Galois Theory for Dummies - Part I

Yaniv LEVIATHAN

September 24 2007

1 Introduction

Galois theory is beautiful. It is also a vast and complicated subject (it requires some getting used to). In this article I will give an introduction to this topic. For those of you interested in a more in-depth covering of Galois Theory, I recommend reading J. S. Milne's "Fields and Galois Theory" (available online at http://www.jmilne.org/math/) or Jacobson's "Basic Algebra" (not available online to my knowledge).

In order to keep this article short (it is after all only an introduction to the topic!) and in order to give a slightly different presentation of the topic than is customary in algebraic literature, I will develop the theory in reverse order, compared to what is usually done in university courses. I will start with one problem Galois theory helps us solve and build only the parts of the theory which are needed to solve it.

I assume the reader is familiar with some basic notions of group theory and ring theory.

2 The Problem

The problem we will solve in this article is that of proving the following statement:

Every polynomial of degree $n \geq 5$ with coefficients in $\mathbb{Q}$ (i.e. the field of rational numbers) that is irreducible over $\mathbb{Q}$ and that has exactly $n-2$ real roots (so that it has exactly 2 complex roots) is such that all its roots cannot be expressed by using rational operations ($+ - \times \div$) and rational exponentiations (e.g. $\sqrt{2}$ or $(-15)^{3/4}$).

The first question to answer is whether such polynomials exist (to show that indeed this problem is of some interest). This is the topic of the next section.

3 An Example Polynomial

Choose k unique even integers $n_1, ..., n_k$. Define

$$g(x) = (x^2+2)(x-n_1)...(x-n_k)$$

Note that $g(x)$ is of degree $k+2$ and has exactly k real roots (namely $n_1, ..., n_k$). The problem is that $g(x)$ is not irreducible. Now consider all the numbers $x \in \mathbb{Q}$ such that $g'(x) = 0$ (where $g'(x)$ is the derivative of $g(x)$ - yes, derivatives are also used in algebra!). As all the real roots (or equivalently the rational roots) of g are simple (the n_i's are distinct) the derivative $g'(x)$ of $g(x)$ doesn't vanish at any of them. Thus $|g(x)| > 0$ for all $x \in \mathbb{Q}$ such that $g'(x) = 0$ (and there are only finitely many such x's). Denote

$$e = min_{g'(x)=0}|g(x)|$$

Thus $e > 0$. Choose an odd n such that $\frac{2}{n} < e$. Define

$$f(x) = g(x) - \frac{2}{n}$$

It is obvious that $f(x)$ has the same number of real roots, k, as $g(x)$ (we merely moved down the graph of $g(x)$ by so little that the number of intersections with the x-axis hasn't changed). All that remains is to show that $f(x)$ is irreducible over $\mathbb{Q}$. This is a direct result of Eisenstein's Lemma below (after multiplying $f(x)$ by n).

Before proving it we will need one extra result, namely

Gauss's Lemma 1. *A polynomial with integer coefficients is reducible over $\mathbb{Z} \iff$ it is reducible over $\mathbb{Q}$.*

Proof. ($\Leftarrow$) is obvious. ($\Rightarrow$) is proved as follows. Suppose $f(x)$ splits in $\mathbb{Q}$. Then $f(x) = g(x)h(x)$ and there are integers m, n such that

$$m \times n \times f(x) = G(x)H(x)$$

such that $G(x), H(x)$ have coefficients in $\mathbb{Z}$. Now say a prime p divides $m \times n$. Then consider the equation modulo p:

$$0 = \bar{G}(x)\bar{H}(x)$$

Where $\bar{G}(x)$ and $\bar{H}(x)$ are $G(x)$ and $H(x)$ modulo p respectively. Now since p is prime, a multiplication of two polynomials yielding zero means that one of them is the zero polynomial (check the coefficients of the highest power of x). WLOG suppose $\bar{G}(x) = 0$. Then $p|G(x)$. Divide both sides of the equation above by p to get

$$\frac{m \times n}{p} f(x) = \frac{G(x)}{p} H(X)$$

Where both sides are still in $\mathbb{Z}[x]$. We can continue in this fashion until the constant multiplying $f(x)$ is 1.

