = \mathrm{Gal}(K/K^G)$? (cardinality argument))

This proof doesn't work if G is infinite: How do we choose a maximal set as in the proof.

If K/k is finite Galois with $G = \mathrm{Gal}(K/k)$, then for any $H \leq G$, K is Galois over the intermediate field K^H. By Artin's theorem, we know that $\mathrm{Gal}(K/K^H) = H$. Also, if $K^H = K^{H'}$, then $H = H'$.

This concludes the "Galois correspondence" for finite Galois extensions.

Galois groups are invariant under isomorphisms:

$$\begin{array}{ccc} K & \xrightarrow{\sim} & L \\ | & & | \\ k & \xrightarrow{\sim} & \sigma k \\ & & \| \\ & & \ell \end{array} \qquad \begin{array}{ccc} \mathrm{Gal}(K/k) & \longrightarrow & \mathrm{Gal}(L/\ell) \\ \tau & \longmapsto & \sigma \circ \tau \circ \sigma^{-1} \end{array}$$

This is an isomorphism of groups.

Theorem: K/k Galois, $G = \mathrm{Gal}(K/k)$, F intermediate field, $H = \mathrm{Gal}(K/F)$

① F/k is Galois $\Leftrightarrow$ $H \lhd G$.

② If F/k is normal, then $\begin{array}{ccc} G & \longrightarrow & \mathrm{Gal}(F/k) \\ \sigma & \longmapsto & \sigma|_F \end{array}$ is a surjective group homomorphism with kernel H.

(So $\mathrm{Gal}(F/k) \simeq G/H$.)

Proof: ① ($\Rightarrow$) Suppose F/k is Galois, with $G' = \mathrm{Gal}(F/k)$. Then $\varphi: \begin{array}{ccc} G & \longrightarrow & G' \\ \sigma & \longmapsto & \sigma|_F \end{array}$ is a group homomorphism with kernel H. So $H \lhd G$.

($\Leftarrow$) Suppose that F/k is not normal. Then there is $\sigma: F \hookrightarrow K$ over k such that $\sigma F \neq F$. We may extend σ to K, an element of G. Now $\mathrm{Gal}(K/\sigma F) = \sigma\,\mathrm{Gal}(K/F)\,\sigma^{-1} = H^\sigma$, but $H^\sigma \neq H$. So H is not normal in G.

② All we need is the surjectivity: Let $\tau \in G'$. Then τ extends to K. Then τ is the image of that extension (under φ). ∎

Proposition: let $K|k$ be (finite) Galois with $G = Gal(K/k)$, and let $F|k$ be any such that $K \cdot F$ exists.

(1) $FK|F$ and $K|F \cap K$ are Galois; let $H = Gal(FK/F)$, $H' = Gal(K/K\cap F)$

(2) Let $\varphi : H \longrightarrow G$, $\sigma \longmapsto \sigma|_K$. Then φ is an injective group homomorphism with $\mathrm{Im}\,\varphi = H'$.

(So $H \simeq H'$.)

(3) $[KF:F] \mid [K:k]$.

Proof: We shall assume that $K|k$ is finite; the infinite case is correct, but its proof requires some less elementary tools.

(1) Done earlier.

(2) It is clear that φ is a homomorphism. If $\sigma \in \ker\varphi$, then $\sigma|_K = \mathrm{id}_K$. So σ is identity on $K \cdot F$ & φ is injective.

If $\sigma \in \mathrm{Im}\,\varphi$, then σ fixes $K\cap F$, and $K\cap F \subseteq K^{\mathrm{Im}\varphi}$. Suppose $\alpha \in K^{\mathrm{Im}\varphi}$; so $\sigma(\alpha) = \alpha$ for any $\sigma \in \mathrm{Im}\varphi$. Such σ are of the form $\tau|_K$ for some $\tau \in H$. So elements of H also fix α & $\alpha \in (KF)^H = F$. This shows $K^{\mathrm{Im}\varphi} \subseteq K\cap F$ and $K^{\mathrm{Im}\varphi} = K\cap F = K^{H'}$. So $\mathrm{Im}\,\varphi = H'$. (Last step uses finiteness.)

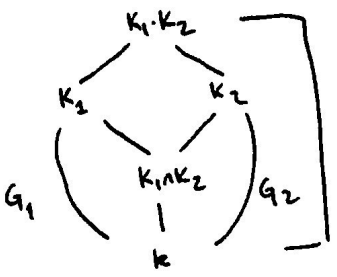
(3) $[KF:F] = |H| = |H'|\,\big||G| = [K:k]$. ∎

Proposition: let $K_1|k$ and $K_2|k$ be Galois with $G_1 = Gal(K_1/k)$, $G_2 = Gal(K_2|k)$. Suppose $K_1 \cdot K_2$ exists.

(1) $K_1 \cdot K_2 | k$ is Galois; say $G = Gal(K_1K_2/k)$.

(2) $\varphi : G \longrightarrow G_1 \times G_2$, $\sigma \longmapsto (\sigma|_{K_1}, \sigma|_{K_2})$ is an inj. group homomorphism.

(3) If $K_1 \cap K_2 = k$, then φ is surjective.



Proof: ① is done before.

② If σ is an automorphism of $K_1 \cdot K_2$, then $\sigma|_{K_1}$ and $\sigma|_{K_2}$ determine σ. So φ is injective.

③ Kernel of φ is automorphisms σ of $K_1 \cdot K_2$ fixing K_1 and K_2. So if $K_1 \cap K_2 = k$, then $G_1 \cong Gal(K_1 \cdot K_2 / K_1)$ and $G_2 \cong Gal(K_1 K_2 / K_2)$ and φ is surjective. ∎

Quadratic Extensions: Let $[K:k] = 2$. Say $K = k + k\alpha$. Then $K = k(\alpha)$ where α is the root of a degree two polynomial; say $f(X) = X^2 + aX + b$. Suppose $\mathrm{char}(k) \neq 2$. Then $f(X) = \left(X - \frac{a}{2}\right)^2 - \left(\frac{a^2}{4} - b\right)$. Let $\beta = \alpha - \frac{a}{2}$.

Then $\beta^2 = \frac{a^2}{4} - b \in k$ and $K = k(\alpha) = k(\beta)$.

So K is generated over k by a square root of an element of k.

Thus, at least in characteristic not equal to 2 case, quadratic extensions are of the form $K = k(\sqrt{A})$ where A is a non-square in k.

(What happens in characteristic 2?)

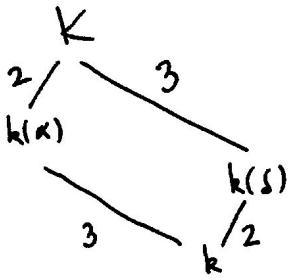
Cubic Extensions: Assume $\mathrm{char}(k) \neq 2, 3$ & let $f(X) = X^3 + aX + b$, be a polynomial in $k[X]$, that has no roots in k (what happened to X^2?) Let α be a root of f (in $\bar{k}$) and let K be the splitting field of f. Then K/k is Galois', because f can't have multiple roots. Note that $[k(\alpha):k] = 3$ and $k(\alpha) \subseteq K$. So $3 \mid [K:k]$ and $[K:k] \mid 3! = 6$ (WHY?).

Therefore $[K:k] = 3$ or $[K:k] = 6$. In the first case $K = k(\alpha)$.

Let $\alpha = \alpha_1, \alpha_2, \alpha_3$ be the roots of f and let $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$ and $\Delta = \delta^2$.

Put $G = Gal(K/k)$. For any $\sigma \in G$ we have $\sigma(\delta) = \pm\delta$; so $\sigma(\Delta) = \Delta$. As a result $\Delta \in k$. Indeed, we may calculate it as $\Delta = -4a^3 - 27b^2$.

If $\delta \notin k$, then $[k(\delta):k]=2$; and $\delta \in K$. So $[K:k]=6$ and $G \simeq S_6$.



So $K=k(\alpha,\delta)$ in this case.

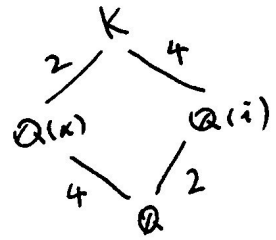
If $\delta \in k$, then $K=k(\alpha)$. (WHY?) ($\delta \in K^G$, hence $\sigma(\delta)=\delta$ for all $\sigma \in G$)

So in that case $[K:k]=3$ and $G \simeq A_3 \simeq C_3$.

A degree 4 Polynomial. $f(x)=x^4-2 \in \mathbb{Q}[x]$.

f is irreducible over $\mathbb{Q}$. (Using Eisenstein Criterion, or by writing down the roots.)

If $\alpha \in \mathbb{R}$ is a real root, then other roots are $-\alpha, i\alpha, -i\alpha$. So $K=\mathbb{Q}(\alpha,i)$ is the splitting field.



So $G=Gal(f):=Gal(K/k)$ has 8 elements.

Consider the following to elements of G:

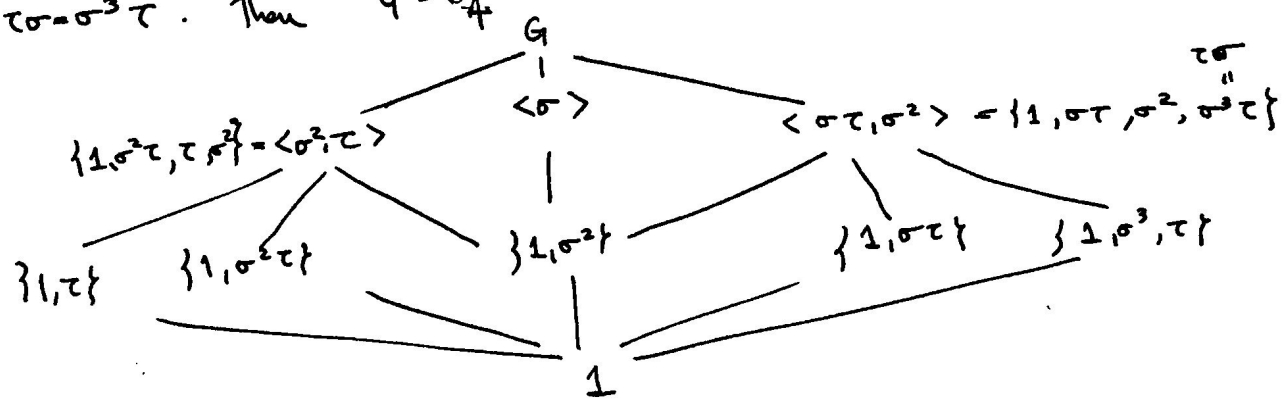
$\tau(i)=-i$ & $\tau(\alpha)=\alpha$.

$\sigma(i)=i$ & $\sigma(\alpha)=i\alpha$.

$o(\tau)=2$, $o(\sigma)=4$, $\tau\sigma(i)=-i$, $\tau\sigma(\alpha)=\tau(i\alpha)=-i\alpha$

$\sigma^3\tau(i)=\sigma^3(-i)=-i$, $\sigma^3\tau(\alpha)=\sigma^3(\alpha)=\sigma^2(i\alpha)=i\,\sigma^2(\alpha)=i\,\sigma(i)\sigma(\alpha)=-i\alpha$.

So $\tau\sigma=\sigma^3\tau$. Then $G \simeq D_4$.



Corresponding intermediate fields:

$G \rightsquigarrow \mathbb{Q}$, $1 \rightsquigarrow K$, $\sigma \rightsquigarrow \mathbb{Q}(i)$ (σ fixes i and has order 4).

$\{1, \sigma^2, \tau, \sigma^2\tau\} \rightsquigarrow \mathbb{Q}(\alpha^2)$ (All elements fix α^2 & $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] = 2$).

$\{1, \tau\} \rightsquigarrow \mathbb{Q}(\alpha)$ $\quad$ $\{1, \sigma^2, \sigma\tau, \sigma^3\tau\} \rightsquigarrow \mathbb{Q}(i\alpha^2)$

$\{1, \sigma^2\} \rightsquigarrow \mathbb{Q}(i, \alpha^2)$ $\quad$ $\{1, \sigma^2\tau\} \rightsquigarrow \mathbb{Q}(i\alpha)$

$\{1, \sigma\tau\} \rightsquigarrow ?$ $\quad$ $\{1, \tau\sigma\} \rightsquigarrow ?$

An Example with $G \cong S_n$: let $K = k(T_1, \dots, T_n)$ where k is a field and $A = \{T_1, \dots, T_n\}$ is a set of indeterminates that are alg. indep over k. Let $G = S_{|A|} = S(A)$. Each element of G gives an automorphism of K; so we think it as a subgroup of $\mathrm{Aut}(K)$. Applying Artin's theorem, we get that K/K^G is Galois with Galois group G. So we found an extension with Galois group S_n, but can we describe K^G? Yes, we can and we will.

Let $f(X) = \prod_{i=1}^{n} (X - T_i)$. Note that K is the splitting field (over K^G) of $f(X)$, which is separable.

$$f(X) = X^n \pm s_1(\vec{T}) X^{n-1} \pm \cdots \pm s_i(\vec{T}) X^{n-i} \pm \cdots \pm s_{n-1}(\vec{T}) X \pm s_n(\vec{T})$$

where $s_1, \dots, s_n$ are elementary symmetric polynomials in $\vec{T} = (T_1, \dots, T_n)$,

for instance, $s_1(\vec{T}) = \sum_{i=1}^{n} T_i$ & $s_n(\vec{T}) = T_1 \cdots T_n$.

Clearly, every element of G fixes each s_i. (This is more or less the definition s_i's.) Thus $k(s_1, \dots, s_n) \subseteq K^G$.

K / K^G)$n!$ / $k(s_1, \dots, s_n)$

$K/k(s_1, \dots, s_n)$ is normal: it's the splitting field of f. And it's degree is less than $n!$. So $K^G = k(s_1, \dots, s_n)$.

A degree 5 Example: let $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$. Let K be its splitting field.

It's irreducible, using Eisenstein Criterion.

$f'(x) = 5x^4 - 4$. So for $\alpha \in \mathbb{R}$, $f'(\alpha) = 0$ iff $\alpha = \sqrt[4]{\frac{4}{5}}$ or $\alpha = -\sqrt[4]{\frac{4}{5}}$.

The other roots of $f'(x)$ are complex.

Then $f(x)$ has at most 3 real roots. Using Newton approximation one may show that it has exactly 3 roots.

Say the roots are $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2$ where $\beta_1, \beta_2 \in \mathbb{C} \setminus \mathbb{R}$.

Then $G = Gal(K/\mathbb{Q})$ has an element switching β_1 and β_2, and fixing $\alpha_1, \alpha_2, \alpha_3$ (Complex conjugation.) So it has a transposition.

As $5 \mid |G| \; (= |S_5|)$, G has an element of order 5, i.e. it's a 5-cycle. It is easy to show that a 5-cycle and a transposition generates the whole S_5. So $G \simeq S_5$.

Cyclotomic Extensions: k a field (of characteristic p). A root of unity in k is a root of $X^n - 1$ for some $n > 0$; these roots are called n^{th} roots of unity.

Put $\mu_n(k) = \{\alpha \in k : \alpha$ is an n^{th} root of unity$\}$.

Note that $|\mu_n(\bar{k})| = n$ if $p \nmid n$, because $X^n - 1$ is separable in that case. Also $\mu_{p^m}(\bar{k}) = \{1\}$.

Clearly, $\mu_n(\bar{k})$ is a (multiplicative) group; hence it is cyclic. A generator is called a primitive n^{th} root of unity.

If $\gcd(m,n) = 1$, then $\mu_{mn}(\bar{k}) \simeq \mu_m(\bar{k}) \times \mu_n(\bar{k})$. $(p \nmid mn, p \nmid n)$

Let $\zeta \in \bar{k}$ be a primitive n^{th} root of unity, and consider $k(\zeta)$. Any conjugate of ζ under an embedding is again an n^{th} root of unity, and hence $k(\zeta)/k$ is normal. (and separable). Let $G = Gal(k(\zeta)/k)$. Let $\sigma \in G$, then $\sigma(\zeta) = \zeta^i$ for some i. We need the order of ζ^i to be n as well; so it follows that $\gcd(i,n) = 1$. Also this i is

determined up to a multiple of n.
Then we have a group homomorphism:

$$\varphi: G \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \qquad (\text{So } |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n).)$$

$$\sigma \longmapsto i(\sigma), \text{ where } \sigma(\zeta) = \zeta^{i(\sigma)}.$$

This map is injective, so $|G| \mid \varphi(n)$, $[k(\zeta):k] \mid \varphi(n)$.

If $k = \mathbb{R}$, then $[\mathbb{R}(\zeta):\mathbb{R}] = 2$ for any primitive n^{th} root of unity ζ.

7th Lecture

Theorem: Let $\zeta \in \mathbb{C}$ be a primitive n^{th} root of unity. Then $[\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(n)$.

Proof: Let $f(x) \in \mathbb{Q}[x]$ be the minimal pol. of ζ (over $\mathbb{Q}$).
Then $X^n - 1 = f(x)\,h(x)$ for some $h \in \mathbb{Q}[x]$. By Gauss lemma, $f, h \in \mathbb{Z}[x]$.
It suffices to show that ζ^p is root of f, where $p \nmid n$ a prime.
(That would mean all the $\varphi(n)$ primitive n^{th} roots of unity are root of f; Then $\deg f \geq \varphi(n)$.)

Suppose that ζ^p is not a root of f. Then it's a root of $h(x)$, and hence ζ is a root of $h(X^p)$. Then $f(x) \mid h(X^p)$. Say $h(X^p) = f(x)\,g(x)$ with $g \in \mathbb{Z}[x]$. Consider this equality modulo p:

$\overline{h(X^p)} \equiv \overline{f(x)}\ \overline{g(x)} \pmod p$. Then $\overline{h(X^p)} \equiv \overline{h(x)}^p \equiv \overline{f(x)} \cdot \overline{g(x)} \pmod p$

Then $\overline{h(x)}$ & $\overline{f(x)}$ have a common root; but this means that $X^n - \overline{1}$ has a double root; which is not possible as $p \nmid n$.
Hence ζ^p is a root of f. ∎

Norm and Trace: Let $E|k$ be finite, $r=[E:k]_s$, $p^m=[E:k]_i$, and let $\{\sigma_1,\dots,\sigma_r\}$ be the set of embeddings of E into $\overline{k}$, over k. Define (for $\alpha\in E$):

$$N_{E/k}(\alpha)=\prod_{i=1}^{r}\sigma_i(\alpha)^{p^m} \quad \& \quad Tr_{E/k}(\alpha)=[E:k]_i\sum_{i=1}^{r}\sigma_i(\alpha)$$

($=0$ if non-sep. ext.)

Proposition: $N_{E/k}$ is a multiplicative group homomorphism from $E^\times$ to $k^\times$.

Proof: Let $\alpha,\beta\in E^\times$.

$$N_{E/k}(\alpha\cdot\beta)=\left(\prod_{i=1}^{r}\sigma_i(\alpha\cdot\beta)\right)^{p^m}=\left(\prod_{i=1}^{r}\sigma_i(\alpha)\cdot\sigma_i(\beta)\right)^{p^m}=\left(\prod_{i=1}^{r}\sigma_i(\alpha)\right)^{p^m}\left(\prod_{i=1}^{r}\sigma_i(\beta)\right)^{p^m}$$

$$=N_{E/k}(\alpha)\cdot N_{E/k}(\beta).$$

If σ_i is an embedding of E into $\overline{k}$ over k, then $\sigma_i(N_{E/k}(\alpha))=N_{E/k}(\alpha)$.

