Introductory Galois Theory Cheat Sheet

Definition of a Field

A field F is a set with two binary operators $(+, \times)$ satisfying the following axioms,

- (F,+) is an abelian group with identity 0.
- The non zero elements of F form an abelian group under multiplication with identity $1 \neq 0$.
- Left and right distributivity

Characteristic of Fields

A characteristic of a field F, denoted by $\mathrm{ch}(F)$ is defined as is the smallest integer p such that $\underbrace{1+1+\cdots+1}_{p \text{ times}} = 0$. If such a p does not, exist $\mathrm{ch}(F) = 0$.

K-algebra

A K-algebra (or algebra over a field) is a ring A which is a module over field K with multiplication being K-bilinear, (i.e., $k_1 a_1 \cdot k_2 a_2 = k_1 k_2 a_1 a_2$).

Field Extensions

For fields K, L. We say L is a field extension of K if K is a subfield of L. Alternatively, L is a field extension of K, if L is a K-algebra.

Algebraic elements and Algebraic extensions

For a field extension $K \subset L$.

Algebraic element: $\alpha \in L$ is called algebraic if $\exists P \in K[x]$ s.t. $P(\alpha) = 0$.

Transcendental element: If such a P does not exist then α is transcendental.

Consider the following definitions,

- Denote the smallest subfield of L containing K and α to be $K(\alpha)$.
- Denote the smallest sub ring of L containing K and α to be $K[\alpha]$.

The following statements are equivalent,

- α is algebraic over K.
- $K[\alpha]$ is finite dimensional algebra over K.
- $K[\alpha] = K(\alpha)$.

Algebraic extension: L is called algebraic over K if all $\alpha \in L$ are algebraic over K.

- If L is algebraic over K then any K-subalgebra of L is a field.
- Consider $K \subset L \subset M$. If $\alpha \in M$ is algebraic over K, then it is algebraic over L, also its minimal polynomial over L divides its minimal polynomial over K.
- If $K \subset L \subset M$ then M is an algebraic extension over $K \iff M$ is algebraic over L and L is algebraic over K.

Algebraic closure: A subfield L' of L s.t. $L' = \{\alpha \in L \mid \alpha \text{ is algebraic over } K\}$

Minimal Polynomial

If α is an algebraic element then $\exists!$ monic polynomial P of minimal degree such that $P(\alpha) = 0$ such a polynomial is called the **minimal polynomial**.

- The minimal polynomial is irreducible
- Any other polynomial Q s.t. $Q(\alpha) = 0$ will be divisible by P.

Pritmitive polynomials and Gauss' lemma

Primitive polynomial: A polynomial $P \in \mathbb{Z}[X]$ is called primitive if if has a positive degree and the gcd of its coefficients is 1.

Gauss' lemma: A polynomial $P \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Z}[X] \iff$ it is primitive and irreducible over $\mathbb{Q}[x]$

Eisenstein criterion for irreducibility

A polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ is irreducible if $\exists p$ prime s.t. p divides all coefficients except a_n and p^2 does not divide a_0.

Finite extensions

For a field extension $K \subset L$. L is called a **finite extension** of K if the vector space of L over K has a finite dimension.

Degree of finite extension: Denoted as $[L : K] = \dim_K L$

- $K \subset L \subset M$. Then M is finite over $K \iff M$ is finite over L and L is finite over K. Also in this case, $[M : K] = [M : L][L : K]$.
- Let $K(\alpha_1, \ldots, \alpha_n) \subset L$ denote the smallest subfield of L containing K and $\alpha_i \in L$. This $K(\alpha_1, \ldots, \alpha_n)$ is generated by $\alpha_1, \ldots, \alpha_n$.
- L is finite over $K \iff L$ is generated by a finite number of algebraic elements over K .
- $[K(\alpha) : K] = \deg P_{\min}(\alpha, K)$

Stem field

Let $P \in K[X]$ be an irreducible monic polynomial. A field extension E is called a stem field of P if $\exists \alpha \in E$, s.t. α is a root of P and $E = K[\alpha]$

- If E, E' are two stem fields for $P \in K[x]$, s.t. $E = K[\alpha], E' = K[\alpha']$ where α, α' are roots of P. Then $\exists!$ isomorphism $E \cong E'$ of K-algebras which maps α to α'.
- If a stem field contains two roots of P, then $\exists!$ automorphism that maps one root to another.
- If E is a stem field, $[E : K] = \deg P$
- If $[E : K] = \deg P$ and E contains a root of P then E is a stem field.

