Field & Galois Theory Reference

UW Student Seminars

A **group** is a collection of objects which can be multiplied and divided. (If the group operation is addition, we instead say "added" and "subtracted".) For example S_n, the set of all bijections between $\{1,...,n\}$ and itself, forms a group where the multiplication operation is function composition. A subgroup H of G is a **normal subgroup** if $gH = Hg$ for all $g \in G$. If this is the case we can define a **quotient group** $G/H = \{gH : g \in G\}$. This construction gives us a natural projection $\pi : G \to G/H$ given by $\pi(g) = gH$.

A **field** is a collection of objects which can be added and subtracted, and further can be multiplied and (except zero) divided. Furthermore, the multiplication distributes over addition. For example: $\mathbf{Q}$, the rational numbers; $\mathbf{R}$, the real numbers; $\mathbf{C}$, the complex numbers.

When a field is contained within another field, e.g. $\mathbf{Q} \subseteq \mathbf{C}$, we call the larger field a **field extension** of the smaller field. Note that the larger field is naturally a vector space over the smaller field, by only allowing multiplication of elements of the larger field by elements of the smaller field.

If $K \subseteq L$ are fields, then an element $\alpha \in L$ is **algebraic** over K if it is the root of some nonzero polynomial with coefficients in K. For instance i is a root of x^2+1 so i is algebraic over $\mathbf{Q}$. π is **transcendental** (not algebraic) over $\mathbf{Q}$.
If L contains only algebraic elements over K, then L is an algebraic extension of K. Otherwise L is a transcendental extension. For instance $\mathbf{Q} \subseteq \mathbf{C}$ is transcendental, whereas $\mathbf{R} \subseteq \mathbf{C}$ is algebraic. Can you see why?

If a is algebraic over K then the **minimal polynomial** of a over K is the smallest degree nonzero monic polynomial with coefficients in K with a as a root.

Let $K \subseteq L$ be an extension. Then $[L : K] = \dim_K L$ is the **degree** of L over K. We will use that $[K(a) : K] = \deg_K a$.

If $K \subseteq L$ are fields, and $S \subseteq L$ is a set, then $K(S)$ is the smallest subfield of L (i.e. $K(S) \subseteq L$) such that $S \subseteq K(S)$ and $K \subseteq K(S)$. For example $\mathbf{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 : (a,b,c) \in \mathbf{Q}^3\}$. (Check that this is a field, and that it's smallest.)

From now on, we mostly work with $\mathbf{Q} \subseteq \mathbf{C}$.

If p is a nonzero polynomial with coefficients in $\mathbf{Q}$, then the **splitting field** of p is the smallest field containing all roots of p. For example the splitting fiesld of x^2+1 is $\mathbf{Q}(i) = \{a + bi : (a,b) \in \mathbf{Q}^2\}$.

Let $K \subseteq L$. An **automorphism** φ of the extension L/K is a map that preserves the field structure and the extension structure. (That is, it fixes all elements of K, and is compatible with the field operations.) More concretely $\varphi : L \to L$ is a bijection such that $\varphi(ab^{-1} - c) = \varphi(a)\varphi(b)^{-1} - \varphi(c)$ and $\varphi(k) = k$ for $k \in K$.

If $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$ with L finite-dimensional over K as a vector space, and L is the splitting field for some $f(x) \in K[x]$, then we say L/K is **Galois**. Furthermore we define the **Galois group** of L/K to be $\mathrm{Gal}(L/K) = \{\sigma : \sigma \text{ an automorphism of L/K}\}$.

If $\mathbf{Q} \subseteq K \subseteq L \subseteq \mathbf{C}$ with L/K Galois, then the **fundamental theorem of Galois theory** says:
- there is a correspondence between subfields of L that contain K and the subgroups of $\mathrm{Gal}(L/K)$
- the normal subgroups of $\mathrm{Gal}(L/K)$ correspond to Galois extensions of K
- $|\mathrm{Gal}(L/K)| = [K : L]$

Theorem 1 (Universal Property of Quotients)**.** Let G be a group, H be a normal subgroup of G. Let $\pi : G \to G/H$ be the natural projection from G to G/H. Let Z be some other group and suppose there is a group homomorphism $\varphi : G \to Z$ such that $H \subseteq \ker(\varphi)$. Then there is a unique homomorphism $\widetilde{\varphi} : G/H \to Z$ such that $\widetilde{\varphi} \circ \pi = \varphi$.