Then $N_{E/k}(\alpha)\in k^\times$. (This is because α^{p^m} is sep. $/k$.)
(That's why we need p^m in the def.)
(Consider the normal closure of $k(\alpha^{p^m})$.) ▨

Proposition: $Tr_{E/k}$ is an additive group homomorphism from E into k.

Proof: Similar to the proof above.

Let $E\supseteq F\supseteq k$ be a tower of fields. Then we have $N_{E/k}$, $N_{E/F}$, $N_{F/k}$.
We claim that $N_{E/k}=N_{F/k}\circ N_{E/F}$.

Let $\sigma_1,\dots,\sigma_r$ be the embeddings of E into $\overline{F}$ over F & $\tau_1,\dots,\tau_s$ embeddings of F into $\overline{k}$ over k.

Then $N_{E/k}(\alpha)=\left(\prod_{j=1}^{s}\prod_{i=1}^{r}\tau_j\sigma_i\alpha\right)^{[E:k]_s}=\left(\prod_{j=1}^{s}\tau_j\left(\left(\prod_{i=1}^{r}\sigma_i\alpha\right)^{[E:F]_s}\right)\right)^{[F:k]_s}=$ ↵

$$=\left(\prod_{T=1}^{s}\tau_T(N_{E/F}(\alpha))\right)^{[F:k]_s}=N_{F/k}(N_{E/F}(\alpha)).$$

Similarly, $Tr_{E/k} = Tr_{F/k} \circ Tr_{E/F}$.

Let $E = k(\alpha)$, $f(x) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in k[X]$ min. pol. of α over k.

Let $\alpha_1, \cdots, \alpha_r$ be the distinct roots of f in $\bar{k}$.

Then $f(x) = \left(\prod_{i=1}^{r} (X - \alpha_i) \right)^{[E:k]_s}$.

Then $N_{E/k}(\alpha) = (\alpha_1 \cdots \alpha_r)^{[E:k]_s} = (-1)^n a_0$ & $Tr_{E/k}(\alpha) = -a_{n-1}$.

Therefore, we have:

① $N_{E/k}(\alpha) = \alpha^n$ if $\alpha \in k$ $(n = [E:k])$.

② $N_{E/k}(\alpha) = N_{k(\alpha)/k}\left(N_{E/k(\alpha)}(\alpha) \right)$

$= N_{k(\alpha)/k}\left(\alpha^{[E:k(\alpha)]} \right)$

$= \left(-1^{[k(\alpha):k]} a_0 \right)^{[E:k(\alpha)]}$

$= (-1)^{[E:k]} \cdot a_0^{[E:k]/[k(\alpha):k]}$ $\quad ([k(\alpha):k] = \deg. \text{ of min. poly.})$

③ $Tr_{E/k}(\alpha) = n\alpha$ if $\alpha \in k$

④ $Tr_{E/k}(\alpha) = -[E:k(\alpha)]\, a_{n-1}$.

⑤ $Tr_{E/k}$ is k-linear.

Proposition: E/k finite separable. Then $(x,y) \mapsto Tr_{E/k}(xy)$ is a bilinear map from $E \times E$ to k.

Proof: Clear.

As a result $Tr_{\sharp}: E \to E^*$ is a k-linear map.
$x \mapsto Tr_x : E \to k$
$y \mapsto Tr_{E/k}(xy)$

($Tr_{E/k}(1) \neq 0$ for char $\neq$)

Let $x \in \ker(Tr)$; so $Tr_{E/k}(xE) = 0$. If $x \neq 0$, then $xE = E$, so $Tr_{E/k}(E) = Tr_{E/k}(xE) \neq 0$.
So Tr is 1-1 and it's an isomorphism of k-linear spaces because of dimension reasons. Hence E is identified with E^* via Tr.

[Characters: G a monoid, K a field. A character is a homomorphism $\chi : G \to K^\times$.
Identically 1 map is called the trivial character.

Theorem: $\chi_1, \dots, \chi_n$ distinct characters of G in K. Then they are lin. independent over K: If $a_1, \dots, a_n \in k$ such that $a_1\chi_1 + \cdots + a_n\chi_n \equiv 0$, then $a_i = 0$ for all i.

Proof: We proceed by induction on n.
n=1: Clear. (no character gets 0 value.)
n>1: Suppose not. Let n be the smallest number such that there are dist. $\chi_1, \dots, \chi_n$ and $a_1, \dots, a_n \in K^\times$ s.t. $a_1\chi_1 + \cdots + a_n\chi_n$ is identically 0.
Let $g \in G$ s.t. $\chi_1(g) \neq \chi_2(g)$. Then

$$a_1\chi_1(gx) + a_2\chi_2(gx) + \cdots + a_n\chi_n(gx) = 0 \quad \text{for all } x \in G.$$

So after dividing by $\chi_1(g)$:

$$a_1\frac{\chi_1(g)}{\chi_1(g)}\chi_1(x) + a_2\frac{\chi_2(g)}{\chi_1(g)}\chi_2(x) + \cdots + a_n\frac{\chi_n(g)}{\chi_1(g)}\chi_n(x) = 0 \quad \text{for all } x \in G.$$

We also have

$$a_1\chi_1(x) + a_2\chi_2(x) + \cdots + a_n\chi_n(x) = 0 \quad \text{for all } x \in G.$$

Adding these:

$$a_2\left(\frac{\chi_2(g)}{\chi_1(g)}-1\right)\chi_2+\cdots+a_n\left(\frac{\chi_n(g)}{\chi_1(g)}-1\right)\chi_n\equiv 0.$$

This contradicts the minimality of n. ∎]

Proposition: E/k finite separable extension, $\sigma_1,\dots,\sigma_n$ distinct embeddings of E into $\overline{k}$ over k. If $\{w_1,\dots,w_n\}$ is a basis of E over k, then $\xi_j=(\sigma_j w_i)_{i=1,\dots,n}\in E^n$ $(j=1,\dots,n)$ are linearly independent over E.

Proof: Let $\alpha_1,\dots,\alpha_n\in E$ be such that $\alpha_1\xi_1+\cdots+\alpha_n\xi_n=\vec{0}$. Then

$(\alpha_1\sigma_1+\cdots+\alpha_n\sigma_n)(w_i)=0$ for all i. But then $\alpha_1\sigma_1+\cdots+\alpha_n\sigma_n\equiv 0$ at $E^\times$ in E^n

since $\sigma_1|_{E^\times},\dots,\sigma_n|_{E^\times}$ are characters, by the lin. indep of characters we get $\alpha_1=\cdots=\alpha_n=0$ ∎

Let E/k be finite and let $\alpha\in E$. Consider the k-linear map:

$$m_\alpha: E\to E,\quad x\mapsto \alpha\cdot x$$

. Let M_α be the matrix of m_α for a given basis. We claim that $\det M_\alpha=N_{E/k}(\alpha)$.

First, let $E=k(\alpha)$ & let $1,\alpha,\dots,\alpha^{d-1}$ be a basis; and let $f(X)=X^d+a_{d-1}X^{d-1}+\cdots+a_1X+a_0$ be the minimal polynomial of α over k. Write M_α with respect to $1,\alpha,\dots,\alpha^{d-1}$:

$m_\alpha(1)=\alpha$, $m_\alpha(\alpha)=\alpha^2$, $\dots$, $m_\alpha(\alpha^{d-1})=\alpha^{d-1}=-a_{d-1}\alpha-\cdots-a_1\alpha-a_0\cdot 1$.

$$M_\alpha=\begin{bmatrix}0 & 0 & \cdots & 0 & -a_0\\ 1 & 0 & & \vdots & -a_1\\ \vdots & 1 & 0 & \vdots & \vdots\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ \vdots & \vdots & 0 & 0 & \vdots\\ 0 & 0 & & 1 & -a_{d-1}\end{bmatrix}$$

& $\det M_\alpha=(-1)^{d-1}(-a_0)$

$=(-1)^d a_0=N_{k(\alpha)/k}(\alpha)$.

In general : $N_{E/k}(\alpha) = \left(-1^d a_0\right)^{[E:k]/d}$.

let $w_1, \dots, w_k$ be a basis of E over $k(\alpha)$.

Then $\{ \alpha^i w_j : i,j \}$ is a basis of E over k.

$m_\alpha(\alpha^i w_j) = \alpha^{i+1} \cdot w_j$ for $i = 1, \dots, d-1$. Then

$$M_\alpha = \begin{bmatrix} \begin{matrix} 0 & \cdots & 0 & -a_0 \\ 1 & \ddots & & -a_1 \\ 0 & \ddots & & \vdots \\ 0 & \cdots & 1 & -a_{d-1} \end{matrix} & 0 & 0 \\ 0 & \begin{matrix} 0 & \cdots & 0 & -a_0 \\ 1 & \ddots & & \\ 0 & \cdots & 1 & -a_{d-1} \end{matrix} & 0 \\ 0 & 0 & \ddots \\ \ddots & \ddots & \ddots \end{bmatrix}$$

& let $M_\alpha = \left((-1)^d a_0\right)^{[E:k]/d}$

$= N_{E/k}(\alpha)$.

Similarly, $\mathrm{Tr}_{E/k}(\alpha) = \mathrm{Tr}(M_\alpha)$.

Cyclic Extensions

AIM: E/k Galois. When is it the case that $E = k(\alpha)$ for some $\alpha \in E$, with minimal polynomial dividing $X^n - a$ for some $n \geq 1$ and $a \in k$.

Theorem (Hilbert's 90): Let K/k be cyclic of order n; say $\mathrm{Gal}(K/k) = \langle \sigma \rangle$. Let $\alpha \in K$. Then $N_{K/k}(\alpha) = 1$ iff $\alpha = \frac{\beta}{\sigma\beta}$ for some $\beta \in K^\times$.

Proof: ($\Leftarrow$) Clear.

($\Rightarrow$) First, as they are distinct characters of $K^\times$ (in $K^\times$), $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ are linearly independent over K.

let $a_1 = 1$, $a_2 = \alpha$, $a_3 = \alpha \cdot \sigma(\alpha)$, , $\dots$, $a_n = \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)$; all are elements of $K^\times$. (Notation: $\alpha^{1+\sigma}$ in the place of $\alpha \cdot \sigma(\alpha)$.)

Now $a_1 \cdot 1 + a_2\sigma + \cdots + a_n\sigma^{n-1} \neq 0$; so let $\theta \in K$ such that

$$\beta := \theta + \alpha\sigma(\theta) + \alpha\sigma(\alpha)\sigma^2(\theta) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\theta) \neq 0.$$

We claim that $\alpha = \dfrac{\beta}{\sigma\beta}$.

$$\sigma\beta = \sigma(\theta) + \sigma(\alpha)\sigma^2(\theta) + \sigma(\alpha)\sigma^2(\alpha)\sigma^3(\theta) + \cdots + \underbrace{\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-2}(\alpha)}_{N_{K/k}(\alpha)}\underbrace{\sigma^n(\theta)}_{\theta}$$

$$= N_{K/k}(\alpha)\,\theta + \sigma(\theta) + \sigma(\alpha)\sigma^2(\theta) + \cdots + \sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\theta)$$

Then
$$\frac{\beta}{\sigma(\beta)} = \alpha \iff N_{K/k}(\alpha) = 1. \qquad \square$$

Theorem: Let k be a field, n a natural number such that $\operatorname{char} k \nmid n$. Suppose that k contains a primitive n^{th} root of unity, say ζ.

(a) If K/k is cyclic of order n, then $K = k(\alpha)$ for some $\alpha \in K$ which is a root of $X^n - a$ for some $a \in k$.

(b) If $\alpha \in \bar{k}$ is a root of $X^n - a$ for some $a \in k$, then $k(\alpha)/k$ is cyclic of order $d \mid n$. Also $\alpha^d \in k$.

Proof: (a) Let $\operatorname{Gal}(K/k) = \langle\sigma\rangle$. Note that $N_{K/k}(\zeta) = \zeta^n = 1$, hence $N_{K/k}(\zeta^{-1}) = 1$. So by Hilbert 90, $\zeta^{-1} = \dfrac{\beta}{\sigma\beta}$ for some $\beta \in K^\times$, and $\sigma\beta = \zeta\beta \neq 0$. $\sigma^i(\beta) = \beta\zeta^i$ for $i = 1, \ldots, n$. So $\beta, \beta\zeta, \ldots, \beta\zeta^{n-1}$ are all conjugate over k. Then $[k(\beta) : k] \geq n$ & $k(\beta) = K$. Note that $\sigma(\beta^n) = (\sigma\beta)^n = \beta^n\zeta^n = \beta^n$. Thus $a = \beta^n \in k$ & β is a root of $X^n - a$.

(b) Let α be a root of $X^n - a$. Then $\zeta^i\alpha$ are also roots of $X^n - a$. Then $k(\alpha)/k$ is Galois; say $G = \operatorname{Gal}(k(\alpha)/k)$. Let $\sigma \in G$, Then $\sigma\alpha$ is a root of $X^n - a$, as well. Thus $\sigma\alpha = \zeta_\sigma\,\alpha$ for some n^{th}-root of unity ζ_σ. This gives an injective map

homomorphism $G \longrightarrow \mu_n(k) \simeq Z_{\varphi(n)}$. So G is cyclic.

If $|G| = d$, then $d \mid n$. For a generator σ of G, we have $\sigma(\alpha^d) = (\sigma\alpha)^d = (\zeta_\sigma \alpha)^d = \alpha^d$. So $\alpha^d \in k$. (ζ_σ is primitive.) ∎

Theorem (Hilbert's 90 - Additive form): K/k cyclic with $G = \mathrm{Gal}(K/k) = \langle\sigma\rangle$ of order n. Let $\beta \in K$. Then $\mathrm{Tr}_{K/k}(\beta) = 0$ if and only if $\beta = \alpha - \sigma\alpha$ for some $\alpha \in K$.

Proof: ($\Leftarrow$) Clear.

($\Longrightarrow$) Take some $\theta \in K$ with $\mathrm{Tr}_{K/k}(\theta) \neq 0$. (Tr is not identically 0.)

$$\text{let } \alpha = \frac{\beta\sigma\theta + (\beta+\sigma\beta)\sigma^2\theta + \cdots + (\beta + \sigma\beta + \cdots + \sigma^{n-2}\beta)\sigma^{n-1}(\theta)}{\mathrm{Tr}(\theta)}$$

$$\text{Then } \sigma\alpha = \frac{\sigma(\beta)\,\sigma^2(\theta) + (\sigma(\beta)+\sigma^2(\beta))\,\sigma^3(\theta) + \cdots + \overbrace{(\sigma(\beta)+\sigma^2(\beta)+\cdots+\sigma^{n-1}(\beta))}^{-\beta}\sigma^n(\theta)}{\mathrm{Tr}(\theta)}$$

$$\text{Now } \alpha - \sigma\alpha = \frac{\beta\,\sigma(\theta) + \beta\sigma^2(\theta) + \cdots + \beta\,\sigma^{n-1}(\theta) + \beta\theta}{\mathrm{Tr}(\theta)} = \beta.$$ ∎

Theorem (Artin-Schreier): Let k be a field of characteristic p.

(a) Let K/k be cyclic of degree p. Then there is $\alpha \in K$ s.t. $K = k(\alpha)$ and α is a root of $X^p - X - a = 0$ for some $a \in k$.

(b) If $\alpha \in \bar{k}$ is a root of an irreducible polynomial of the form $X^p - X - a$ for some $a \in k$, then $k(\alpha)/k$ is cyclic of order p.

Proof: (a) Let $G = \mathrm{Gal}(K/k) = \langle\sigma\rangle$.

$\mathrm{Tr}_{K/k}(-1) = p(-1) = 0$. So $1 = \sigma\alpha - \alpha$ for some $\alpha \in K$. So $\sigma\alpha = \alpha + 1$ and $\sigma^i(\alpha) = \alpha + i$ for each $i \in \{0, 1, \cdots, p-1\}$. These are all distinct conjugates of α. So $[k(\alpha) : k] \geq p$ & $k(\alpha) = K$.

$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha+1)^p - (\alpha+1) = \alpha^p - \alpha.$

So $a = \alpha^p - \alpha \in k$ & hence α is a root of $X^p - X - a$.

(b) If $\alpha \in \bar{k}$ is a root of $X^p - X - a$, then each $\alpha + i$ is a root of $X^p - X - a$ $(i = 0, \cdots, p-1)$. So these are exactly the roots.

We claim that if no root of $X^p - X - a$ is in k, then it is irreducible. Suppose $f(X) = g(X)\,h(X)$, $\deg g, \deg h < p$; let $d = \deg g$.

So $g(X)$ is a product of $(X - \alpha - i)$ for d many i's. The coefficient of X^{d-1} is $-d\alpha + j$ for some j. But this element is not in k unless $d = 0$. So $X^p - X - a$ is irreducible over k. Hence $k(\alpha)/k$ is Galois of degree p; so it's cyclic. (It is generated by $\alpha \mapsto \alpha + 1$.) ∎

Solvability By Radicals: F/k finite separable ($\operatorname{char} k = p$ (could be 0)). We say F/k is solvable-by-radicals if there is a finite extension E/k with $F \subseteq E$, and there is a tower $k = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{n-1} \subseteq E_n = E$ of intermediate fields such that E_{i+1} is obtained by one of the following:

(i) Adjoining a root of unity.

(ii) Adjoining a root of $X^n - a$ where $a \in E_i$ & $p \nmid n$.

(iii) Adjoining a root of $X^p - X - a$ with $a \in E_i$.

(i is a part of ii, but we still want to isolate the case of adding a root of unity. iii appears only when $p > 0$.)

[Recall: A group G is solvable if there is a tower

$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m$ such that

(i) $G_{i+1} \trianglelefteq G_i$ for $i = 0, 1, \ldots, m-1$ (ii) G_i / G_{i+1} is abelian (iii) $G_m = 1$.

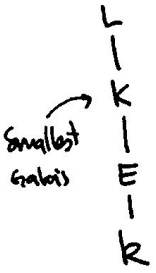
Facts: ① If G is finite, then we can refine the tower in a way that G_i/G_{i+1} are cyclic.

② G a group, $H \triangleleft G$. Then G is solvable iff H & G/H are solvable.

③ S_n is not solvable for $n \geq 5$.]

Definition: E/k finite extension. E/k is solvable if the smallest Galois extension K/k with $E \subseteq K$ is solvable.

Note that "smallest" is not necessary; i.e if there is a solvable Galois extension K/k with $E \subseteq K$, then E/k is solvable.



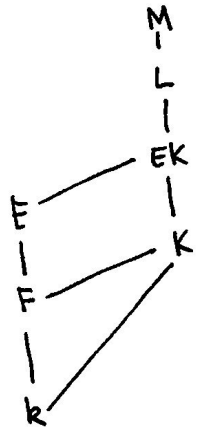
$\mathrm{Gal}(L/k) \leq \mathrm{Gal}(L/K) \simeq \mathrm{Gal}(L/k)/\mathrm{Gal}(K/k)$.

Proposition: (a) $k \subseteq F \subseteq E$ fields. E/k is solvable iff E/F and F/k are solvable.
(b) E/k solvable, F/k arbitrary. Then EF/F is solvable.

Proof: (b) Let K/k be solvable with $E \subseteq K$. Then KF/F is Galois and $\mathrm{Gal}(KF/F) \hookrightarrow \mathrm{Gal}(K/k)$. So $\mathrm{Gal}(KF/F)$ is solvable and $EF \subseteq KF$ & EF/F is solvable.