Some irreducibility criteria,

- $P \in K[X]$ is irreducible over $K \iff$ it does not have roots in L/K of degree $\leq \deg P/2$.
- $P \in K[X]$ is irreducible over K with $\deg P = n$. If L/K with $[L : K] = m$ if $\gcd(m, n) = 1$ then P is irreducible over L.

Splitting field

Let $P \in K[X]$. The splitting field of P over K is an extension of L where P is split into linear factors and the roots of P generate L (alternatively if P cannot be factored into any intermediate field).

- Splitting field L exists and its degree is $\leq d!$, where $d = \deg P$. And it is unique up to isomorphism.

Algebraic closure

- A field K is algebraically closed if any non-constant polynomial $P \in K[X]$ has a root in K.
- L is called an **algebraic closure** of K if it is algebraically closed and a field extension over K.
- Every field has an algebraic closure.
- Algebraic closures of K are unique up to isomorphism as $K-$algebras.

Properties of finite fields

Let p be a prime integer and let $q = p^r$ for some positive integer r. Then the following statements hold.

- There exists a field of order q.
- Any two fields of order q are isomorphic.
- Let K be a field of order q. The multiplicative group $K^\times$ of non-zero elements of K is a cyclic group of order $q - 1$.
- Let K be a field of order q. The elements of K are the roots of $x^q - x \in \mathbb{F}_p[x]$.
- A field of order p^r contains a field of order $p^k \iff k | r$
- The irreducible factors of $x^q - x$ over $\mathbb{F}_p$ are the irreducible polynomials in $\mathbb{F}_p[x]$ whose degree divides r.
- The splitting field of $x^q - x$ has q elements.
- $\mathbb{F}_q$ is a stem field and a splitting field of any irreducible polynomial $P \in \mathbb{F}_p$ of degree n.

Frobenius homomorphism

Let K be a field, $\mathrm{ch}(K) = p > 0$. There exists a homomorphism $\varphi : K \to K$, s.t. $\varphi(x) = x^p$. This is Frobenius homomorphism.

- The group of automorphisms over $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$ is cyclic and is generated by the Frobenius map.

Separability

- **Separable polynomial:** A irreducible polynomial $P \in K[X]$ is called separable if $\gcd(P, P') = 1$.
- **Degree of separability:** $\deg_{\text{sep}} P = \deg Q$ for some $P(X) = Q(X^p)$
- **Degree of inseparability:** $\deg_i P = \frac{\deg P}{\deg Q}$
- **Purely inseparable polynomial:** P is purely inseparable if $\deg_i P = \deg P$. Also if P is purely inseparable $P = X^{p^r} - a$
- **Separable element:** If L/K is an algebraic extension, then $\alpha \in L$ is called separable if its minimal polynomial over K is separable. And vice versa.
- If $\alpha \in K$ is separable then $|\mathrm{Hom}(K(\alpha), \overline{K}| = \deg P_{\min}(\alpha, K))$
- **Separable degree:** For L/K, we have $[L : K]_{\text{sep}} = |\mathrm{Hom}_K(K(\alpha), \overline{K})|$. Inseparable degree is degree of extension divided by separable degree.
- **Separable extension:** L is separable over K if $[L : K]_{\text{sep}} = [L : K]$.
  - If $\mathrm{ch}(K) = 0$ then any extension of K is separable.
  - If $\mathrm{ch}(K) = p$ then pure inseparable extension has degree p^r with degree of inseparability p^r
- Separable degrees obey the multiplicative property.
- TFAE
  - L is separable over K
  - Any element of L is separable over K
  - $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, where each α_i is separable over K.
  - $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, then α_i is separable over $K(\alpha_1, \ldots, \alpha_{i-1})$.
- **Separable closure:** $L^{\text{sep}} = \{x \mid x \text{ separable over } K\}$

Multilinear map

For a module M over ring A. A function L from $M^r = \underbrace{M \times M \times \cdots \times M}_{r \text{ times}}$ into A is called multilinear if $L(\alpha_1, \ldots, \alpha_r)$ is linear as a function of each α_i when the other α_j are fixed.

