Lecture 1-29: Transcendental and inseparable extensions

January 29, 2025

By now you have seen quite a bit of material on finite Galois extensions. The time has come to explore what happens when one moves beyond that setting. I will consider first simple transcendental extensions and then inseparable ones.

Suppose first that $L = K(t)$the field of rational functions in one variable t over a field K. The first order of business is to determine that group of automorphisms of L fixing K. Of course any such automorphism ϕ is determined by the image $\phi(t)$ of the variable t. It turns out that the possible images are the fractions $\frac{at+b}{ct+d}$, where $a, b, c, d \in K$ are such that $ad - bc \neq 0$ (so that $\frac{at+b}{ct+d}$ is not a constant). The maps $m_{a,b,c,d}$ sending t to $\frac{at+b}{ct+d}$ are called linear fractional transformations; they play a prominent role in a first course in complex analysis when $K = \mathbb{C}$ and the maps are regarded as functions from $\mathbb{C}$ to itself. Note that the map $m_{a,b,c,d}$ coincides with $m_{ka,kb,kc,kd}$ for any nonzero $k \in K$; apart from this case distinct choices of a, b, c, d lead to distinct maps $m_{a,b,c,d}$.

If we label the map $M_{a,b,c,d}$ by the matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then a simple calculation shows that the composite $m \circ m'$ of the maps m, m' with respective matrices M, M' is another linear fractional transformation with the matrix MM'. The upshot is that the Galois group G of K-automorphisms of L is isomorphic to $PGL_2(K)$, the quotient of the group $GL_2(K)$ of 2×2 invertible matrices over K by the normal subgroup of nonzero scalar matrices.

Armed with this calculation we can now ask whether there is a bijection between subgroups of G and fields between K and L, as there is in the case of a finite extension. The answer is very quickly seen to be no; for example, if K is finite, then so is $PGL(2, K)$ is also finite, but the degree $[L : K]$ is still infinite, so there is already a mismatch between $[L : K]$ and the order of G. The fixed field L^G is not K but a much larger field of which L is a finite extension. Thus we might want to restrict to the case where K is infinite, but here again we run into trouble. The subgroup U of linear fractional transformations of the form $t \to t + k$ for $k \in K$ corresponds to the image of the subgroup $\{\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} : k \in K\}$ of $GL(2, K)$ in G, which has infinite order and index in G, but there are no nonconstant rational functions f such that $f(t) = f(t + k)$ for all $k \in K$, so that the fixed field L^U collapses to the basefield K, even though $U \neq G$.

The reason for the mismatch becomes apparent when we look at the field side of the picture. Every nonconstant element of L is transcendental over K, so there is no field strictly between K and L that is finite over K. In fact it turns out by a famous result called Lüroth's Theorem that every field strictly between K and L takes the form $K(u)$, the rational function field generated by u, for some $u \in L$. Moreover, if we write $u = p/q$ in lowest terms for p, q in the polynomial ring $K[t]$, then a simple calculation using Gauss's Lemma shows that L is finite over $K(u)$ and $[L : K(u)]$ is the larger of the degrees of p and q. (In particular, this is why maps sending t to $\frac{p}{q}$ are not automorphisms of L if p and q are not both linear.) Thus we get a large number of finite extensions $L/K(u)$, to which Galois theory can be applied.

Whenever L is Galois over a subfield $K(u)$ there is a finite subgroup F of $PGL_2(K)$ such that $K(u) = L^F$. Unfortunately, very few finite groups F arise in this way! Last term, I showed that all finite subgroups of the orthogonal group $SO_(3, \mathbb{R})$ are either cyclic, dihedral, or isomorphic to one of the groups A_4, S_4, or A_5. The same list accounts for all the finite subgroups of $PGL_2(\mathbb{C})$). Thus, at least in the case $K = \mathbb{C}$, there are very few subfields $K(u)$ such that L is Galois over $K(u)$. For $K = \mathbb{R}$ things are even worse, as only cyclic and dihedral groups can occur. Also in general L need not even be separable over $K(u)$, as I will show below.

It turns out the subgroups of a different Galois group (not that of f over K, but rather that of $f(x) - t$ over $K(t)$) account for all the fields between $K(f(t))$ and $K(t)$, for $f \in K[t]$. Rather than pursue this any further, however, I make some general remarks about field extensions. Given an extension L of K, there will always be a maximal subset S of L consisting of elements algebraically independent over K, generating a subfield K' of L that is said to be purely transcendental over K; the subset S is called a transcendence base of L over K. Then L is algebraic over K'. A simple argument along the lines of the proof that any two bases of a vector space have the same cardinality shows that any two transcendence bases of L over K also have the same cardinality, called the transcendence degree of L over K (see p. 645).

I now turn to the other big skeleton in the closet of Galois theory, namely inseparable extensions. We already know that it takes some work even to construct an example of an inseparable extension, since even in characteristic $p > 0$, any finite field is Galois over any subfield of itself.

The simplest example of an inseparable extension starts with the subfield $K(t^p)$ of the rational function field $K' = K(t)$, where this time the field K has characteristic p. The field $L = k(t)$ is then inseparable over K'; as the only root of $x^p - t^p$ in L' is $x = t$, the automorphism group of L over K' is trivial. Nevertheless, the extension L' is not too badly behaved over K'; the multiplicativity of field degrees shows that the only fields between K' and L are K' and L themselves (since every such field has degree 1 or p over K').

One runs into trouble, however, as soon as one introduces a second variable. The extension $L = K(t, u)$ of the rational function field $K' = K(t^p, u^p)$ in two variables has degree p^2 over K' and trivial automorphism group, but now there are many fields between K' and L. Moreover, L is not a simple extension of K', since an easy calculation shows that $q^p \in K'$ for any $q \in L$, so that all simple nontrivial extensions of K' inside L have degree p over K'.

An extension L of a field K in characteristic p such that every $x \in L$ has $x^{p^k} \in K$ for some nonnegative integer k is called purely inseparable (p. 649) The automorphism group Aut (L/K) is always trivial in this case. In general, if $x \in L$ is not separable over K, then some power x^{p^k} of L is separable. Iterating this, one deduces that any algebraic extension L of a field K in characteristic p is a separable extension of an intermediate field K' purely inseparable over K (possibly K itself). The degree of L over this subfield K' is called the separable degree of L over K. Given three fields K, L, M with $K \subset L \subset M$, the separable degree of M over K is the product of the separable degrees of M over L and of L over K.