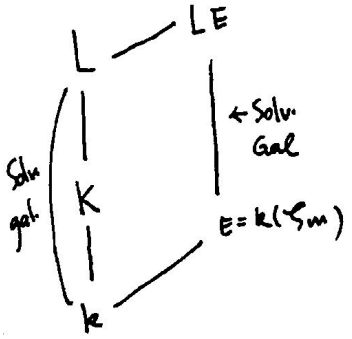
(a) It's clear that E/F and F/k are solvable if E/k is.
For the other implication, let F/F & F/k be solvable. Let $K \supseteq F$ s.t K/k is Galois and solvable. Also by (b), EK/K is solvable. Let $L \supseteq EK$ such that L/K is Galois and $\mathrm{Gal}(L/K)$ is solvable.
Let $\sigma : L \to \bar{k}$ over k. Then $\sigma K = K$ as K/k is Galois. So $\sigma L/K$ is solvable. Let M be the compositum of all σL's. Then M/k is Galois; hence M/K is Galois and $\mathrm{Gal}(M/K) \subseteq \prod_\sigma \mathrm{Gal}(\sigma L/K)$ is solvable.

Consider $\mathrm{Gal}(M/k) \longrightarrow \mathrm{Gal}(K/k)$ given as restriction. It is a surjective group homomorphism & kernel is normal in $\mathrm{Gal}(M/k)$ and it's isomorphic to $\mathrm{Gal}(M/K)$. So $\mathrm{Gal}(M/k)/\ker \simeq \mathrm{Gal}(K/k)$. Then by fact ②, $\mathrm{Gal}(M/k)$ is solvable finishing the proof.



Theorem: K/k finite extension. Then K/k is solvable iff it is solvable-by-radicals.

Proof: ($\Longrightarrow$) Let L/k be Galois with $L \supseteq K$ and $\mathrm{Gal}(L/k)$ solvable. Let m be the product of all primes dividing $[L:k]$ and not equal to $\mathrm{char}\, k$. Let ζ_m be a primitive m^{th} root of unity and put $E = k(\zeta_m)$. Then LE/E is Galois and solvable; say $G = \mathrm{Gal}(LE/E)$. Then there is a tower $\{1\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$ such that G_i/G_{i+1} is cyclic. By the correspondence, we get intermediate fields $E = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{n-1} \subseteq LE$ such that $\mathrm{Gal}(E_{i+1}/E_i) \simeq G_i/G_{i+1}$, hence cyclic of prime order. Using the previous theorems, we get that LE/k is Galois with solvable subgroup. Hence K/k is solvable-by-radicals.



($\Longleftarrow$) Let K/k be solvable-by-radicals, then the normal closure L of K over k is also solvable-by-radicals. Again, let m be the product of all primes dividing $[L:k]$ and not equal to $\mathrm{char}\, k$, and let ζ_m be a primitive m^{th} root of unity. Put $F = k(\zeta_m)$. It suffices to prove that LF/F is solvable. But this again follows from previous (with 2) theorems on cyclic extensions. ∎

Theorem: Let k be any field, $n>1$, $a \in k^\times$. Suppose that $a \notin k^p$ for every prime $p \mid n$, and $a \notin -4k^4$ if $4 \mid n$. Then $X^n - a$ is irreducible in $k[X]$.

Proof: We proceed by induction on n. $n=2$ case is clear.

Step 1: (Reduction to the case that n is a prime power)

Let $n = p^r \cdot m$, $p \nmid m$, $p \neq 2$. Suppose that $\alpha = \alpha_1, \alpha_2, \cdots, \alpha_m$ are the roots of $X^m - a$ (with possible repetitions). By induction $X^m - a$ is irred.

Write $X^n - a = (X^{p^r})^m - a = \prod_{i=1}^{m} (X^{p^r} - \alpha_i)$.

If $\alpha = \beta^p$ in $k(\alpha)$, then $-a = (-1)^m N_{k(\alpha)/k}(\alpha) = (-1)^m N_{k(\alpha)/k}(\beta^p)$

$= (-1)^m N_{k(\alpha)/k}(\beta)^p$.

If m is odd, then $a \in k^p$, and if m is even, then $a = (-N_{k(\alpha)/k}(\beta))^p \in k^p$.

So $\alpha \notin k(\alpha)^p$.

As a result if we know that $X^{p^r} - \alpha$ is irreducible in $k(\alpha)[X]$, then we would have concluded that $[k(\beta):k] = [k(\beta):k(\alpha)] \cdot [k(\alpha):k]$,

$= p^r \cdot m = n$.

where β is a root of $X^{p^r} - \alpha$. Then $X^n - a$ would be the min. pol. of β over k, and hence $X^n - a$ would be irreducible in $k[X]$.

Step 2: ($X^{p^r} - a$ is irreducible in $k[X]$)

Case 1: ($p = \operatorname{char} k$): $(X^{p^r} - a) = (X^{p^{r-1}} - \alpha)^p$ where $\alpha^p = a$. By induction $X^{p^{r-1}} - \alpha$ is irreducible in $k(\alpha)[X]$, hence $X^p - a$ is irreducible in $k[X]$.

Case 2: ($p \nmid \operatorname{char} k$): Let α be a root of $X^p - a$.

If $X^p - a$ is not irreducible in $k[X]$ then $[k(\alpha):k] = d < p$. Then $d = N_{k(\alpha)/k}(\alpha^p) = N_{k(\alpha)/k}(\alpha)^p \in k^p$ & hence $a \in k^p$. Therefore $X^p - a$ is irreducible.

We proceed by induction on r with $r=1$ case being the previous paragraph.

Let $\alpha_1, \cdots, \alpha_p \in \bar{k}$ be the roots of $X^p - a$. Then

$$X^{p^r} - a = \prod_{i=1}^{p} (X^{p^{r-1}} - \alpha_i).$$

Case a: $\alpha \notin k(\alpha)^p$: Let β be a root of $X^{p^{r-1}} - \alpha$.
(i.e. $\alpha = \beta^{p^{r-1}}$)

If $p \neq 2$, then $[k(\beta) : k(\alpha)] = p^{r-1}$ & $[k(\beta) : k] = p^{r-1} \cdot p = p^r$. This shows that $X^{p^r} - a$ is irreducible in $k[X]$.

If $p = 2$ and let $\beta \in k(\alpha)$ be such that $\alpha = -4\beta^4$. Then $-a = N_{k(\alpha)/k}(\alpha) = 16\, N_{k(\alpha)/k}(\beta)^4$ is a square in k and $\sqrt{-1} \in k(\alpha)$.
Then $\alpha = (\sqrt{-1}\, 2\beta^2)^2$ in a contradiction.

Case b: $\alpha \in k(\alpha)^p$: Say $\alpha = \beta^p$ with $\beta \in k(\alpha)$.
Now $-a = (-1)^p N_{k(\alpha)/k}(\alpha) = (-1)^p N(\beta)^p$.
If $p \neq 2$, then $a \in k^p$ and we get a contradiction once again.
Let $p = 2$. Then $-a = N(\beta)^2$, put $b = N(\beta) \in k$. So $-1 \notin k^2$, let $i \in \bar{k}$ be with $i^2 = -1$. Then

$$X^{2^r} - a = X^{2^r} + b^2 = (X^{2^{r-1}} + ib)(X^{2^{r-1}} - ib) \text{ in } k(i)[X].$$

By induction, if $X^{2^{r-1}} + ib$ or $X^{2^{r-1}} - ib$ is not irreducible in $k(i)[X]$ then either $\pm ib \in k(i)^2$ or $\pm ib \in -4(k(i))^4$. So in that case $\pm ib$ is a square in $k(i)$; say $\pm ib = (c+di)^2 = c^2 - d^2 + 2cd\,i$ with $c, d \in k$.
Then $c^2 = d^2$ and hence $d = \pm c$ and $\pm ib = 2cdi = \pm 2c^2 i$. But then $a = -b^2 = -4c^4 \in -4k^4$. So $X^{2^{r-1}} \pm ib$ are irreducible in $k(i)[X]$.
Therefore $X^{2^r} - a$ is irreducible in $k[X]$. ∎

10th Lecture

Example: Note that $X^4 + 4b^4 = (X^2 + 2bX + 2b^2)(X^2 - 2bX + 2b^2)$.
So $X^{4m} - a$ is reducible in $k[X]$ if we choose $a \in -4k^4$.
Therefore the assumptions of the theorem are right.

If $a \in k$ such that $a \notin k^p$ for some odd prime p, then $X^{p^r} - a$ is irreducible in $k[X]$ for all $r \geq 1$.

Covollary: Let k be a field of characteristic 0 such that $[\bar{k}:k]$ is finite. Then either k is algebraically closed or $\bar{k} = k(i)$ with $i^2 = -1$. (In other words, if $[\bar{k}:k]$ is finite, then it's either 1 or 2.)

Proof: Clearly $\bar{k}|k$ is a Galois extension. Put $k_1 = k(i)$ with $i^2 = -1$. Let $G = \mathrm{Gal}(\bar{k}/k_1)$; say $|G| = n$. Suppose that $n \neq 1$ and take p, a prime dividing n. Let $H \leq G$ with $|H| = p$ and let $F = \bar{k}^H$. Since $[\bar{k}:F] = p$, we have that $\mu_p(\bar{k}) \subseteq F$. (WHY?) Then by the earlier theorem about cyclic extensions we have that $\bar{k}$ is the splitting field of $X^p - a$ over F. Then $X^{p^2} - a$ is reducible in $F[x]$. Then $p = 2$ and $a \in -4F^4$. Therefore $\bar{k} = F(\sqrt{a}) = F(i) = F$. This is a contradiction; so $n = 1$ and hence $\bar{k} = k(i)$. If $i \in k$, then $\bar{k} = k$; otherwise $[\bar{k}:k] = 2$. ∎

Remark: As a matter of fact, we don't have to assume that characteristic is 0. It follows from the assumption that $[\bar{k}:k]$ is finite and not 1. (See Lang-Algebra pp 299 for details.)

Theorem (Normal Basis Theorem): Let $K|k$ be a finite Galois extension with $G := \mathrm{Gal}(K/k) = \{\sigma_1, \dots, \sigma_n\}$. Suppose that k is infinite. Then there is $w \in K$ such that $\sigma_1(w), \dots, \sigma_n(w)$ is a (linear) basis of K over k.

Proof: Let $K = k(\alpha)$ and let $f(X) \in k[x]$ be the minimal polynomial of α. Without loss of generality $\sigma_1 = id$.

Define $g(X) = \dfrac{f(x)}{(X-\alpha) f'(\alpha)}$, a polynomial in $K[X]$. Note that for $i = 1, \dots, n$

$$\sigma_i(g(X)) = \frac{f(X)}{(X-\alpha_i) f'(\alpha_i)}$$ where $\alpha_i = \sigma_i(\alpha)$. Note that $g(\alpha) = 1$ and $\sigma_i g(\alpha) = 0$ for $i \neq 1$. (Note that $\sigma_i g(\alpha) \neq \sigma_i(g(\alpha))$.)

Let $D(X) = \det\left(\sigma_i \sigma_j g(X)\right)_{i,j \in \{1,\dots,n\}}$. Note that $D(X)$ is a polynomial, and $D(a) = \pm 1 \neq 0$. So $D(X) \not\equiv 0$, and hence we may take $a \in k$ such that $D(a) \neq 0$. Put $w = g(a)$. We'd like to show that $w, \sigma_2(w), \dots, \sigma_n(w)$ are linearly independent over k.

Suppose that $b_1 w + b_2 \sigma_2(w) + \cdots + b_n \sigma_n(w) = 0$. For $i = 1, \dots, n$, applying σ_i to this equality we get $b_1 \sigma_i(w) + b_2 \sigma_i \sigma_2(w) + \cdots + b_n \sigma_i \sigma_n(w) = 0$.
Then $\left(\sigma_i \sigma_j g(a)\right)_{i,j} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Since $\left(\sigma_i \sigma_j g(a)\right)_{i,j}$ is invertible, we get that $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. So $w, \sigma_2(w), \dots, \sigma_n(w)$ are linearly independent over k. ▨

As an example, let's consider the case of a quadratic extension $K = k(\sqrt{d})$ for some $d \in k$. Then $\mathrm{Gal}(K/k) = \{id, \sigma\}$ where $\sigma(\sqrt{d}) = -\sqrt{d}$. We'd like to find $w = a + b\sqrt{d}$ such that w and $a - b\sqrt{d}$ are lin. independent over k. Note that we can't take $a = 0$ or $b = 0$. So suppose $a \neq 0$ and $b \neq 0$ and let $c(a + b\sqrt{d}) + d(a - b\sqrt{d}) = 0$ with $c, d \in k$. Then $a(c+d) = 0$ and $b(c-d) = 0$. So $c + d = c - d = 0$ & hence $c = d = 0$. Therefore in this case, any $w = a + b\sqrt{d}$ with $a \neq 0$, $b \neq 0$ gives a normal basis.

Generic Resolvents

Let $\vec{X} = (X_1, \dots, X_n)$ be a tuple of independent variables, and let k be a field. (Most of the times, we'll assume that $\mathrm{Char}\, k = 0$ to avoid separability issues.)

Put $L = k(\vec{X})$ and $K = k(s_1, \dots, s_n)$, where $s_i(\vec{X})$ is the elementary symmetric polynomial of degree i. Recall that L/K is Galois and $\mathrm{Gal}(L/K) \simeq S_n$. (From now on, we identify these groups. So S_n acts on L by permuting X_i's.)

Put $\theta(T) := (T-X_1)\cdots(T-X_n) = \sum_{i=0}^{n} (-1)^i s_i T^{n-i} \in K[T]$.
($s_0 = 1$.) So L is the splitting of $\theta(T)$ over K.

Let $H \leq S_n$ and put $F = L^H$. Hence $L|F$ is Galois with $\mathrm{Gal}(L/F) = H$. Write $F = K(\alpha)$ for some $\alpha \in F$. This α is called a <u>generic resolvent for H</u>.

<u>Example</u>: Let $H = A_n$. In this case $A_n \lhd S_n$; so $F|K$ is Galois with $\mathrm{Gal}(F/K) \simeq S_n/A_n \simeq \mathbb{Z}_2$. So α must have degree 2 over K. We may determine it to be $\Delta := \prod_{i<j} X_i - X_j$. Clearly, Δ is fixed exactly by elements of A_n and thus $\Delta^2 \in K$ and $F = K(\Delta)$.

Let's go to the opposite direction: Let $\alpha \in L$; actually there is no harm to assume $\alpha \in k[\vec{X}]$. Define $H(\alpha)$ to be the stabilizer of α (under the S_n-action):

$$H(\alpha) = \{\sigma \in S_n : \sigma(\alpha) = \alpha\}.$$

Then $L \mid L^{H(\alpha)}$ is Galois with $\mathrm{Gal}(L/L^{H(\alpha)}) = H(\alpha)$. Clearly, $K(\alpha) \subseteq L^{H(\alpha)}$. Actually, they are equal. (Take this as an exercise.) Therefore α is a generic resolvent for $H(\alpha)$. Also we have

$$H(\alpha) = H(\beta) \iff K(\alpha) = K(\beta) \quad \text{for all } \alpha, \beta \in L.$$

Let $\sigma_1 = id, \sigma_2, \cdots, \sigma_m \in S_n$ be a complete set of coset representatives for $H(\alpha)$. Then $\alpha_i := \sigma_i(\alpha)$ are the conjugates of α and hence

$$m_\alpha(T) := \prod_{i=1}^{m} (T - \alpha_i)$$

is the minimal polynomial of α over K. Write

$$m_\alpha(T) = T^m + c_{m-1}(\vec{s})T^{m-1} + \cdots + c_1(\vec{s})T + c_0(\vec{s}),$$

where $c_0, c_1, \cdots, c_m \in k[Y_1, \cdots, Y_n]$ and $\vec{s} = (s_1, \cdots, s_n)$.

Let $f(x) \in k[x]$ be irreducible and separable with roots $a_1, \dots, a_n$ (in $\overline{k}$). Put $b_i := s_i(a_1, \dots, a_n)$ & let $\vec{b} = (b_1, \dots, b_n) \in \overline{k}^n$. Then

$$f(x) = x^n - b_1 x^{n-1} + \cdots + (-1)^n b_n.$$

Define $m_{\alpha, f} := T^m + c_{m-1}(\vec{b}) T^{m-1} + \cdots + c_1(\vec{b}) T + c_0(\vec{b})$. So if we think of m_α as a function of $X_1, \dots, X_n$, then $m_{\alpha, f}$ is that function evaluated at $(a_1, \dots, a_n)$.

Here is the main result, which we left proofless:

Theorem: Given k and $f \in k[x]$, the Galois group of the splitting field of f over k is contained in a conjugate of $H(\alpha)$ (in S_n) if and only if $m_{\alpha, f}$ has a root in k.

Galois Groups over $\mathbb{Q}$

Let $f \in \mathbb{Z}[x]$ be irreducible, and let K be the splitting field of f over K. We'd like to understand $G = \mathrm{Gal}(K/\mathbb{Q})$.

Let $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}$ be roots of f and put $\Delta := \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$.

Fact 1: Let p be a prime and let $\overline{f} \in \mathbb{F}_p[x]$ be the reduction of f modulo p. Then $\overline{f}$ is separable iff $p \nmid \Delta$.

There are only finitely many primes dividing Δ. Let $p \nmid \Delta$ and write $\overline{f} = \overline{f}_1 \cdots \overline{f}_k$ in $\mathbb{F}_p[x]$; $\overline{f}_i$ are irreducible in $\mathbb{F}_p[x]$.

Fact 2: $\mathrm{Gal}(\overline{f}/\mathbb{F}_p) \le \mathrm{Gal}(f/\mathbb{Q})$.

This means that there are orderings of roots of f and $\overline{f}$ so that each action of $\mathrm{Gal}(\overline{f}/\mathbb{F}_p)$ on the roots of $\overline{f}$ gives an action of $\mathrm{Gal}(f/\mathbb{Q})$ on the roots of f. Also $\mathrm{Gal}(\overline{f}/\mathbb{F}_p)$ is cyclic, say generated by σ.

Since $Gal(\bar{f}/\mathbb{F}_p)$ permutes roots of $\bar{f}_i$ among themselves in a transitive way, we see that σ is a product of k disjoint cycles; moreover the lengths of the cycles are the same as the degrees of $\bar{f}_i$; say $n_i = \deg \bar{f}_i$. As a result $G = Gal(f/\mathbb{Q})$ has an element with the cycle structure $(n_1, \dots, n_k)$.

Example: Let $f(X) = X^5 - X - 1 \in \mathbb{Z}[x]$. One may calculate the discriminant to be $\Delta = 2869 = 19 \cdot 151$.
First let $p=2$. Then $\bar{f} = (x^2+x+1)(x^3+x+1)$. Therefore $G = Gal(f/\mathbb{Q})$ contains a $(2,3)$-cycle.
Now let $p=3$. Then $\bar{f}$ is irreducible and hence G contains a 5-cycle.
Hence $G \simeq S_5$.

Exercise: Show that for any $n>1$, there are infinitely many polynomials in $\mathbb{Q}[X]$ whose Galois groups over $\mathbb{Q}$ are isomorphic to S_n.

Infinite Galois Extensions

Most of the results we talked about were about finite extensions. Now we give an idea about how infinite extensions can be handled.

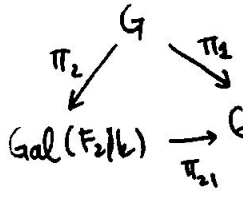
Let K/k be an infinite Galois extension. For any intermediate field F with F/k finite Galois, we have $Gal(F/k)$ is finite and hence $Gal(K/F)$ is of finite index in $G = Gal(K/k)$. Also we have the natural projection

$$\pi : Gal(K/k) \to Gal(K/k)/Gal(K/F) \simeq Gal(F/k).$$

If $k \subseteq F_1 \subseteq F_2 \subseteq K$ are such that F_2/k and F_1/k are finite Galois, then we also have $H_2 := Gal(K/F_2) \subseteq H_1 := Gal(K/F_1)$, and hence we have

$$\pi_{F_2F_1} : G/H_2 \to G/H_1 \; ; \quad G/H_2 \simeq Gal(F_2/k) \;\&\; G/H_1 \simeq Gal(F_1/k).$$

So we have an "inverse system" $\mathcal{S} := \{\pi_{F_2F_1} : Gal(F_2/k) \to Gal(F_1/k) : F_1 \subseteq F_2\}$
$= \{\pi_{H_1H_2} : G/H_2 \to G/H_1 : H_2 \subseteq H_1\}$.