Tensor product

Consider a ring A and two $A-$modules, M, N. The tensor product is denoted as $M \otimes_A N$ is an $A-$module along with a $A-$bilinear map, $\varphi : M \times N \to M \otimes_A N$ which a "universal property".

Universal property of tensor product:
For a $A-$module P, if for an $A-$bilinear map, $f : M \times N \to P$, then $\exists!$ homomorphism $\tilde{f}$ of $A-$modules s.t. $f = \tilde{f} \circ \varphi$

$$\begin{tikzcd}
M \times N \arrow[r, "\varphi"] \arrow[dr, "f"'] & M \otimes_A N \arrow[d, dashed, "\tilde{f}"] \\
& P
\end{tikzcd}$$

- Commutativity of tensor product $M \otimes_A N \cong N \otimes_A M$
- $A \otimes_A M \cong M$
- The basis for the tensor product of free modules is the tensor product of their individual basis elements.
- The tensor product is associative.

Base change theorem: For a ring A, B an $A-$algebra, M an $A-$module and N a $B-$module. Then we have the following bijection

$$\text{Hom}_A(M, N) \leftrightarrow \text{Hom}_B(B \otimes_A M, N)$$

- For I an ideal of a ring A and M an $A-$module we have, $A/I \otimes_A M \cong M/IM$

Chinese remainder theorem

Comaximal ideals: Two ideals of a ring are called comaximal (or coprime) if their sum gives the ring itself.

- If I, J are comaximal then $IJ = I \bigcap J$
- If $I_1, \dots, I_k$ comaximal w.r.t J then $\prod_{i=1}^k I_i$ is also relatively prime with J.
- If I, J are comaximal then so are I^m, J^n for any m, n.

Chinese remainder theorem: For a ring A, consider two comaximal ideals I, J, then $\forall a, b \in R, \exists x \in A$ s.t. $x \equiv a(\text{mod } I)$ and $x \equiv b(\text{mod } J)$

Generalized Chinese remainder theorem: For a ring A, let $I_1, \dots, I_n$ be ideals of the ring A. Consider the map $\pi : A \to A/I_1 \times \cdots \times A/I_n$ defined as $\pi(a) = (a \mod I_1, \dots, a \mod I_n)$. Then $\ker \pi = I_1 \bigcap \cdots \bigcap I_n$, i.e. it is surjective iff $I_1, \cdots I_n$ are pairwise comaximal. If π is a surjection we have,

$$A/\bigcap I_k \cong A/\prod I_k \cong \prod(A/I_k)$$

Structure of finite algebras

Let A be a finite $K-$algebra then,

- There are only finitely many maximal ideals in A.
- For finitely many maximal ideals m_i. Let $J = m_1 \bigcap \cdots \bigcap m_r$. Then $J^n = 0$ for some n.
- $A \cong A/m_1^{n_1} \times \cdots \times A/m_r^{n_r}$ for some (not necessarily unique) $n_1, \dots, n_r$.

Reduced *K*-Algebra: If it has no nilpotent elements.

Local ring: If it has only one maximal ideal. A non zero ring in which every element is either a unit or nilpotent is local.

Further results on separability

Let L be a finite extension over K then the following hold,

- L is separable $\iff$ $L \otimes_K \overline{K}$ is reduced.
- L is purely inseparable $\iff$ $L \otimes_K \overline{K}$ is local.
- L is separable $\iff$ $\forall$ algebraic extensions Ω, $L \otimes_K \Omega$ is reduced.
- L is purely separable $\iff$ $\forall$ algebraic extensions Ω, $L \otimes_K \Omega$ is local.
- If L is separable then the map $\varphi : L \otimes_K \overline{K} \to \overline{K}^n$ defined as $\varphi(l \otimes k) = (k\varphi_1(l), \dots, k\varphi_n(l))$ (where φ_i are distinct homomorphisms from L to $\overline{K}$), is an isomorphism.
- Let L be a finite separable extension of K then it has only finitely many sub extensions.

