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 $\text{ch}(F)$ 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 $\text{ch}(F) = 0$.

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 there exists a $P \in K[x]$ 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 there exists a unique 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.

Minimal Polynomial

If α is an algebraic element then there exists a unique 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.

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 .
- $[K(\alpha) : K] = \deg P_{\min}(\alpha, K)$

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.