$\pi_1 = \pi_{21} \circ \pi_2$

So $G = \varprojlim_{H \trianglelefteq S} G/H$

Somehow $\sigma \in G$ is determined by $\sigma|_F$ with $k \subseteq F \subseteq \bar{k}$, $[F:k] < \infty$.

The important thing with inverse limit is that we may equip G with the topology of the limit. We are not going to get into this, but we'll just say that Galois correspondence holds with closed subgroups of G.

Example: let K be the splitting field of $\{X^{p^n}-1 : n>0\}$ for a fixed prime p. So $K = \mathbb{Q}(\zeta_p, \zeta_{p^2}, \cdots)$ where $\zeta_{p^n} = e^{2\pi i/p^n}$.

let $K_n = \mathbb{Q}(\zeta_{p^n})$. Then $[K_n:\mathbb{Q}] = \varphi(p^n)$ and $G_n = \mathrm{Gal}(K_n/\mathbb{Q}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$.

Also $K_n \subseteq K_{n+1}$ since $\zeta_{p^{n+2}}^p = \zeta_{p^n}$; and we have $\pi_{n+1} : G_{n+1} \to G_n$, given by $\pi_{n+1}(\bar{a}) = \bar{a}$; or $\pi_{n+1}(a + p^{n+1}\mathbb{Z}) = a + p^n\mathbb{Z}$. π_{n+1} is a p-to-1 map.

Now $G := \mathrm{Gal}(K/\mathbb{Q}) \simeq \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times$. This means that $\sigma \in G$ is determined by $\sigma_n := \sigma|_{K_n} : \mathbb{Q}(\zeta_{p^n}) \to \mathbb{Q}(\zeta_{p^n})$. We know that σ_n is determined by $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{a_n}$ where $p \nmid a_n$. However, a_{n+1} and a_n have a relation:

$\sigma(\zeta_{p^{n+1}}) = \zeta_{p^{n+1}}^{a_{n+1}}$, and $\zeta_{p^n} = \zeta_{p^{n+1}}^p$, $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{a_n} = \sigma(\zeta_{p^{n+1}})^p = \left(\zeta_{p^{n+1}}^{a_{n+1}}\right)^p$

$= \zeta_{p^n}^{a_{n+1}}$.

This means that $a_n = a_{n+1} \pmod{p^n}$; this is exactly $\pi_{n+1}(a_{n+1}) = a_n$.

Example: Let $K = \overline{\mathbb{F}_p}$. Then $\overline{\mathbb{F}_p} = \bigcup_{n>0} \mathbb{F}_{p^n}$. We know that $G_n := \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n. We have $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ iff $m \mid n$.

This time $G := \mathrm{Gal}(K/\mathbb{F}_p) \simeq \varprojlim_n \mathbb{Z}/n\mathbb{Z}$. This is called the profinite closure of $\mathbb{Z}$, and is denoted as $\hat{\mathbb{Z}}$.

(Note that here we ordered $\mathbb{N}^{>0}$ by divisiblity rather than usual ordering)

Definition: Let $K|k$ be any field extension. A subset $\{a_1,\dots,a_n\}$ of K is said to be algebraically independent over if there is no $f \in k[x_1,\dots,x_n]\setminus\{0\}$ such that $f(a_1,\dots,a_n)=0$.
An arbitrary subset $S \subseteq K$ is called algebraically independent over k if each finite subset of S is algebraically indep. over k.

A singleton $\{a\}$ is algebraically independent over k if and only if a is transcendental over k.

Theorem: Let $K|k$ be a field extension. Then there is a maximally indep. (over k) subset S of K; that is S is algebraically independent over k and if $T \supseteq S$ is also algebraically indep. over k, then $T=S$. Moreover if S and T are maximally independent (over k) subsets of K, then $|S|=|T|$.

Proof: Standard: Zorn's Lemma + Exchange Lemma.

Definition: Given $K|k$, a maximally independent (over k) subset of K is called a transcendence basis and its cardinality is called transcendence degree; denoted as $\mathrm{trdeg}(K|k)$

Note that if S is transcendence basis of K over k, then it might not be the case that $k(S)=K$. All we know is that $K|k(S)$ is algebraic. For instance, let $K=k(T)$. Then a natural choice for transcendence basis is $\{T\}$. However, $\{T^2\}$ is also a transcendence basis. As a matter of fact any non-constant element of K gives a trans. basis. 12th Lecture

Example: Let $K|k$ be such that $\mathrm{trdeg}(K/k)=1$ & let $\{t\}$ be a tran. basis. Then $K|k(t)$ is algebraic. Assume that $\mathrm{char}\, k=0$, we have $K=k(t)(s)$ for some $s \in K$ algebraic over $k(t)$. Say $f \in k(t)[X]\setminus\{0\}$ such that $f(s)=0$.
Write $f(X)=\sum_{i=0}^{d} f_i(t)X^i$, where $f_i \in k[Y]$. So there is $g(X,Y):=\sum f_i(Y)X^i \in k[X,Y]$ such that $g(s,t)=0$. So (s,t) is on a curve in k^2. In this case we say that K is a function field over k. If $k=\mathbb{C}$, then elements of K could be thought as meromorphic functions on that curve.

Theorem: Let $K|k$ and $S \subseteq K$ be algebraically independent over k with $|S| = n$. Then $k(S) \simeq k(X_1, \dots, X_n)$.

Proof: Define $\varphi: k[X_1, \dots, X_n] \longrightarrow k[a_1, \dots, a_n]$ where $S = \{a_1, \dots, a_n\}$, by $\varphi(X_i) = a_i$. This is clearly a (surjective) ring homomorphism and it's injective since S is alg. indep. over k. Hence it extends to the fraction fields. ∎

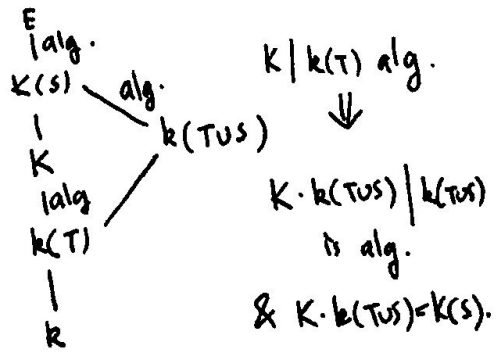
Corollary: Let $K_1|k_1$, $K_2|k_2$ be extensions and let $S_1 \subseteq K_1$ and $S_2 \subseteq K_2$ be alg. indep. over k_1 and k_2. Suppose that we have an injective function $\varphi: S_1 \to S_2$ and $\sigma: k_1 \longrightarrow k_2$ embedding of fields. Then σ extends to a field embedding $k_1(S_1) \longrightarrow k_2(S_2)$. If φ is a bijection and σ is an isomorphism, then $k_1(S_1) \simeq k_2(S_2)$.

An extension of the form $k(S)$ is said to be purely transcendental.

Theorem: Let $E|K$ and $K|k$ be field extensions. Then $\operatorname{trdeg}(E/k) = \operatorname{trdeg}(E/K) + \operatorname{trdeg}(K/k)$.

Proof: Let S and T be trans. bases of $E|K$ and $K|k$ respectively. Note that $S \cap T = \emptyset$. So it's enough to show that $S \cup T$ is a trans. basis of E over k.

We first show that $E|k(S \cup T)$ is algebraic:



It remains to show that $S \cup T$ is alg. indep. over k.

Let $f(X_1, \dots, X_m, Y_1, \dots, Y_n) \in k[\vec{X}, \vec{Y}]$, and $s_1, \dots, s_m \in S$, $t_1, \dots, t_n \in T$ with $f(s_1, \dots, s_m, t_1, \dots, t_n) = 0$.

Let $g(\vec{X}) := f(\vec{X}, t_1, \dots, t_n) \in k(\vec{t})[\vec{X}]$. Since $s_1, \dots, s_m$ are alg. indep. over K, we see that $g \equiv 0$. Write $g(\vec{X}) = \sum_{i \in I} h_i(\vec{X})\, \ell_i(\vec{t})$ where $h_i \in k[\vec{X}]$, $\ell_i \in k[\vec{Y}]$.

Then $\ell_i(\vec{t}) = 0$ for all i; hence $\ell_i \equiv 0$ for all i. But then $f(\vec{X}, \vec{Y}) = 0$ ∎

Theorem: Let K_1/k_1, K_2/k_2 be field extensions where k_1, K_2 are algebraically closed with $\operatorname{trdeg}(K_1/k_1) = \operatorname{trdeg}(K_2/k_2)$. Then every isomorphism of k_1 and k_2 extends to an isomorphism of K_1 and K_2.

Proof: Let $\sigma: k_1 \to k_2$ be an isomorphism. Using the corollary from the previous page σ extends to an isomorphism $\sigma: k_1(S_1) \to k_2(S_2)$. By an earlier result, this extends to an isomorphism $\sigma: \overline{k_1(S_1)} \to \overline{k_2(S_2)}$. However, it's clear that $\overline{k_1(S_1)} = K_1$ and $\overline{k_2(S_2)} = K_2$. ∎

Let's look at the case $\operatorname{trdeg}(K/k) = 1$ in a little bit more detail. In that case, there is $T \in K$ s.t $K/k(T)$ is algebraic. We also know that $k(T) \simeq k(X)$. What are between k and $k(T)$? The next theorem answers that:

Theorem (Lüroth): Let $k \subsetneq F \subsetneq k(T)$. Then $F = k(Y)$ for some $Y \in k(T)$.

So they are all purely transcendental over k.

(We are not going to prove this theorem)

Consider an automorphism $\sigma: k(T) \to k(T)$ over k. This σ is determined by $\sigma(T)$; say $\sigma(T) = \frac{f(T)}{g(T)}$ where $f, g \in k[T]$, $g \neq 0$.

First thing to note is that not both f, g are constant.

Exercise: Let $f, g \in k[T]$ be relatively prime, and that they are not both constant and $g \neq 0$. Then $[k(T) : k(\frac{f}{g})] = \max\{\deg(f), \deg(g)\}$.

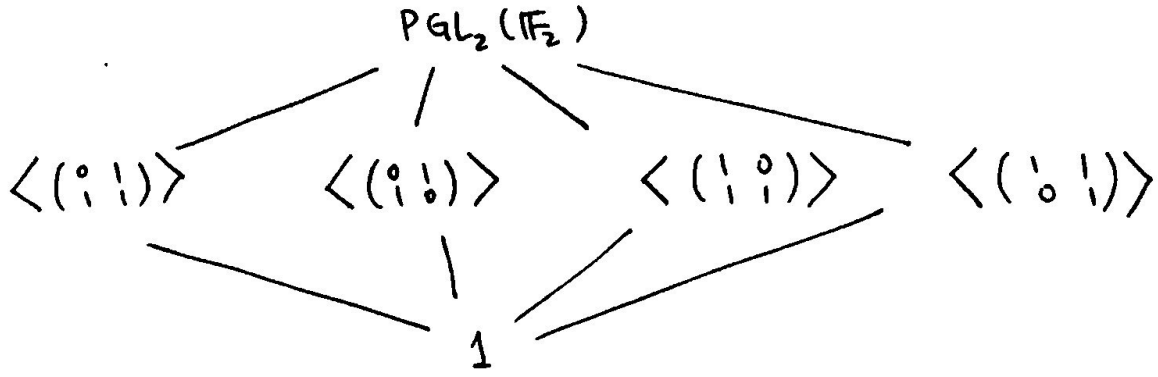
Assuming this exercise, we see that if σ is an automorphism, then $\deg(f), \deg(g) \leq 1$; and not both 0. Say $\frac{f}{g} = \frac{aT+b}{cT+d}$ with $a,b,c,d \in k$

Note that $\frac{f}{g} \in k$ if $ad - bc = 0$. So $ad - bc \neq 0$.

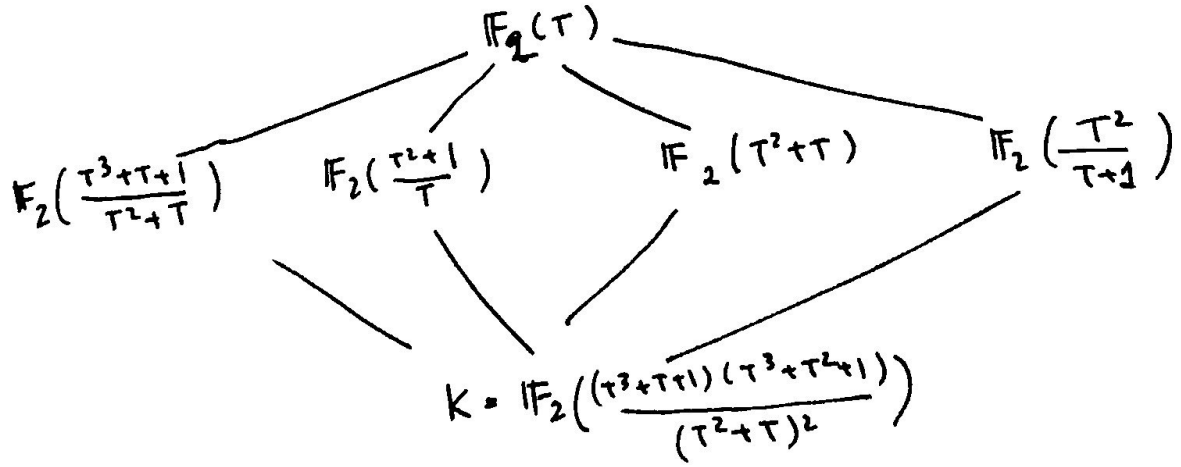
Therefore the group homomorphism $\psi: GL_2(k) \to \operatorname{Aut}(k(T)/k)$ given by $\psi\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(T) = \frac{aT+b}{cT+d}$ is surjective.

Note that $\psi\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = id_{k(T)}$ if and only if $a=d$ & $b=c=0$.
So $\ker \psi = \left\{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) : a \neq 0\right\} \simeq k^\times$. Hence $Aut(k(T)/k) \simeq PGL_2(k)$.

let $k = \mathbb{F}_q$ $(q = p^m)$. Note that $|PGL_2(\mathbb{F}_q)| = q\cdot(q-1)(q+1)$. (why?)
Consider $q=2$ case. Then $PGL_2(\mathbb{F}_2)$ is a non-abelian group of order 6. So $PGL_2(\mathbb{F}_2) \simeq S_3$, and its subgroups look like as follows:



let $K = \mathbb{F}_q(T)^{PGL_2(\mathbb{F}_2)}$. Then $\mathbb{F}_q(T) \mid K$ is Galois with Galois group isomorphic to $PGL_2(\mathbb{F}_2)$.
One may calculate K to be $\mathbb{F}_q\left(\frac{(T^3+T+1)(T^3+T^2+1)}{(T^2+T)^2}\right)$.
The other intermediate fields are as follows:



Linear Disjointness

Definition: Let k be a field and K, L its extensions. We say that K is linearly disjoint from L over k if the following is satisfied for all $a_1, \dots, a_n \in K$:

$$a_1, \dots, a_n \text{ are lin. indep. over } k \implies a_1, \dots, a_n \text{ are lin. indep over } L.$$

When this is the case, we write $K \perp_k L$.

Proposition: For field extensions K/k and L/k we have

$$K \perp_k L \iff L \perp_k K.$$

Proof: Suppose that $K \perp_k L$, and let $y_1, \dots, y_n \in L$ be linearly independent over k. Suppose, for a contradiction that there are $x_1, \dots, x_n \in k$ such that $x_1 y_1 + \cdots + x_n y_n = 0$ and not all x_i are zero. Without loss of generality, $x_1, \dots, x_r$ are linearly independent over k and $x_{r+1}, \dots, x_n$ are in $\mathrm{Span}_k(x_1, \dots, x_r)$. Say $x_i = \sum_{j=1}^{r} a_{ij} x_j$ for $i > r$ with $a_{ij} \in k$. Therefore $x_1 y_1 + \cdots + x_r y_r + \sum_{i=r+1}^{n} \sum_{j=1}^{r} a_{ij} x_j y_i = 0$. This gives

$$\sum_{j=1}^{r} \left(y_j + \sum_{i=r+1}^{n} a_{ij} y_i \right) x_j = 0,$$ and hence $y_j + \sum_{i=r+1}^{n} a_{ij} y_i = 0$ for all $j = 1, \dots, r$, since $K \perp_k L$. However, this means that $y_1, \dots, y_n$ are not linearly independent over k. ∎

Theorem: Let k be a field with extensions K, L. Then the following are equivalent:

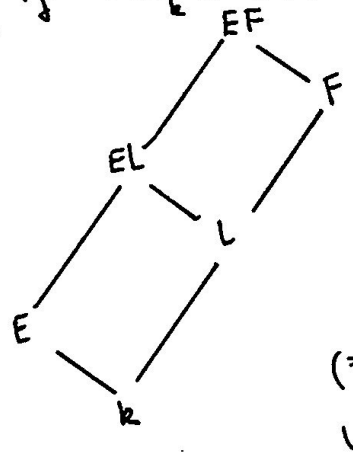
(1) $K \perp_k L$

(2) If R, S are rings with K, L are fractions fields of them, and if $a_1, \dots, a_n \in R$ are linearly independent over k, then $a_1, \dots, a_n$ are linearly indep over R.

(3) Suppose that $R \subseteq K$ is a vector space over k with basis B such that the fraction field of R is K. Then B is linearly indep. over L.

Proof: Straightforward calculations. ∎

Theorem: Let $k \subseteq E$, $k \subseteq L \subseteq F$ be fields. Then $E \perp_k F$ if and only if $E \perp_k L$ and $EL \perp_L F$.



Proof: ($\Leftarrow$) Let $X \subseteq E$ be linearly indep. over k. Then X is lin. indep over L. Considered as a subgroup of EL, it is independent over F.

($\Rightarrow$) $E \perp_k L$ is automatic.

Let $EL = L(R)$ where $R = L[E]$. Note that a linear basis of E as a k-vector space is also a basis of R as an L-vector space. Such a basis remains linearly independent over F, by assuption that $E \perp_k F$. Then $EL \perp_k F$ by the previous theorem. ∎

Definition: Let K/k and L/k be field extensions. We say that K is free from L over k if every algebraically independent (over k) subset $X \subseteq K$ remains algebraically independent over L.
We denote this as $K \downarrow_k L$.

Proposition: Let K/k and L/k be field extensions. Then $K \downarrow_k L$ if and only if $L \downarrow_k K$.

Proof: Similar to the corresponding result for linear disjointness. ∎

Theorem: Let $K|k$ and $L|k$ be extensions such that $K \perp_k L$. Then $K \downarrow_k L$.

Proof: Suppose that $x_1, \dots, x_n \in K$ are alg. dependent over L; say $\sum_{\vec{i} \in I} \beta_{\vec{i}} \vec{x}^{\vec{i}} = 0$ where I is a finite set of multi-indices and $\beta_{\vec{i}} \in L$ for each $\vec{i} \in I$, not all 0. But then $\{\vec{x}^{\vec{i}} : \vec{i} \in I\}$ is linearly dependent over L, hence over k. This means that $x_1, \dots, x_n$ are alg. dependent over k. ∎

Proposition: Let $u_1, \dots, u_n$ be in some field containg L such that they are algebraically independent over L. Then $k(u_1, \dots, u_n) \perp_k L$.