Primitive element theorem

There exists $\alpha \in L$ s.t. $L = K(\alpha)$ whenever L is finite and separable.

Normal extensions

A normal extension of K is a splitting field of a family of polynomials in $K[X]$.
TFAE for an extension L of K,

- $\forall x \in L, P_{\text{min}}(x, K)$ splits in L.
- L is a normal extension.
- All homomorphisms from L to $\overline{K}$ have the same image.
- The group of automorphisms, $\text{Aut}(L/K)$ acts transitively on $\text{Hom}_K(L, \overline{K})$.

Some properties of normal extensions,

- $K \subset L \subset M$, if M is normal over K then it is normal over L, but L need not be normal over K.
- Extensions with degree 2 are normal.

Galois extensions

A field extension that is both normal and separable is called a Galois extension.

- For a finite extension L over K the number of automorphisms $|\text{Aut}(L/K)| \leq [L : K]$. Equality holds iff L is a Galois' extension.

If L is normal over K then,

- Isomorphism of sub extensions extend to automorphisms of L.
- $\text{Aut}(L/K)$ acts transitively on the roots of any irreducible polynomial in $K[X]$.
- If $\text{Aut}(L/K)$ fixes $x \notin K$. Then x is purely inseparable.

Galois groups

If L is a Galois extension, $G = \text{Gal}(L/K) = \text{Aut}(L/K)$ is called the Galois group of the extension.

- $L^{\text{Gal}(L/K)} = K$, (i.e. the set of invariants in L with the action of the Galois group is equal to K).
- Let L be a field and G a subgroup of $\text{Aut}(L)$, then
  - If all orbits of G are finite, then L is a Galois extension of L^G.
  - If order of G is finite then, $[L, L^G] = n$ and G is a Galois group.

The Fundamental theorem of Galois theory

Let L/K be a Galois extension, and $\text{Aut}(L/K) = \text{Gal}(L/K)$ is its Galois group.

- If L is finite over K, then for a intermediate field F and a subgroup $H \subset \text{Gal}(L/K)$ we have the following correspondence,
  - $F \to \text{Gal}(L/F)$
  - $H \to L^H$
- F is Galois over K $\iff$ $g(F) = F, \ \forall g \in \text{Gal}(L/K)$ $\iff$ $\text{Gal}(L/F) \trianglelefteq \text{Gal}(L/K)$

Discriminant

For a polynomial with roots x_i,the discriminant is $\Delta = \prod_{i<j}(x_i - x_j)^2$. For $\text{Gal}(P) \subset S_n$,

- Δ is preserved by any permutation.
- $\sqrt{\Delta}$ is preserved only by even permutations
- $G \subset A_n \iff \sqrt{\Delta} \in K$

Cyclotomic polynomials

Let $P_n = X^n - 1$ where n is coprime to the characteristic of a finite field K.
P_n has n distinct roots which form a cyclic multiplicative subgroup $\mu_n \subset \overline{K}^\times$.
Let μ_n* denote the set of **primitive roots of unity** (no roots of degree $< n$).

- $|\mu_n * | = \varphi(n)$

Cyclotomic polynomials: $\Phi_n = \prod_{\alpha \in \mu_n *}(X - \alpha) \in \overline{K}[X]$.

- $P_n = \prod_{d|n} \Phi_d$.
- Φ_n has coefficients in prime fields.
- If $\text{ch}(K) = 0$ then $\Phi_n \in \mathbb{Z}[X]$, else if $\text{ch}(K) = p$, we have Φ_n is the reduction mod p of the n^{th} cyclotomic polynomial over $\mathbb{Z}$.
- If $\text{ch}(K) = 0$, then Φ_n is irreducible over $\mathbb{Z}[X]$.

Consider L, splitting field of K

- The splitting field of P_n over K is $K(\zeta)$ where ζ is a root of Φ_n.
- All $g \in \text{Gal}L/K$ acts as $\zeta \to \zeta^{a^g}$, $(a^g, n) = 1$.
- $\text{Gal}(L/K)$ injects into $\mathbb{Z}/n\mathbb{Z}^\times$ and this is an isomorphism when Φ_n is irreducible over K.