Proof: A linear basis of $k[u_1, \dots, u_n]$ over k consists of monomials of $\vec{u} = (u_1, \dots, u_n)$. They remain linearly independent over L. Hence $k(u_1, \dots, u_n) \perp_k L$. ∎

Separable Extensions

Definition: Let $K|k$ be a finitely generated extension. A separating basis of $K|k$ is a transcendental basis S of $K|k$ such that $K|k(S)$ is separable.

Definition: Let k be a field of characteristic $p > 0$, and let $m > 0$. We define $A_m := \{\alpha \in \bar{k} : \alpha^{p^m} \in k\}$ and $k^{1/p^m} := k(A_m)$. We also define $k^{1/p^\infty} = \bigcup_{m>0} k^{1/p^m}$.

Clearly, $k^{1/p^m} \subseteq k^{1/p^{m+1}}$; and hence k^{1/p^∞} is a field.

Theorem: Let K/k be a field extension. Then TFAE:

(i) $K \perp_k k^{1/p^\infty}$.

(ii) $K \perp_k k^{1/p^m}$ for some $m>0$.

(iii) Every subfield of k that is finitely generated over k has a separating basis over k.

Proof: (i $\Rightarrow$ ii) Clear.

(ii $\Rightarrow$ iii) Let L be finitely generated subfield of K over k; say $L = k(x_1, \dots, x_n)$. If $\operatorname{trdeg}(L/k) = n$, then $x_1, \dots, x_n$ are algebraically independent over k, and hence is a separating basis of L over k.

So let's assume that $r := \operatorname{trdeg}(L/k) < n$; without loss of generality $x_1, \dots, x_r$ is a transcendence basis of L over k. Let $f \in k[X_1, \dots, X_{r+1}]$ be a polynomial with lowest degree such that $f(x_1, \dots, x_r, x_{r+1}) = 0$. Then f is irreducible. Suppose that each appearance of each X_i in f is a p^{th} power. Then $f = \sum_{\vec{i} \in I} c_{\vec{i}} (\vec{X}^{\vec{i}})^p$ where I is a finite set of multi-indices and $c_{\vec{i}} \in k$. For each $\vec{i} \in I$, let $d_{\vec{i}} \in \overline{k}$ be such that $d_{\vec{i}}^p = c_{\vec{i}}$. Then $d_{\vec{i}} \in k^{1/p}$, and $f(x_1, \dots, x_{r+1}) = \sum_{i \in I} d_i^p (\vec{x}^i)^p = \left(\sum_{i \in I} d_i \vec{x}^i \right)^p$.

Therefore $\{ \vec{i}^{\,i} : i \in I \}$ is linearly dependent over $k^{1/p}$; hence by assumption they are linearly dependent over k. But this is against f being of lowest degree. Therefore there is X_i that doesn't appear in f as a p^{th} power; without loss of generality let $i=1$. Consider $f(X_1, x_2, \dots, x_{r+1}) \in k(x_2, \dots, x_{r+1})[X_1]$. This is the minimal polynomial of x_1 over $k(x_2, \dots, x_{r+1})$ (after dividing by an elements of k). Hence x_1 is separable over $k(x_2, \dots, x_{r+1})$, and so over $k(x_2, \dots, x_n)$.

If $\operatorname{trdeg}(L/k) = n-1$, then we are done. Otherwise we continue the same process with $x_2, \dots, x_n$ to eventually get a separating basis for L over k.

(iii $\to$ i) It suffices to prove that every subfield of K that is finitely generated over k is linearly disjoint from k^{1/p^∞}.

So let $L \subseteq K$ be finitely generated over k with a separating basis $u_1, \dots, u_n$. Note that $u_1, \dots, u_n$ remain algebraically independent over k^{1/p^∞}. So $k(\vec{u}) \perp_k k^{1/p^\infty}$.

We know that $L = k(\vec{u})(\alpha)$ for some $\alpha \in L$; say α is of degree d over $k(\vec{u})$. Then $1, \alpha, \dots, \alpha^{d-1}$ is a linear basis of L over $k(\vec{u})$. It's clear that $1, \alpha, \dots, \alpha^{d-1}$ remain linearly independent over $k(\vec{u}) \cdot k^{1/p^\infty} = k^{1/p^\infty}(\vec{u})$ since $k^{1/p^\infty}(\vec{u}) \,|\, k(\vec{u})$ is purely inseparable. Therefore $L \perp_{k(u)} k^{1/p^\infty}(\vec{u})$, and hence $L \perp_k k^{1/p^\infty}$. ∎

An extension K/k satisfying one of the three conditions of this theorem is called <u>separable</u>. It's easy to see that if K/k is algebraic, then it's separable with the original definition if and only if it's separable with this definition. (It's easiest to use iii to see this.)

Below we list some properties of separable extensions.

<u>Proposition</u>: Let K/k, E/k, L/k be extensions with $E \subseteq K$.

(1) If K/k is separable, then E/k is separable.

(2) If K/E and E/k are separable, then K/k is separable.

(3) If k is perfect (i.e $k^p = k$), then any extension of k is separable.

(4) If K/k is separable, and $K \perp_k L$, then KL/L is separable.

(5) If K/k and L/k are separable, and $K \perp_k L$, then KL/k is separable.

(6) Let $K \perp_k L$. Then K/k is separable if and only if KL/L is separable.

Proof: (1) Clear.

(2) Note that $E \cdot k^{1/p^\infty} \subseteq E^{1/p^\infty}$. If $K \perp_E E^{1/p^\infty}$, then $K \perp_E E \cdot k^{1/p^\infty}$. Also if $E \perp_k k^{1/p^\infty}$, then $K \perp_k k^{1/p^\infty}$. This finishes the proof.

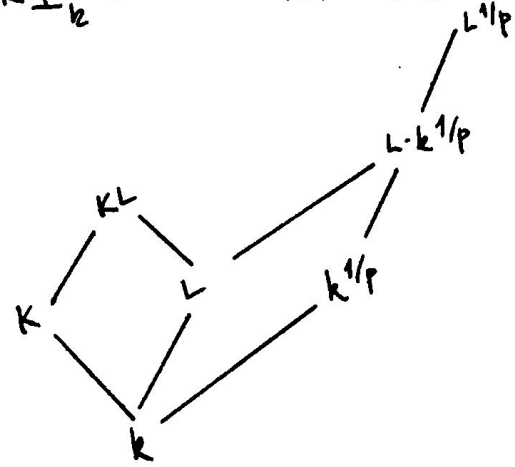
(3) If $k^p = k$, then $k^{1/p^\infty} = k$; and $K \perp_k k$ for any extension K.

(4) A finitely generated (over L) subfield of KL is of the form FL where $F \subseteq K$ is finitely generated over k. So let $\{t_1, \dots, t_n\}$ be a separating basis of F over k. Since $K \perp_k L$, $\{t_1, \dots, t_n\}$ remains algebraically indep. over L and hence it is a basis over L. It also follows that $FL \mid L(t_1, \dots, t_n)$ is separable. Hence $KL \mid L$ is separable.

(5) Since $K \mid k$ is separable and $K \perp_k L$, we have $KL \mid L$ is separable. Hence $KL \mid k$ is separable by (2).

(6) Since $K \perp_k L$ implies $K \downarrow_k L$, we get $\Rightarrow$ by (4).

($\Leftarrow$) Suppose that $K \not\downarrow_k k^{1/p}$. Then $K \not\downarrow_k L \cdot k^{1/p^\infty}$ and hence $KL \not\downarrow_L L k^{1/p^\infty}$. If $KL \mid L$ is separable, then $KL \perp_L L^{1/p}$. Then $K \perp_k L^{1/p}$ and $K \perp_k L \cdot k^{1/p}$. But this contradicts $KL \perp_L L \cdot k^{1/p}$. (See picture below.) ∎



Proposition: Let $K \mid k$ be finitely generated. If $K^{p^m} \cdot k = K$ for some $m > 0$, then $K \mid k$ is separable algebraic. Conversely if $K \mid k$ is separable algebraic, then $K^{p^m} \cdot k = K$ for some $m > 0$.

Definition: An extension $K|k$ is called **regular** if it is separable and for any $\alpha \in K$ if α is algebraic over k, then $\alpha \in k$.

The second condition can simply be interpreted as "k is algebraically closed in K".

Theorem: An extension $K|k$ is regular if and only if $K \perp_k \bar{k}$.

Proof: ($\Leftarrow$) If $K \perp_k \bar{k}$, then in particular $K \perp_k k^{1/p}$. So $K|k$ is separable,
Also $K \cap \bar{k} = k$, and hence k is algebraically closed in K.

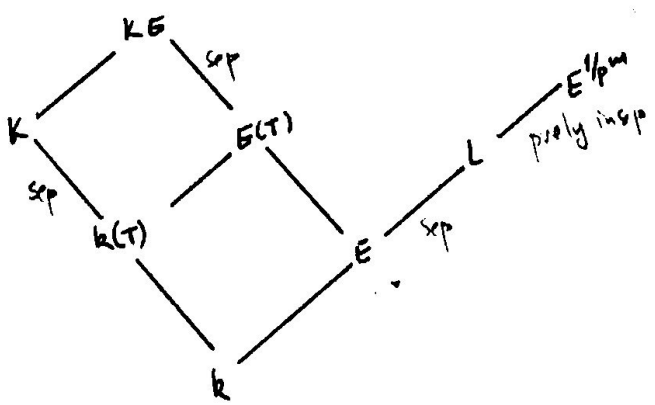
($\Rightarrow$) First a lemma:

Lemma: Let k be algebraically closed in K. Let α be an element in some extension of k that is algebraic over k. Then $k(\alpha) \perp_k K$ and $[k(\alpha):k] = [K(\alpha):K]$.

Proof: The minimal polynomial of α over k is also the minimal polynomial over K. Hence $[K(\alpha):K] = [k(\alpha):k]$ and since $1, \alpha, \ldots, \alpha^d$ forms a basis of $k(\alpha)$ over k, it also forms a basis of $K(\alpha)$ over K.
So $k(\alpha) \perp_k K$. ∎

Let's assume that $K|k$ is regular, and let $L|k$ be finite extension.
We'd like to show that $K \perp_k L$.

Let $E \subseteq L$ be the maximal separable extension of k (in L). Then $L|E$ is purely inseparable, and hence $L \subseteq E^{1/p^m}$ for some $m > 0$.
We have the following picture:



Here T is a separating basis of K over k.
So $K|k(T)$ is separable.
Since $E|k$ is separable, it is gen. by one element over k and $K \perp_k E$ by the lemma
Also T remains a separating basis of KE over E.
Hence $KE|E$ is separable, and $KE \perp_E E^{1/p^m}$. Then $KE \perp_E L$ & $K \perp_k L$. ∎

Proposition: Let $k \subseteq E \subseteq K$ be fields. If K/k is regular, then E/k is regular. If both K/E and E/k regular, then K/k is regular

Proof: The first is clear.
For the second statement, note that $E\bar{k} \subseteq \bar{E}$. So if $K \perp_E \bar{E}$, then $K \perp_{\bar{E}} E\bar{k}$.
Also if $E \perp_k \bar{k}$, then $K \perp_k \bar{k}$ and K/k is regular. ∎

Proposition: If k is algebraically closed, then any extension of k is regular.

Proof: Trivial. ∎

Theorem: Let K/k be regular and $K \not\perp_k L$. Then $K \perp_k L$.

Proof: ...

Theorem: Suppose that K/k is regular and $K \not\perp_k L$, Then KL/L is regular.

Proof: If $K \not\perp_k L$, then $K \not\perp_k \bar{L}$ as a general fact. When K/k is regular, we get that $K \perp_k \bar{L}$. Then $KL \perp_L \bar{L}$, meaning KL/L is regular. ∎

Corollary: ① Let K/k and L/k be regular, and $K \not\perp_k L$. Then KL/k is regular.

② Let $K = k(\alpha_1, \dots, \alpha_n)$ be a finitely generated regular extension with $K \not\perp_k L$. Then the natural k-algebra homomorphism $L \otimes_k k[\vec{\alpha}] \to L[\vec{\alpha}]$ is an isomorphism.

Proof: ① We have both KL/L and KL/K are regular by the previous theorem. Then KL/k is regular by the proposition above.

② This map is always surjective, and it's injective if and only if $L \perp_k K$ But if $K \not\perp_k L$ and K/k is regular, then $K \perp_k L$ by the theorem above. ∎

From this point on all rings are commutative; even though many things in the beginning works for non-commutative rings as well. Also most of the times, we assume that the rings have a (multiplicative) unit as well.

Definition: • An R-module M is Noetherian if every chain $A_1 \subseteq A_2 \subseteq \cdots$ of R-submodules of M stabilizes: there is $m>0$ such that $A_i = A_m$ for all $i \geq m$. (This property is sometimes called the Ascending Chain Condition (ACC) for submodules.)

• An R-module M is Artinian if every chain $A_1 \supseteq A_2 \supseteq \cdots$ of R-submodules of M stabilizes. (This property is called the Descending Chain Condition (DCC) for submodules.)

A ring R is an R-module in a natural way and R-submodules are exactly the ideals. We say that a ring R is Noetherian/Artinian if it has ACC/DCC for ideals.

Examples: ① $\mathbb{Z}$ is Noetherian: ideals are exactly the subgroups and they are $m\mathbb{Z}$ for some $m \geq 0$ and $m\mathbb{Z} \subseteq n\mathbb{Z}$ iff $n \mid m$.
Clearly, it is not Artinian.

② Any field is Noetherian and Artinian since the only ideals are $\{0\}$ and everything.

③ Prüfer p-group is not Noetherian:

$$\mathbb{Z}(p^\infty) := \{ \alpha \in \mathbb{C}^\times : \alpha^{p^n} = 1 \text{ for some } n>0 \} = \{ e^{k2\pi i/p^n} : n>0,\ k \in \{0, \dots, p^n-1\} \}.$$

Again ideals are subgroups, and for any $n>0$, $\mathbb{Z}(p^n) = \{ x : x^{p^n} = 1 \}$ is a subgroup, and $\mathbb{Z}(p^m) \subseteq \mathbb{Z}(p^n)$ iff $m \leq n$.
One may show that $\mathbb{Z}(p^\infty)$ is Artinian.

④ Any PID is Noetherian. Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals. Let $I = \bigcup_{i=1}^{\infty} I_i$. Then I is an ideal, hence $I = \langle a \rangle$ for some $a \in R$. But then $a \in I_m$ for some $m>0$. Then $I_i = I_m$ for all $i \geq m$. A particular example is $k[x]$ for a field k. Later we'll see that any

polynomial ring over a Noetherian ring is Noetherian. (Hilbert Basis Th.)

Theorem: An R-module M is Noetherian if and only if every non-empty set of submodules of M contains a maximal element.

Proof: ($\Rightarrow$) let S be a non-empty set of submodules of M ; partially ordered by set inclusion. If S has no maximal element, then using Zorn's lemma S has a chain that doesn't have an upper bound in S. That chain gives an ascending chain of submodules, which is against Noetherianity.

($\Leftarrow$) let $A_1 \subseteq A_2 \subseteq \cdots$ be a chain of submodules of M. Then $S = \{A_i : i = 1, 2, \ldots\}$ has a maximal element, say A_m. Then $A_i = A_m$ for all $i \geq m$. ∎

Proposition: let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be an exact sequence of R-modules. Then B is Noetherian iff both A and C are Noetherian.

Proof: ($\Rightarrow$) let B be Noetherian. Then it's clear that A is Noetherian. let $C_1 \subseteq C_2 \subseteq \cdots$ be an ascending chain of submodules of C. Let $B_i = g^{-1}(C_i)$ Then $B_1 \subseteq B_2 \subseteq \cdots$ is an ascending chain of submodules. Let $m > 0$ be such that $B_i = B_m$ for all $i \geq m$. Since g is surjective, we have $C_i = C_m$ for all $i \geq m$.

($\Leftarrow$) let A and C be Noetherian. Let $B_1 \subseteq B_2 \subseteq \cdots$ be an ascending chain of submodules of B. let $A_i := f^{-1}(B_i \cap f(A))$ and $C_i := g(B_i)$. Then $A_1 \subseteq A_2 \subseteq \cdots$ and $C_1 \subseteq C_2 \subseteq \cdots$ Therefore there is $m > 0$ such that $A_i = A_m$ and $C_i = C_m$ for $i \geq m$. We claim that $B_i = B_m$ for $i \geq m$. We have the following diagram for $i \geq m$:

$$\begin{array}{ccccccc} 0 & \to & A_m & \xrightarrow{f_m} & B_m & \xrightarrow{g_m} & C_m \to 0 \\ & & \downarrow \mathrm{id} & & \downarrow & & \downarrow \mathrm{id} \\ 0 & \to & A_i & \xrightarrow{f_i} & B_i & \xrightarrow{g_i} & C_i \to 0 \end{array}$$

Let $b \in B_i$. We claim that $b \in B_m$. Consider $c = g_i(b) \in C_i = C_m$. So let $b' \in B_m$ s.t. $g_m(b') = c = g_i(b)$. Then $b - b' \in \ker g_i = \mathrm{Im} f_i$. Let $a \in A_i$ s.t. $f_i(a) = b - b_i$ But $a \in A_m$. So $f_m(a) = b - b_i$ is in B_m. So $b \in B_m$. ∎

Corollary: ① An R-module M is Noetherian if and only if for every/some submodule N, both N and M/N are Noetherian.

② If $A_1, \cdots, A_n$ are Noetherian, then so is $A_1 \times A_2 \times \cdots \times A_n$.

③ If R is a Noetherian ring, then any finitely generated free R-module is also Noetherian.

Proposition: Let R be a Noetherian ring with identity. Then any finitely generated R-module is Noetherian.

Proof: If M is a finitely generated R-module, then there is a surjective $g: R^n \to M$. Then we have a short exact sequence $0 \to \ker g \to R^n \to M \to 0$. Then M is Noetherian by the previous proposition. ☐

Theorem: Let M be an R-module. Then M is Noetherian if and only if every submodule of M is finitely generated. (Here we do not assume that R has identity.)

Proof: ($\Rightarrow$) Let N be a submodule of M and let S be the set of finitely generated submodules of N. Note that $S \neq \emptyset$ since $\{0\} \in S$. Then S has a maximal element; say $C = \langle a_1, \cdots, a_n \rangle$. We claim that $C = N$. Let $b \in N$. Then $\langle b, a_1, \cdots, a_n \rangle$ is finitely generated, and contains C. Thus $\langle b, a_1, \cdots, a_n \rangle = C$ and hence $b \in C$.

($\Leftarrow$) Let $A_1 \subseteq A_2 \subseteq \cdots$ be an ascending chain of submodules of M. Then $N = \bigcup_{i=1}^{\infty} A_i$ is a submodule of M. Thus $N = \langle a_1, \cdots, a_n \rangle$ for some $a_1, \cdots, a_n \in N$. Therefore $N = A_m$ for some $m > 0$ with $a_1, \cdots, a_n \in A_m$. ☐

Corollary: A ring is Noetherian if and only if its every ideal is finitely generated.

Prime and Primary Ideals

Recall that an ideal P of R is called prime if $P \neq R$ and for any $x, y \in R$ one of x or y is in P provided that $x \cdot y \in P$. This is equivalent to the ring R/P being an integral domain or to the condition that $R \setminus P$ is a multiplicative subset of R. Another condition is that if $IJ \subseteq P$, then either $I \subseteq P$ or $J \subseteq P$.
Here is a technical result on multiplicative subsets.

Proposition: Let $S \subseteq R$ be a multiplicative set, and let I be an ideal of R with $S \cap I = \emptyset$. Then there is an ideal $P \subseteq R$ which is maximal in the set of ideals that are disjoint from S and contain I. Moreover every such maximal ideal is a prime ideal.

Proof: Let $\mathcal{C} = \{ J : J \subseteq R \text{ an ideal } I \subseteq J \text{ \& } J \cap S = \emptyset \}$. Clearly, $\mathcal{C} \neq \emptyset$ as $I \in \mathcal{C}$ and the union of every chain in $\mathcal{C}$ is again in $\mathcal{C}$. So $\mathcal{C}$ has a maximal element by Zorn's lemma.

Let P be such a maximal element of $\mathcal{C}$. Let $I \cdot J \subseteq P$. Suppose for a contradiction that $I \not\subseteq P$ and $J \not\subseteq P$. Then $P \subsetneq P + I$ and $P \subsetneq P + J$. So $P + I \cap S \neq \emptyset$ and $P + J \cap S \neq \emptyset$; say $s_1 = p_1 + a$, $s_2 = p_2 + b$ are in S with $p_1, p_2 \in P$, $a \in I$, $b \in J$. Then $s_1 \cdot s_2 = p_1 p_2 + p_1 b + p_2 a + ab \in S$. But $s_1 s_2 \in P + IJ$. So $s_1 \cdot s_2 \in P$, which is a contradiction. So P is prime. ∎

Proposition: Let $K \subseteq R$ be a subring such that $K \subseteq P_1 \cup \cdots \cup P_n$ for some prime ideals $P_1, \ldots, P_n$. Then $K \subseteq P_i$ for some i.

Proof: Suppose that $K \not\subseteq P_i$ for any i, and assume that n is minimal. So let $a_i \in K \setminus \bigcup_{j \neq i} P_j$. Then $a_i \in P_i$. Consider $a_1 + a_2 a_3 \cdots a_n \in K \subseteq P_1 \cup \cdots \cup P_n$; say $a_1 + a_2 \cdots a_n \in P_j$. If $j > 1$, then $a_1 \in P_j$. So $j = 1$; but then $a_2 \cdots a_n \in P_1$ and hence $a_i \in P_1$ for some $i > 2$: Another contradiction. ∎

Proposition: Any ideal that is maximal among non-finitely generated ideals is a prime ideal.

(Such ideal might not exist.)

Proof: Let P be such an ideal. Suppose that it is not prime, and take $a,b \in R$ with $ab \in P$, $a \notin P$, $b \notin P$. Then the ideals $P+\langle a\rangle$ and $P+\langle b\rangle$ are finitely generated; say $P+\langle a\rangle = \langle p_1+r_1a, \dots, p_m+r_ma\rangle$ and $P+\langle b\rangle = \langle q_1+s_1b, \dots, q_n+s_nb\rangle$

Let $J = \{r \in R : ra \in P\}$; this is an ideal of R. Also $(q_i+s_ib)a \in P$, and hence $P+\langle b\rangle \subseteq J$. So J is finitely generated, say $J = \langle c_1, \dots, c_k\rangle$. We claim that P is generated by $p_1, \dots, p_m, c_1a, \dots, c_ka$. This will give a contradiction as P is not finitely generated and will conclude the proof.

Let $x \in P$. Then $x \in P+\langle a\rangle$. Write $x = \sum_{i=1}^{m} t_i(p_i+r_ia)$. Then $x = \sum_{i=1}^{m} t_ip_i + \sum_{i=1}^{m} t_ir_ia$. Note that the first summand is in P. Then so is the second one: $a\sum_{i=1}^{m} t_ir_i \in P$. So $\sum_{i=1}^{m} t_ir_i \in J$; say $\sum_{i=1}^{m} t_ir_i = \sum_{j=1}^{k} u_jc_j$.

Then $x = \sum_{i=1}^{m} t_ip_i + \sum_{j=1}^{k} u_jc_ja \in \langle p_1, \dots, p_m, c_1a, \dots, c_ka\rangle$. ∎

Definition: For an ideal I of R define the radical (or nilradical) of I to be:

$$\mathrm{Rad}(I) := \bigcap_{\substack{I \subseteq P \\ P \text{ prime}}} P .$$

Example: Let $R = \mathbb{Z}$ and $I = 12\mathbb{Z}$. Then $\mathrm{Rad}(I) = 2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$. We see from this example that the radical itself is not necessarily a prime ideal.

Theorem: Let I be an ideal of R. Then $\mathrm{Rad}(I) = \{r \in R : r^n \in I \text{ for some } n>0\}$

Proof: ($\supseteq$) If there is no prime ideal containing I, then $\{r \in R : r^n \in I \text{ for some } n\} \subseteq R = \operatorname{Rad} I$. Otherwise let $P \supseteq I$ be a prime. If $r^n \in I$, then $r^n \in P$, and hence $r \in P$. Thus such $r \in \operatorname{Rad} I$.

($\subseteq$) Suppose that $r \in R$ such that $r^n \notin I$ for any $n > 0$. Let $S = \{r^n + x : n > 0, x \in I\}$. Then S is a multiplicative set with $S \cap I = \emptyset$. By an earlier proposition take a maximal $P \supseteq I$ with $P \cap S = \emptyset$, which in turn is prime. Thus $r^n \notin P$ and hence $r \notin \operatorname{Rad}(I)$. ∎

Corollary: Let $I, J, I_1, \dots, I_m \subsetneq R$ be ideals. Then we have the following:

① $\operatorname{Rad}(\operatorname{Rad}(I)) = \operatorname{Rad}(I)$

② If $I \subseteq J$, then $\operatorname{Rad}(I) \subseteq \operatorname{Rad}(J)$

③ $\operatorname{Rad}(I_1 \cdots I_m) = \operatorname{Rad}(I_1 \cap \cdots \cap I_m) = \bigcap_{i=1}^{m} \operatorname{Rad}(I_i)$.

④ $\operatorname{Rad}(I^m) = \operatorname{Rad}(I)$.

Proof: ① Clear, by the theorem.

② Clear by definition.

③ $\bigcap_{i=1}^{m} \operatorname{Rad}(I_i) \subseteq \operatorname{Rad}(I_1 \cdots I_m)$ is clear. $\operatorname{Rad}(I_1 \cdots I_m) \subseteq \operatorname{Rad}(I_1 \cap \cdots \cap I_m)$ is clear by part ②. $\operatorname{Rad}(I_1 \cap \cdots \cap I_m) \subseteq \bigcap_{i=1}^{m} \operatorname{Rad} I_i$ is clear by the theorem.

④ Clear by part ③. ∎

Definition: A proper ideal $Q \subseteq R$ is called primary if for given $a, b \in R$ $b^n \in Q$ for some $n > 0$ provided that $ab \in Q$ and $a \notin Q$.

Example: $R = \mathbb{Z}$; $Q = p^n\mathbb{Z}$ is primary for any prime p.

Proposition: Let $Q \subseteq R$ be primary. Then $\operatorname{Rad}(Q)$ is prime.

Proof: Suppose that $a, b \in R$ are such that $a \cdot b \in \operatorname{Rad}(Q)$ and $a \notin \operatorname{Rad} Q$. Then $(ab)^n = a^n b^n \in Q$ for some $n > 0$. But $a^n \notin Q$, so $(b^n)^m \in Q$ for some $m > 0$. Therefore $b \in \operatorname{Rad} Q$. ∎

If $P = \mathrm{Rad}(Q)$ for some primary ideal $Q \subseteq R$, then we say Q is a primary ideal belonging to P, or Q is primary for P, or P is the associated prime for Q.

Proposition: Let Q, P be ideals of R. Then Q is primary for P if and only if $Q \subseteq P \subseteq \mathrm{Rad}(Q)$, and for every $a, b \in R$ we have $b \in P$ if $ab \in Q$ and $a \notin Q$.

Proof: ($\Rightarrow$) Clear.

($\Leftarrow$) Let $ab \in Q$ and $a \notin Q$. Then $b \in P \subseteq \mathrm{Rad}(Q)$ and hence $b^n \in Q$ for some $n > 0$. Therefore Q is primary.

Now let $b \in \mathrm{Rad}\, Q$, and let $b^n \in Q$ for a minimal $n > 0$. If $n = 1$, then $b \in Q \subseteq P$. If $n > 1$, then $b^n = b^{n-1} b \in Q$ and $b^{n-1} \notin Q$. So $b \in P$. ∎

Proposition: Let $Q_1, \dots, Q_n \subseteq R$ be primary for P. Then $Q_1 \cap \dots \cap Q_n$ is also primary for P.

Proof: Let $Q := Q_1 \cap \dots \cap Q_n$. Then $\mathrm{Rad}(Q) = \bigcap_{i=1}^{n} \mathrm{Rad}(Q_i) = P$.

So $Q \subseteq P \subseteq \mathrm{Rad}(Q)$. Let $a, b \in R$ with $ab \in Q$ and $a \notin Q$. Then $ab \in Q_i$ for each i and $a \notin Q_j$ for some j. Applying the previous proposition to Q_j, we get that $b \in P$, proving that Q is primary for P. ∎

Next we introduce the concept of primary in the generality of R-modules.

Definition: Let A be an R-module. A (proper) submodule B of A is called primary if for every $r \in R$ and $a \in A \setminus B$, we have

$$ra \in B \Rightarrow r^n A \subseteq B \text{ for some } n > 0.$$

Exercise: Check that this definition really generalizes the previous definition. This means that an ideal I of R is primary if and only if it is a primary submodule of the R-module R.

Proposition: Let A be an R-module and let B be a primary submodule of A. Then $Q_B := \{r \in R : rA \subseteq B\}$ is a primary ideal of R.

Proof: First note that $1 \notin Q_B$ since $B \subsetneq A$, and hence $Q_B \neq R$. Now let $rs \in Q_B$ and $s \notin Q_B$. Then $rsA \subseteq B$ and $sA \not\subseteq B$. Say $sb \in B$ such that $sb \notin A$. Then $r^n A \subseteq B$ for some $n > 0$. Therefore $r^n \in Q_B$. ∎

Based on this proposition, we may give the following definition.

Definition: Let A be an R-module and $B \subsetneq A$ a primary submodule. Let $P = \mathrm{Rad}(Q_B)$; Q_B is primary for P. Then we say B is *P-primary*.

Definition: Let A be an R-module, and $C \subseteq A$ a submodule. We say that C has a *primary decomposition* if $C = B_1 \cap \cdots \cap B_n$, where each B_i is a primary submodule of A.
Such a decomposition is said to be *reduced* if $\bigcap_{j \neq i} B_j \not\subseteq B_i$ for each i, and $\mathrm{Rad}(Q_{B_i}) \neq \mathrm{Rad}(Q_{B_j})$ for $i \neq j$.

Exercise: Show that any primary decomposition can be reduced to a reduced primary decomposition. (Just note that if B_i, B_j are P-primary, then so is $B_i \cap B_j$.)

Our longer term goal is to show that Noetherian R-modules have (reduced) primary decompositions. But first we would to prove that reduced primary decompositions are somehow unique.

Definition: Let $A, C, B_1, \ldots, B_n$ be as in the definition above, and let $P_i = \mathrm{Rad}(Q_{B_i})$. We say that P_i is an *isolated prime of C* if $P_j \not\subseteq P_i$ for any $j \neq i$. Otherwise, we say P_i is *embedded*.

Theorem (Uniqueness): Let A be an R-module, and $C \subseteq A$ submodule with reduced primary decompositions: $C = B_1 \cap \cdots \cap B_m = B_1' \cap \cdots \cap B_n'$.
Then $m = n$ and $P_i = P_i'$ after reordering. If P_i is isolated, then $B_i = B_i'$.

Proof: After reordering indices let P_1 be maximal among $P_1, P_2, \dots, P_m, P_1', \dots, P_n'$.
Therefore $P_1 \not\subseteq P_i$ for $i \in \{2, \dots, m\}$ since the decomposition is reduced.
Suppose also that $P_1 \not\subseteq P_j'$ for $j \in \{1, \dots, n\}$. Then $P_1 \not\subseteq P_2 \cup \dots \cup P_m \cup P_1' \cup \dots \cup P_n'$ using an earlier proposition. Let $r \in P_1 \setminus (P_2 \cup \dots \cup P_m \cup P_1' \cup \dots \cup P_n')$.
This means that $r^n A \subseteq B_1$ for some $n > 0$.
Define $C^* := \{ x \in A : r^n x \in C \}$. Clearly, $C \subseteq C^*$.
If $k=1$, then $C^* = A$. Suppose $k > 1$ and let $x \in B_2 \cap \dots \cap B_m$.
Then $r^n x \in (B_2 \cap \dots \cap B_m) \cap B_1 = C$ and hence $x \in C^*$. And conversely if $x \notin B_2 \cap \dots \cap B_m$, then $x \notin B_i$ for some $i \in \{2, \dots, m\}$ and $r^n x \notin B_i$. (Otherwise $r^n \in P_i$ and hence $r \in P_i$, which is not the case.) Then $x \notin C^*$, and $C^* = B_2 \cap \dots \cap B_m$ for $k > 1$.
Using similar arguments, we may see that $C^* = B_1' \cap \dots \cap B_m'$, regardless of what k is. However, this is against reducedness. So $P_1 \subseteq P_j'$ for some $j \in \{1, \dots, n\}$. After re-ordering we have $P_1 = P_1'$.

Next we prove that $m = n$ by induction on m. If $m = 1$ and $n > 1$, then we get $B_1 = C = B_1' \cap \dots \cap B_n'$, $C^* = A$, and $C^* = B_2' \cap \dots \cap B_n'$ from the arguments above; and once again this is against reducedness. So if $m = 1$, then $n = 1$.

Now suppose $m > 1$. Then $C^* = B_2 \cap \dots \cap B_m = B_1' \cap \dots \cap B_n'$. These are reduced primary decompositions of C^*. Therefore $m - 1 = n - 1$ and $P_i = P_i'$ for $i = 2, \dots m$ using the induction hypothesis.

Suppose after re-ordering that $P_1 = \mathrm{Rad}(Q_{B_1}) = \mathrm{Rad}(Q_{B_1'})$ is isolated. Therefore $P_j \not\subseteq P_1$ for all $j \in \{2, \dots, m\}$. Take $r_j \in P_j \setminus P_1$ for all j, and let $t := r_2 \cdots r_m \in (P_2 \cap \dots \cap P_m) \setminus P_1$. Then for every $j \in \{2, \dots, m\}$ there are $n_j, m_j > 0$ such that $t^{n_j} A \subseteq B_j$ & $t^{m_j} A \subseteq B_j'$. Let n be the maximum of n_j and m_j's. Then $t^n A \subseteq B_2 \cap \dots \cap B_m$ & $t^n A \subseteq B_2' \cap \dots \cap B_n'$

let $D := \{x \in A : t^n x \in C\}$. We claim that $D = B_1 = B_1'$.

If $x \in B_1$, then $t^n x \in B_1$ and $t^n x \in B_2 \cap \cdots \cap B_m$. So $B_1 \subseteq D$. Similarly $B_1' \subseteq D$. Let $x \in D$. Then $t^n x \in C \subseteq B_1$ and $t \notin P_1$. So we need to have $x \in B_1$. So $D \subseteq B_1$. Similarly $D \subseteq B_1'$ as well. So $B_1 = B_1'$ as desired. ▨

Theorem: Let A be a Noetherian R-module. Then every proper submodule of A has a (reduced) primary decomposition.

Proof: Suppose that there are proper submodules of A without primary decomposition. Using Noetherianity there is a maximal among such submodules; say $C \subsetneq A$. In particular, C itself is not primary. So there are $r \in R$ and $b \in A \setminus C$ such that $rb \in C$, but $r^n A \not\subseteq C$ for all $n > 0$.

For $n > 0$, let $A_n := \{x \in A : r^n x \in C\}$. Then $C \subsetneq A_1 \subseteq A_2 \subseteq \cdots$. Using Noetherianity once again there is $k > 0$ such that $A_i = A_k$ for all $i \geq k$. Note that $C \subsetneq A_k \subsetneq A$, and hence A_k has a primary decomposition by the maximality of C.

Now let $D := \{x \in A : x = r^k y + c$ for some $y \in A$ & $c \in C\}$. Then $C \subseteq D$, and $C \neq D$ since $r^k A \not\subseteq C$ and $D \neq A$ for the same reason. Therefore D has a primary decomposition as well.

We claim that $C = A_k \cap D$: Let $x \in A_k \cap D$. Then $x = r^k y + c$ for $y \in A, c \in C$ and $r^k x \in C$. Then $r^{2k} y + r^k c \in C$ and $r^{2k} y \in C$. So $y \in A_{2k} = A_k$ and $r^k y \in C$. So $x \in C$, and $A_k \cap D \subseteq C$. It's clear that $C \subseteq B_k \cap D$. Therefore $C = A_k \cap D$ has a primary decomposition, which is against the choice of C. So any proper submodule of A has a primary decomposition. ▨

Corollary: ① Let R be a Noetherian ring and A a finitely generated R-module. Then every proper submodule of A has a primary decomposition.

② If R is a Noetherian ring, then every proper ideal of R has a primary decomposition.

Lemma: A ring R is Noetherian iff every prime ideal of R is finitely generated.

Proof: ($\Rightarrow$) Trivial.

($\Leftarrow$) Just recall that a maximal non-finitely generated ideal is prime. ∎

Definition: Let A be an R-module. The annihilator of A (in R) is

$$\mathrm{Ann}_R(A) := \{ r \in R : ra = 0 \text{ for all } a \in A \}.$$

Clearly, $\mathrm{Ann}_R(A)$ is an ideal of R.

Proposition: Let A be a finitely generated R-module. Then A is Noetherian if and only if $R/\mathrm{Ann}_R(A)$ is a Noetherian ring.

Proof: Let $I := \mathrm{Ann}_R(A)$. Note that A is also an R/I-module.

Suppose that $A = \langle a_1, \dots, a_n \rangle = Ra_1 + \cdots + Ra_n$, and let $I_i := \mathrm{Ann}_R(Ra_i)$. Then $I = \bigcap_{i=1}^{n} I_i$, and by Chinese Remainder Theorem we have an injective ring morphism $R/I \to R/I_1 \times \cdots \times R/I_n$, which in turn is also an R-module morphism.

Consider the map $f_i : R/I_i \to Ra_i$ defined by $f_i(\bar{r}) = ra_i$. This is well-defined and injective map. It's also clear that it is an R-module morphism & that it is surjective. Note that Ra_i is a Noetherian R-module (if A is). Hence $R/I_1 \times \cdots \times R/I_n$ is also Noetherian, and being isomorphic to a submodule of $R/I_1 \times \cdots \times R/I_n$, the R-module R/I is also Noetherian. As the ideals of R/I are also R-submodules, it follows that R/I is a Noetherian ring.

Now assume that R/I is a Noetherian ring. As noted above A is an R/I-module, and it is finitely generated as such. So A is Noetherian as an R/I-module. However, it's easy to see that R-submodules are R/I-submodules. Therefore A is Noetherian as an R-module as well. ∎

Lemma: Let A be a Noetherian R-module, and $P \subseteq R$ a prime ideal. If $C \subsetneq A$ is a P-primary submodule, then $P^m A \subseteq C$ for some $m > 0$.

Proof: Let $I := \mathrm{Ann}_R(A)$ & put $\bar{R} := R/I$. Then we know that $\bar{R}$ is a Noetherian ring.

Note that $I \subseteq \{r \in R : rA \subseteq C\} \subseteq P$. Therefore $\bar{P} := P/I$ is an ideal of $\bar{R}$. Note that both A and C are naturally $\bar{R}$-modules. We claim that C is primary $\bar{R}$-module with $\mathrm{Rad}(Q_C) = \bar{P}$; so $\bar{P}$ is automatically a prime ideal of $\bar{R}$. So let $\bar{r} \cdot a \in C$ and $a \notin C$. Then $ra \in C$, and so $r^n A \subseteq C$ for some $n > 0$. But then $\bar{r}^n A \subseteq C$ as well.

Also $\{\bar{r} \in \bar{R} : \bar{r}^k A \subseteq C \text{ for some } k > 0\} = \{\bar{r} \in \bar{R} : r^k A \subseteq C \text{ for some } k > 0\}$

$= \{\bar{r} \in \bar{R} : r \in P\} = \bar{P}$.

So C is $\bar{P}$-primary. Since $\bar{R}$ is Noetherian, $\bar{P}$ is finitely generated; say $\bar{P} = \langle \bar{r}_1, \dots, \bar{r}_k \rangle$. For each $i \in \{1, \dots, k\}$, take n_i with $\bar{r}_i^{n_i} A \subseteq C$, and let $n = n_1 + \cdots + n_k$. Then $\bar{P}^n A \subseteq C$, and hence $P^m A \subseteq C$. ∎

Theorem (Krull Intersection Theorem): Let A be a Noetherian R-module, and $I \subsetneq R$ an ideal. Put $B = \bigcap_{n>0} I^n A$. Then $IB = B$.

Proof: It's clear that $IB \subseteq B$.

If $IB = A$ then $A \subseteq B$ and hence $IB = A = B$. So suppose that $IB \neq A$, and let $IB = B_1 \cap \cdots \cap B_m$ be a primary decomposition with $P_i := \mathrm{Rad}(Q_{B_i})$. We'll show that $B \subseteq B_i$ for each i.

If $I \subseteq P_i$, then by the lemma above there is $m > 0$ such that $I^m A \subseteq P_i^m A \subseteq B_i$. Since $B \subseteq I^m A$, we are done in this case.

Suppose that $I \not\subseteq P_i$ & take $r \in I \setminus P_i$. Assuming $B \not\subseteq B_i$, we have $b \in B \setminus B_i$. But then $rb \in IB \subseteq B_i$ & $b \notin B_i$, and hence $r^k A \subseteq B_i$ for some $k > 0$. This means that $r \in P_i$, but it's not the case. So $B \subseteq B_i$. ∎

Theorem (Nakayama lemma): Let $J \subseteq R$ be an ideal. Then the following are equal:

1. J is contained in every maximal ideal.
2. $1 - j \in R^\times$ for every $j \in J$.
3. If A is a finitely generated R-module such that $JA = A$, then $A = 0$.
4. If A is a finitely generated R-module, and $B \subseteq A$ a submodule with $A = JA + B$, then $B = A$.

Proof: (1 $\Rightarrow$ 2) If $1 - j \notin R^\times$ for some $j \in J$, then $\langle 1 - j \rangle \neq R$, and hence is contained in a maximal ideal M. But $J \subseteq M$; therefore $j \in M$ and $1 \in M$. So $1 - j \in R^\times$ for all $j \in J$.

(2 $\Rightarrow$ 3) Let A be a non-zero and generated by $\{a_1, \dots, a_n\}$, and suppose that no subset of $\{a_1, \dots, a_n\}$ generates A. In particular, $a_1 \neq 0$. Write $a_1 = j_1 a_1 + j_2 a_2 + \dots + j_n a_n$ with $j_i \in J$. Then $(1 - j_1) a_1 = j_2 a_2 + \dots + j_n a_n$, and $1 - j_1 \in R^\times$ by (2). Then $a_1 \in \langle a_2, a_3, \dots, a_n \rangle$, which is against minimality. Thus $A = 0$.

(3 $\Rightarrow$ 4) Consider the R-module A/B; it's easy to see that $J \cdot A/B = A/B$, when $A = JA + B$. Therefore $A/B = 0$, and $B = A$.

(4 $\Rightarrow$ 1) Let $M \subseteq R$ be a maximal ideal. Then $M \subseteq JR + M \neq R$. Thus $M = JR + M$, and hence $J \subseteq M$. ∎

Corollary: Let $J \subseteq R$ be an ideal. Then J is contained in every maximal ideal if and only if $\bigcap_{n>0} J^n A = 0$ for every Noetherian R-module A.

Proof: ($\Rightarrow$) Let $B = \bigcap_{n>0} J^n A$. Then $JB = B$ by the Krull Intersection Theorem. Since A is Noetherian, B is finitely generated, and by part (3) of Nakayama's Lemma, we get $B = 0$.

($\Leftarrow$) Let $M \subseteq R$ be a maximal ideal. Then, being a field, $A = R/M$ is a Noetherian

R-module. Then $\bigcap_{n>0} J^n A = 0$ by assumption. Also $JA \subseteq A$ is a submodule; therefore either $JA = A$ or $JA = 0$. If $JA = A$, then $J^n A = A$ for all $n > 0$ and $\bigcap_{n>0} J^n A = A \neq 0$. So we need to have $JA = 0$. This means that $J \subseteq M$, and hence $J \subseteq M$. ∎

Definition: A (commutative) ring R is called local if it has a unique maximal ideal.

An example is $R = \mathbb{C}[[x]]$, the ring of formal series (with complex coefficients). Note, in general, that a ring is local if and only if $R \setminus R^\times$ is an ideal (and that is indeed the maximal ideal). So the maximal ideal m of R is $\langle x \rangle$.

Corollary: Let R be a Noetherian local ring, and $M \subseteq R$ its maximal ideal. Then $\bigcap_{n>0} M^n = 0$.

Proof: Take $J = M$, and $A = R$ in the previous corollary. ∎

Back to the example above: $M = \langle x \rangle$ can be thought as "all functions around the origin that are 0 at 0". Then $m^n = \langle x^n \rangle$ is the ideal of all functions that are 0 at 0 at least with multiplicity n. Clearly, no function in R is 0 at 0 infinitely many times, and this is what the last corollary tells us.

Theorem (Hilbert Basis Theorem): Let R be a Noetherian ring. Then $R[x]$ is also Noetherian.

Proof: Let $J \subseteq R[x]$ be an ideal. We'll show that J is finitely generated. For $n \geq 0$, let $I_n := \{ a \in R : \text{there is } f \in J \text{ of degree } n \text{ whose lead. coef. is } a \} \cup \{0\}$. Then $I_0 \subseteq I_1 \subseteq \dots$ is an ascending chain of ideals of R. Therefore there is $k \geq 0$ such that $I_\ell = I_k$ for all $\ell \geq k$.

Also each I_n is finitely generated; say $I_n = \langle r_{n1}, \dots, r_{ni_n} \rangle$ for $0 \le n \le k$. Take $f_{nj} \in J$ whose leading coefficient is r_{nj}, and $\deg(f_{nj}) = n$. We claim that $\langle f_{nj} : n = 0, \dots, k, j = 1, \dots, i_n \rangle = J$. All we need to show is that each element of J is in $J^* := \langle f_{nj} : n, j \rangle$. We do this by induction on the degree of an element from J.

Suppose that $f \in J$ has degree 0, then $f \in I_0$, and hence $f \in J^*$. Now assume that each element of J of degree less than $m > 0$ is in J^*, and let $f \in J$ be of degree m, and let α be the leading coefficient of f. Then $\alpha \in I_m$. If $m \le k$, then $\alpha = s_1 r_{m1} + \cdots + s_{i_m} r_{mi_m}$ with $s_j \in R$. Therefore $\sum_{j=1}^{i_m} s_j f_{mj} \in J^*$. Now degree of $f - \sum_{j=1}^{i_m} s_j f_{mj}$ is at most $m-1$, hence it is in J^* and $f \in J^*$.

If $m > k$, then again $\alpha = s_1 r_{k1} + \cdots + s_{i_k} r_{ki_k}$ with $s_j \in R$, and $\sum_{j=1}^{i_k} s_j f_{kj} \in J^*$. This time $f - \sum s_j x^{m-k} f_{kj}$ has degree at most $m-1$ and we get that it is in J^*. So $f \in J^*$. ∎

Corollary: If R is Noetherian, then the polynomial ring $R[X_1, \dots, X_n]$ in n variables is also Noetherian.

Exercise: Show that if R is Noetherian, then so is $R[[X]]$.

Ring Extensions

As in the case of fields, when $S \subseteq R$ are rings, we say that R is an extension of S and denote it as R/S.

Definition: Let R/S be a ring extension, and let $\alpha \in R$. We say that α is integral over S if there is a monic $f \in S[X]$ with $f(\alpha) = 0$.

The extension R/S is integral if each element of R is integral over S.

As in the case of field, for R|S and $A \subseteq R$, we let $S[A]$ denote the subring of R generated by A over S. So

$$S[A] = \{ f(a_1, \cdots, a_n) : f(x_1, \cdots, x_m) \in S[x_1, \cdots, x_m], a_1, \cdots, a_n \in A \}.$$

Theorem: Let R|S be a ring extension, and let $\alpha \in R$. Then the following are equivalent:

(1) α is integral over S.

(2) $S[\alpha]$ is a finitely generated S-module.

(3) There is a subring T of R, containing $S[\alpha]$ that is finite generated as an S-module.

(4) There is an $S[\alpha]$-submodule B of R that is finitely generated as an S-module and $\mathrm{Ann}_{S[\alpha]}(B) = 0$.

Proof: (1 $\Rightarrow$ 2) let α be the zero of a monic $f \in S[x]$ of degree n. Then $S[\alpha]$ is generated by $1, \alpha, \cdots, \alpha^{n-1}$ as an S-module.

(2 $\Rightarrow$ 3) Clear.

(3 $\Rightarrow$ 4) let $B = T$. Then T is finitely generated as an S-module, so it is finitely generated as an $S[\alpha]$-module. let $u \in \mathrm{Ann}_{S[\alpha]}(T)$. Since T is a subring, we have $1 \in T$. So $u = u \cdot 1 = 0$, and hence $\mathrm{Ann}_{S[\alpha]}(T) = 0$.

(4 $\Rightarrow$ 1) let $B = \langle r_1, \cdots, r_n \rangle = Sr_1 + \cdots + Sr_n$. Note that $\alpha \cdot r_i \in B$ for all i. Say $\alpha \cdot r_i = \sum_{j=1}^{n} s_{ij} r_j$ $(s_{ij} \in S)$. let $M = (s_{ij})_{i,j \in \{1, \cdots, n\}}$ be a matrix with S-entries.

Then if $\det(M - \alpha I_n) = d$, then we have $d r_j = 0$ for all j. Therefore $dB = 0$ and $d \in \mathrm{Ann}_{S[\alpha]} B = 0$. So α is a zero of the polynomial $\det(M - XI_n)$. It is clear that the leading coefficient of this polynomial is either 1 or -1. So α is integral over S. ∎

Corollary: Let $R|S$ be a ring extension.

(1) If R is a finitely generated S-module, then the extension is integral.

(2) Let $\alpha_1, \dots, \alpha_n \in R$ be integral over S. Then $S[\alpha_1, \dots, \alpha_n] | S$ is integral.

(3) Let $T|R$ be another extension. If both $T|R$ and $R|S$ are integral, then so is $T|S$.

(4) $\hat{S} := \{\alpha \in R : \alpha$ is integral over $S\}$ is a subring of R, containing S.

The subring $\hat{S}$ of R in (4) is called the integral closure of S in R. If $\hat{S} = S$, then we say that S is integrally closed in R. For a domain S, we say that S is integrally closed if it is integrally closed in its field of fractions.

Proposition: Let R be an integral domain with a multiplicative subset T, not containing 0. If R is integrally closed, then so is its localization $T^{-1}R$ at T.

Proof: Note that the field of fractions of $T^{-1}R$ is the same as the field of fractions of R; let K be that field.

Suppose that $u \in K$ is integral over $T^{-1}R$; say:

$$u^n + \frac{r_{n-1}}{s_{n-1}} u^{n-1} + \cdots + \frac{r_1}{s_1} u + \frac{r_0}{s_0} = 0 \qquad r_i \in R, s_i \in T.$$

Let $s = s_0 s_1 \cdots s_{n-1} \in T$. Then su is integral over R:

$$(su)^n + \frac{r_{n-1} s \cdots}{s_{n-1}} (su)^{n-1} + \cdots + \frac{r_1 s^{n-1}}{s_1} su + \frac{r_0 s^n}{s_0} = 0.$$

Therefore $su \in R$, and $u \in T^{-1}R$. ∎

Primes in Extensions

Let $S|R$ be a ring extension, and let $I \subseteq S$ be an ideal. Then $J := I \cap R$ is an ideal of R. In this case we say I lies over J; sometimes we say J is a contraction of I.

It is clear that prime ideal lie over prime ideals: If $P \subseteq S$ is prime, then $P \cap R$ is prime in R. Is there always a prime of S over a prime of R?

Not necessarily, but it is the case if the extension is integral.

Theorem: Let S/R be an integral extension of rings, and let $P \subseteq R$ be a prime ideal. Then there is a prime ideal of S lying over P.

Proof: Let $T := R - P$, a multiplicative subset of R and S. We have seen before that an ideal Q of S with $Q \cap T = \emptyset$ and maximal with respect to this property is a prime ideal of S. Such an ideal has the property that $Q \cap R \subseteq P$. Suppose that $P \not\subseteq Q \cap R$, and take $p \in P - Q$. Then $Q + Sp \supsetneq Q$. Then $(Q+Sp) \cap T \neq \emptyset$, say $c \in (Q+Sp) \cap T$, $c = q + sp$ with $q \in Q$, $s \in S$. Take $r_0, r_1, \dots, r_{n-1} \in R$ with

$$s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 = 0.$$

Then $(sp)^n + r_{n-1}p(sp)^{n-1} + \cdots + r_1 p^{n-1}(sp) + r_0 p^n = 0$. So we have $(c-q)^n + r_{n-1}p(c-q)^{n-1} + \cdots + r_1 p^{n-1}(c-q) + r_0 p^n = 0$. Therefore we have $c^n + r_{n-1}pc^{n-1} + \cdots + r_1 p^{n-1} c + r_0 p^n \in Q \cap R \subseteq P$. Then $c^n \in P$ & hence $c \in P$. But $c \in T = R - P$. This is a contradiction. So we have $P = Q \cap R$. ∎

Corollary (Going-Up): Let S/R be an integral extension of rings, $P \subseteq P'$ primes of R, and Q a prime of S lying over P. Then there is a prime Q' of S lying over P' with $Q \subseteq Q'$.

(This is not a corollary of the theorem, but rather a corollary of its proof. So we leave it as an exercise.)

Theorem: Let S/R be an integral extension of rings, $P \subseteq R$ a prime, and $Q \subseteq Q'$ primes of S lying over P. Then $Q = Q'$.

Proof: We'll prove the following: If $Q \subseteq S$ is a prime lying over P, then Q is maximal in $\{I \subseteq S : I \text{ is an ideal of } S,\ I \cap (R-P) = \emptyset\}$.

Suppose not: Let $Q \subseteq S$ be an ideal over P, and let $I \supsetneq Q$ be an ideal of S with $I \cap (R-P) = \emptyset$. Then $I \cap R \subseteq P$.

Take $u \in I \setminus Q$. As a is integral over R, the set of monic polynomials $f \in R[x]$ with $f(u) \in Q$ is non-empty. Let f be such a polynomial with minimal degree among such polynomials.

Say $f(u) = u^n + r_{n-1}u^{n-1} + \cdots + r_1 u + r_0 \in Q$, with $r_0, r_1, \ldots, r_{n-1} \in R$.

Then $r_0 \in I \cap R \subseteq P = Q \cap R \subseteq Q$. Therefore $u(u^{n-1} + r_{n-1}u^{n-2} + \cdots + r_2 u + r_1) \in Q$ and hence $u^{n-1} + r_{n-1}u^{n-2} + \cdots + r_2 u + r_1 \notin Q$. So $u \in Q$. A contradiction! So Q is indeed maximal among ideals of S not intersecting $R \setminus P$. ∎

Corollary: Let S/R be an integral ring extension, $Q \subseteq S$ a prime ideal, and $P = Q \cap R$. Then Q is a maximal ideal of S if and only if P is a maximal ideal of R.

Proof: ($\Rightarrow$) Suppose that Q is maximal. Let $M \supseteq P$ be a maximal ideal of R, and take a prime ideal $Q' \supseteq Q$ of S over M. But then $Q' = Q$ by maximality of Q. Thus $P = Q \cap R = Q' \cap R = M$, and hence P is maximal.

($\Leftarrow$) Suppose that P is maximal. Take $N \supseteq Q$ a maximal ideal of S. Then $P = R \cap Q \subseteq R \cap N \subsetneq R$. So $P = R \cap N$ by maximality. Then $N = Q$ by the previous theorem, and Q is maximal. ∎

20th Lecture

Dedekind Domains

From here on R is an integral domain with K its field of fractions.

Definition: A fractional ideal of R is a nonzero R-submodule I of K such that $aI \subseteq R$ for some $a \in R \setminus \{0\}$.

Let's record some basic and easy facts about fractional ideals:

- Every ideal of R is a fractional ideal; just take $a = 1$.
- If $I \subseteq R$ is a fractional ideal, then it is actually an ideal.
- If I is a fractional ideal, then aI is an ideal of R.
- If I is a finitely generated R-submodule of K, then I is a fractional ideal.

Example: $\frac{1}{2}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$, but obviously not an ideal.

The collection of all fractional ideals of R becomes an abelian monoid with the following product (generalizing the ideal product):

$$I \cdot J := \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J \right\}.$$

R is the identity of this monoid.
A fractional ideal I is called invertible if it is invertible in this monoid. This means that $IJ = R$ for some J, fractional ideal. Note that if we define $I^{-1} = \{a \in K : aI \subseteq R\}$, then $I^{-1}I \subseteq R$. We have the equality if and only if I is invertible. (Note that I^{-1} is also a fractional ideal.)
Note that any principal ideal is invertible.

Lemma: Let $I_1, \dots, I_n \subseteq R$ be ideals. Then $I_1, \dots, I_n$ are all invertible if and only if $I_1 \cdots I_n$ is invertible.

Proof: ($\Rightarrow$) Clear.

($\Leftarrow$) Let $J = (I_1 \cdots I_n)^{-1}$. Then $I_i (I_1 \cdots I_{i-1} I_{i+1} \cdots I_n) J = R \cdot S_0$

$I^{-1} = I_1 \cdots I_{i-1} I_{i+1} \cdots I_n J$. ∎

Lemma: Let $P_1, \dots, P_k, Q_1, \dots, Q_\ell \subseteq R$ be prime ideals such that each P_i is invertible, and $P_1 \cdots P_k = Q_1 \cdots Q_\ell$. Then $k = \ell$, and $P_i = Q_i$ (after reordering).

Proof: We proceed by induction on k.

$k = 1$: $P_1 = Q_1 \cdots Q_\ell$. Since P_1 is a prime, we have $Q_i \subseteq P_1$ for some i. But also $P_1 = Q_1 \cdots Q_\ell \subseteq Q_i$. So $Q_i = P_1$ for some i; we may take $i = 1$.
If $\ell > 1$, then we have $Q_2 Q_3 \cdots Q_\ell = R$ after multiplying by $Q_1^{-1} = P_1^{-1}$.
But this is not possible as Q_i are proper ideals.
So $\ell = 1$ and $P_1 = Q_1$.

$k>1$: Let P_1 be such that $P_i \not\subseteq P_1$ for all $i>2$.
Assuming $Q_1 \cdots Q_\ell = P_i \cdots P_k \subseteq P_1$, we have $Q_i \subseteq P_1$ for some i. Also $P_j \subseteq Q_i$, for some j. Then $Q_i = P_1$ by the choice of P_1. We may also assume $i=1$. We get $P_2 \cdots P_k = Q_2 \cdots Q_\ell$ after multiplying by $Q_1^{-1} = P_1^{-1}$. Then we're done by the induction hypothesis. ∎

Definition: If every proper ideal of R is a product of finite number of prime ideals, then R is called a Dedekind domain.

Theorem: Let R be a Dedekind domain. Then every nonzero prime ideal is invertible and is a maximal ideal of R.

Proof: We first show that every invertible prime ideal P is maximal. Let $a \in R \setminus P$. We'd like to show that $P + Ra = R$. Suppose not. Then $P + Ra = P_1 \cdots P_k$ for some prime ideals P_i. We also have $P + Ra^2 \neq R$; hence let $P + Ra^2 = Q_1 \cdots Q_\ell$ for some prime ideals Q_j.
Let $\pi : R \to R/P$ be the canonical projection. Consider the ideals of R/P generated by $\pi(a)$ and $\pi(a^2)$. It's easy to see that $\langle \pi(a) \rangle = \pi(P_1) \cdots \pi(P_k)$, and $\langle \pi(a^2) \rangle = \pi(Q_1) \cdots \pi(Q_\ell)$.
Since each $P_i \supseteq \ker \pi = P$, we have that $\pi(P_i)$ is prime in R/P. (and Similarly, each $\pi(Q_i)$ is a prime of R/P. Being principal ideals $\langle \pi(a) \rangle$ and $\langle \pi(a^2) \rangle$ are invertible. Therefore each $\pi(P_i)$ and $\pi(Q_j)$ is invertible by the previous lemma. Therefore $\pi(Q_1) \cdots \pi(Q_\ell) = \langle \pi(a^2) \rangle = \langle \pi(a) \rangle^2 = \pi(P_1)^2 \cdots \pi(P_k)^2$. So $\ell = 2k$, and (wlog) $\pi(P_i) = \pi(Q_{2i}) = \pi(Q_{2i-1})$. Then $P_i = \pi^{-1}(\pi(P_i)) = \pi^{-1}(\pi(Q_{2i})) = Q_{2i}$ and similarly $P_i = Q_{2i-1}$.
Therefore $P + Ra^2 = (P + Ra)^2$, and $P \subseteq P + Ra^2 \subseteq (P + Ra)^2 \subseteq P^2 + Ra$. Let $b \in P$, and choose $c \in P^2$, $r \in R$ with $b = c + ra$. Then $ra \in P$ and hence $r \in P$ since $a \notin P$. So $P \subseteq P^2 + Pa \subseteq P$, and $P = P^2 + Pa = P(P + Ra)$. Since P is invertible, we have $R = P^{-1}P = P^{-1}P(P + Ra) = P + Ra$, which is a contradiction. So P is maximal.

Now let $P \subseteq R$ be a prime & let $c \in P \setminus \{0\}$. Then $\langle c \rangle = P_1 \cdots P_k$. Then $P_i \subseteq P$ for some i. Since $\langle c \rangle$ is invertible, each P_i is invertible. So P_i is maximal, But $P_i \subseteq P$, hence $P = P_i$ is maximal. ∎

Lemma: Let I be a fractional ideal of R, and let $f: I \to R$ be an R-module homomorphism. Then $a f(b) = b f(a)$ for all $a, b \in I$.

Proof: Let $a = \frac{r_1}{r_2}$, $b = \frac{s_1}{s_2}$ with $r_1, r_2, s_1, s_2 \in R$, $r_2 s_2 \neq 0$.

Then $r_2 ab = r_1 b \in I$ and $s_2 ba = s_1 a \in I$. Therefore

$$r_2 f(s_2 ba) = f(r_2 s_2 ba) = s_2 f(r_2 ab) = s_2 f(r_1 b) \in R$$

Now $a f(b) = \dfrac{r_2 a f(b)}{r_2} = \dfrac{f(r_2 ab)}{r_2} = \dfrac{f(s_2 ba)}{s_2} = \dfrac{s_2 b f(a)}{s_2} = b f(a)$. ∎

Lemma: Let I be an invertible fractional ideal of R. Then I is finitely generated as an R-module.

Proof: Let I^{-1} be the inverse of I. Then $I^{-1} = \{a \in R : aI \subseteq R\}$.

Then $1 \in R = I^{-1} I$ can be written as $1 = a_1 b_1 + \cdots + a_n b_n$ with $a_i \in I^{-1}$ and $b_i \in I$. We claim that $I = \langle b_1, \ldots, b_n \rangle$.

Let $c \in I$. Then $c = c \cdot 1 = \sum_{i=1}^{n} c a_i b_i$. Since $c a_i \in R$ we get $c \in \langle b_1, \ldots, b_n \rangle$. ∎

Theorem: Let I be a fractional ideal of R. Then I is invertible if and only if it is projective as an R-module.

Proof: ($\Rightarrow$) Let $I = \langle b_1, \ldots, b_n \rangle$ & write $1 = \sum_{i=1}^{n} a_i b_i$ where $a_i \in I^{-1}$ for each i. Let F be the free R-module on $\{e_1, \ldots, e_n\}$, and let $\pi: F \to I$ be given by sending e_i to b_i. So we have the short exact sequence:

$$0 \to \ker \pi \to F \to I \to 0$$

Let $f: I \to F$ be given by $c = \sum c a_i b_i \mapsto \sum c a_i e_i$. Then it's easy to check that $\pi \circ f = id_I$. Hence the sequence splits & I is a direct summand in a free R-module.

So I is projective.

($\Leftarrow$) Let $\{b_j : j \in X\}$ be a generating set for I with $b_j \neq 0$.

Fix b_0 from this set.

Let F be the free R-module on $\{b_j : j \in X\}$ and let $\pi : F \to I$ be given by sending e_j to b_j.

So let $\psi : I \to F$ be such that $\pi \circ \psi = id_I$. Also let $\pi_j : F \to Re_j \overset{\sim}{\to} R$ be the projection onto the j^{th} component. Let $\theta_j = \pi_j \circ \psi$; so $\theta_j : I \to R$ is the R-module homomorphism. Put $c_j := \theta_j(b_0)$.

Now for $c \in I$ we have $c \cdot c_j = c\,\theta_j(b_0) = b_0 \cdot \theta_j(c)$. Therefore $c\frac{c_j}{b_0} = \theta_j(c) \in R$. Therefore $\frac{c_j}{b_0} \in I^{-1}$ since this holds for all $c \in I$.

Now $\psi(c) = \sum_{j \in X} \theta_j(c) e_j = \sum_{j \in X_0} c \frac{c_j}{b_0} e_j$, where $X_0 \subseteq X$ is finite.

So $c = (\pi \circ \psi)(c) = \pi\left(\sum_{j \in X_0} c \frac{c_j}{b_0} e_j\right) = \sum_{j \in X_0} c \frac{c_j}{b_0} b_j = c \sum_{j \in X_0} \frac{c_j}{b_0} b_j$.

Since $\frac{c_j}{b_0} \in I^{-1}$ for all j and $b_j \in I$ for all j, we have $1 \in I^{-1} I$. Hence $I^{-1} I = R$ and I is invertible. ∎

Definition: A discrete valuation ring (DVR) is a PID that has exactly one nonzero prime ideal.

Lemma: Let R be a Noetherian integrally closed domain that has a unique nonzero prime ideal. Then R is a DVR.

Proof: All we need to show is that R is a PID. We do this in four steps.

① For every fractional ideal I of R we have $\bar{I} := \{a \in K : aI \subseteq I\}$ is R.

Proof: It's clear that $R \subseteq \bar{I}$. It's easy to see that $\bar{I}$ is a fractional ideal. Therefore $\bar{I}$ is isomorphic as an R-module to an ideal of R (WHY?) Then

$\bar{I}$ is a finitely generated R-module, so every element of $\bar{I}$ is integral over R. Hence $\bar{I} \subseteq R$ since R is integrally closed. ☐①

② For the any prime ideal P of R we have $R \subsetneq P^{-1}$.

Proof: We just have to show $R \neq P^{-1}$.

For nonzero $a \in P$ we have $\frac{1}{a} \in \langle a \rangle^{-1} \setminus P$. So the collection $\mathcal{F} = \{ J \subseteq R \text{ ideal} \mid R \subsetneq J^{-1} \}$ is non-empty. Using Zorn's lemma, there is a maximal element M of $\mathcal{F}$. We claim that M is a prime ideal. Let $ab \in M$ and $a \notin M$. Also take $c \in M^{-1} \setminus R$. Then $cab \in R$. Now $bc(aR+M) \subseteq R$ and $bc \in (aR+M)^{-1}$. Hence $bc \in R$, and $c(bR+M) \subseteq R$. So $c \in (bR+M)^{-1}$ and hence $bR+M = M$ since $c \notin R$. So $b \in M$, and M is prime. Then $M = P$ and $R \subsetneq M^{-1} = P^{-1}$. ☐②

③ P is invertible.

Proof: Clearly, $P \subseteq P \cdot P^{-1} \subseteq R$. Then either $PP^{-1} = R$ or $PP^{-1} = P$.

If $PP^{-1} = P$, then $P^{-1} \subseteq \bar{P} = R$. So $R \subsetneq P^{-1} \subseteq R$, a contradiction.

So $PP^{-1} = R$ and P is invertible. ☐③

④ $\bigcap_{n>0} P^n = 0$.

Proof: This intersection is a fractional ideal if it is nonzero. But then $R \subsetneq P^{-1} \subseteq \overline{\bigcap_{n>0} P^n} = R$. So $\bigcap_{n>0} P^n = 0$. ☐④

⑤ P is principal.

Proof: We have $P^2 \neq P$ by ④. So let $a \in P \setminus P^2$. Then aP^{-1} is an ideal of R, and $aP^{-1} \not\subseteq P$. Therefore $aP^{-1} = R$. This means that $aR = aPP^{-1} = (aP^{-1})P = RP = P$. ☐⑤

End of the pf: Let $I \subseteq R$ be an ideal. Then $I \subseteq P$. Let $n > 0$ be maximal such that $I \subseteq P^n$. Hence $I \not\subseteq P^{n+1}$. Let $b \in I \setminus P^{n+1}$. Then $P^n = \langle a^n \rangle$ and $b = ua^n$ for some $u \notin P = \langle a \rangle$. So $u \in R^\times$. Then $P^n = \langle a^n \rangle = \langle ua^n \rangle = \langle b \rangle \subseteq I$. So $I = \langle b \rangle$. ■

Theorem: Let R be an integral domain. Then the following are equivalent:

1. R is a Dedekind domain.
2. Every proper ideal can be written uniquely as a product of prime ideals.
3. Every nonzero ideal of R is invertible.
4. Every fractional ideal of R is invertible.
5. The set of fractional ideals of R form a group.
6. Every ideal of R is projective.
7. Every fractional ideal of R is projective.
8. R is Noetherian, integrally closed, and each nonzero prime ideal of R is maximal.
9. R is Noetherian, and for every nonzero prime ideal P of R, the localization of R at P is a DVR.

Proof: The following equivalences follow easily from earlier results:

$1 \leftrightarrow 2$, $2 \to 3$, $4 \leftrightarrow 5$, $3 \leftrightarrow 6$, $4 \leftrightarrow 7$, $6 \leftrightarrow 7$.

$4 \to 8$: R Noetherian: Let $I \subseteq R$ be an ideal. Since I is invertible, it is finitely generated.

R integrally closed: Let $u \in K$ be integral over R. Then $R[u]$ is a finitely generated R-module. Therefore it is a fractional ideal, hence it is invertible. Then $R = R[u]^{-1}R[u] = R[u]^{-1}R[u]R[u] = R \cdot R[u] = R[u]$, and $u \in R$.

Every nonzero prime is maximal: Let $P \subseteq R$ be nonzero and $M \supseteq P$ maximal. Then M is invertible, and $M^{-1} \not\subseteq R$. Also $M^{-1}P$ is a fractional ideal, but $M^{-1}P \subseteq M^{-1}M = R$. So $M^{-1}P$ is a usual ideal of R.

Now $P = RP = (MM^{-1})P = M(M^{-1}P)$. So either $P \supseteq M$ or $P \supseteq M^{-1}P$.

If $P \supseteq M^{-1}P$, then $R \subsetneq M^{-1} = M^{-1}R = M^{-1}PP^{-1} \subseteq P \cdot P^{-1} = R$. So we need to have $P \supseteq M$, and hence $P = M$ is maximal.

$8 \to 9$: Since R is integrally closed, the localization R_P of R at P is also integrally closed. The ideals of R_P are of the form $I_P = \{\frac{i}{s} : i \in I, s \notin P\}$ where $I \subseteq R$ is an ideal. Since each such I is finitely generated, I_P is also finitely generated. So R_P is Noetherian. It remains to show that R_P has a unique prime ideal. If I_P is prime, then $P \subseteq I$ and I is also prime.

Hence I is a maximal ideal, but so is P. Hence $I = P$, and P_p is the unique nonzero prime ideal of R_p. By an earlier result R_p is a DVR.

(9) → (1): Check Hungerford... ∎

Hilbert's Nullstellensatz

Definition: An R-algebra is a ring A equipped with a ring homomorphism

$\varphi: R \to A$.

An R-algebra A has an R-module structure: $r \cdot a = \varphi(r)\, a$.
We'll mostly be interested in the case $R = k$ is a field. Then either $\varphi \equiv 0$ or φ is injective. If $\varphi \equiv 0$ then A is just a ring. If φ is injective then we may assume $k \subseteq A$.
A k-algebra is not necessarily an integral domain: $\mathbb{R}[x]/x^2$ as an $\mathbb{R}$-alg.
Below k denotes an infinite field.

Theorem (Noether Normalization): Let A be a finitely generated k-algebra. Then there are $y_1, \dots, y_r \in A$ such that $\{y_1, \dots, y_r\}$ is algebraically dependent over k, and $A \,|\, k[y_1, \dots, y_r]$ is integral.

Proof: Let $A = k[x_1, \dots, x_n]$. We proceed by induction on n.
If $n = 0$, then there is nothing to prove.
Let (after re-ordering) $x_1, \dots, x_r$ be algebraically independent over k, and each x_i ~~$k[x_1, \dots, x_r]$~~ is algebraic over $k[x_1, \dots, x_r]$; with r maximal possible.
If $r = n$, then we are done by taking $y_i = x_i$ for $i = 1, \dots, n$.
Suppose that $r < n$, and let $f(T_1, \dots, T_n) \in k[T_1, \dots, T_n] - \{0\}$ with $f(x_1, \dots, x_n) = 0$.
Claim: There are $a_1, \dots, a_{n-1} \in k$, and $\lambda \in k$ such that the polynomial

$\lambda f(T_1 + a_1 T_n, \dots, T_{n-1} + a_{n-1} T_n, T_n)$ is monic in T_n.

Write $f(T_1, \dots, T_n) = \sum_{\vec{m} \in M} a_{\vec{m}} \vec{T}^{\vec{m}}$,

where M is a finite set of multi-indices, and $\vec{T}^{\vec{m}} = T_1^{m_1} \cdots T_n^{m_n}$.

Suppose that the (total) degree of f is d, and let f_d be the homogeneous part of f of degree d. Note that:

$$f(T_1+a_1T_n, \dots, T_{n-1}+a_{n-1}T_n, T_n) = \sum_{\vec{m}\in M} a_{\vec{m}} (T_1+a_1T_n)^{m_1}\cdots(T_{n-1}+a_{n-1}T_n)^{m_{n-1}} T_n^{m_n}$$

$$\vdots$$

So considered as a polynomial of T_n, the leading term is

$$\sum_{m_1+\cdots+m_{n-1}+m_n=d} a_{\vec{m}}\, a_1^{m_1}\cdots a_{n-1}^{m_{n-1}}\, T_n^d = f_d(a_1,\dots,a_{n-1},1)\,T^d.$$

Since k is infinite, there are $a_1,\dots,a_{n-1}\in k$ such that $f_d(a_1,\dots,a_{n-1},1)\neq 0$.

Then we are done by taking $\lambda = \dfrac{1}{f_d(a_1,\dots,a_{n-1},1)}$. $\square_{\text{claim}}$

Now let $y_i := x_i - a_i x_n$ for $i = 1,\dots,n-1$, and $y_n = x_n$. Then

$\lambda f(y_1+a_1y_n, \dots, y_{n-1}+a_{n-1}y_n, y_n) = 0$, and $\lambda f(y_1+a_1T, \dots, y_{n-1}+a_{n-1}T, T)$ is a monic element of $k[y_1,\dots,y_{n-1}][T]$. Therefore y_n is integral over $k[y_1,\dots,y_{n-1}]$. By induction hypothesis, there are $z_1,\dots,z_r\in k[y_1,\dots,y_{n-1}]$ such that $k[y_1,\dots,y_{n-1}] \mid k[z_1,\dots,z_r]$ is integral and $\{z_1,\dots,z_r\}$ is algebraically independent over k. So $A \mid k[z_1,\dots,z_r]$ is integral. $\blacksquare$

We present five versions of Hilbert's Nullstellensatz with various strengths

Theorem (HNS - V1) Let A be a finitely generated k-algebra. Suppose A is also a field. Then A/k is a finite field extension.

Proof: By Noether normalization, there are $y_1,\dots,y_r\in A$ that are algebraically independent over k, and $A \mid k[y_1,\dots,y_r]$ is integral. If $y_r\neq 0$, then there is a maximal ideal $m'\subseteq k[y_1,\dots,y_r]$, and hence using earlier results there is a maximal ideal $m\subseteq A$. Since A is a field, this is not possible. So $r=0$ and A/k is finite.

Theorem (HNS-V2): let A be a finitely generated k-algebra, and $\varphi: k \to L$ be a field embedding where L is algebraically closed. Then there is an extension of φ to A.

Proof: Exercise.

Theorem (HNS-V3): let k be algebraically closed. Then every maximal ideal of $k[X_1, \dots, X_n]$ in of the form $\langle X_1 - a_1, \dots, X_n - a_n \rangle$ for some $(a_1, \dots, a_n) \in k^n$.

Proof: let $\mathfrak{M} \subsetneq k[X_1, \dots, X_n]$ be maximal. Then $A = k[X_1, \dots, X_n]/\mathfrak{M}$ is a finitely generated k algebra which is also a field. Then $A = k$ by HNS-V1. So $\bar{x}_1, \dots, \bar{x}_n \in A$ are $\bar{a}_1, \dots, \bar{a}_n$ for some $a_1, \dots, a_n \in k$. This means that $x_i - a_i \in \mathfrak{M}$ for each i. But it is clear that $\langle X_1 - a_1, \dots, X_n - a_n \rangle$ is a maximal ideal. So $\mathfrak{M} = \langle X_1 - a_1, \dots, X_n - a_n \rangle$. ∎

The proof of the remaining three versions are left as exercise:

Theorem (HNS-V4): let $I \subsetneq k[X_1, \dots, X_n]$ where k is algebraically closed. Then there is $\vec{a} = (a_1, \dots, a_n) \in k^n$ such that $f(\vec{a}) = 0$ for all $f \in I$.

Theorem (HNS-V5): let A be a finitely generated k-algebra, and let $I \subseteq A$ be an ideal. Then $\operatorname{Rad} I = \bigcap_{\substack{\mathfrak{m} \supseteq I \\ \text{max. ideal}}} \mathfrak{m}$.

Theorem (HNS-V6): let $X \subseteq k^n$ be an affine variety, where k is algebraically closed. Then for any ideal $J \subseteq k(X)$ we have $I(V(J)) = \operatorname{Rad}(J)$.