□

Eisenstein's Criterion 1. *Let*

$$f(x) = a_n x^n + ... + a_1 x + a_0$$

in $\mathbb{Z}[x]$. If a_n is not divisible by a prime p and a_i is divisible by p for $0 \leq i \leq n-1$ and a_0 is not divisible by p^2 then f is irreducible over $\mathbb{Q}$.

Proof. By Gauss's Lemma it is enough to show that $f(x)$ is irreducible in $\mathbb{Z}$. Suppose it is. Then we have

$$a_nx^n + ... + a_1x + a_0 = (b_mx^m + ... + b_0)(c_lx^l + ... + c_0)$$

Now $a_0 = b_0c_0$. And we know that $p|a_0$ but $p^2 \nmid a_0$. So p divides b_0 or c_0, but not both. WLOG assume $p|b_0$. Now $a_1 = b_1c_0 + b_0c_1$. Now $p|a_0$ and $p|b_0$ but $p \nmid c_0$. Therefore $p|b_1$. Continuing in this fashion we get $p|b_m$, but then $p|a_n = b_mc_l$. Contradiction.

□

This proves our claim that the example polynomial above is indeed irreducible over $\mathbb{Q}$ (use Eisenstein's Criterion with $p = 2$).

4 Field Extensions

Let E, F be fields such that $F \subseteq E$ (e.g. $\mathbb{Q} \subseteq \mathbb{R}$). We say that E is a *field extension* of F, or that F is a *subfield* of E. We denote a field extension E over F as $\frac{E}{F}$.

Now suppose F is a field and $f(x) \in F[x]$ is irreducible of degree n. Consider the set $E = (a_1, ..., a_n), a_i \in F$ of n-tuples of elements of F. Define two operations on E, namely $+$ and $\times$ as follows. If $u, v \in E, u = (u_1, ..., u_n), v = (v_1, ..., v_n)$ then

$$u + v = (u_1 + v_1, ..., u_n + v_n)$$
$$u \times v = \sigma^{-1}(\sigma(u) \times \sigma(v))$$

Where $\sigma : E \to \frac{F[x]}{(f(x))}$ is defined as $\sigma(u_1, ..., u_n) = u_1 + ... + u_nx^{n-1} + (f(x))$.

I will now show that the set E which we have constructed is in fact a field, and using the natural isomorphism $\pi : F \to E, \pi(x) = (x, 0, ..., 0)$, we see that E is a field extension of F. Note that disregarding the × operation E constitutes an n-dimensional vector space over F.

It is clear that E is closed under the operations just defined.

We need to prove that for all $0 \neq u \in E$ there is a $v \in E$ such that $u \times v = 1$ $(= (1, 0, ..., 0))$. Consider the polynomial $p(x)$ in $F[x]$ of lowest degree belonging to the equivalence class of $\sigma(u)$. It is a nonzero polynomial of degree at most n-1 in $F[x]$. Thus it is co-prime to $f(x)$. Thus there are polynomials $s(x), t(x) \in F[x]$ such that $s(x)p(x) + t(x)f(x) = 1$ (using Euclid's gcd algorithm). Let $v = \sigma^{-1}(s)$. It is clear that $v \times u = 1$ as required (if this is not clear to you at this point try to prove it).

The other field axioms are proved similarly. Note that sometimes it is helpful to think of E as a collection of polynomials (actually a set of *equivalence classes of polynomials*) rather than as a collection of n-tuples (using σ to go back and forth between the two). So the above also states that if $f(x)$ is an irreducible polynomial over a field F, then the ring $\frac{F[x]}{(f(x))}$ is in fact a field containing F (F is identified with the set of constant polynomials).

4.1 Example

Consider the field $\mathbb{Z}_2 = 0, 1$. Let $f(x) = x^2 + x + 1$. As $f(x)$ has no roots in $\mathbb{Z}_2$ it is irreducible. Consider the field $E = \mathbb{Z}_2^2$. Then for example, $(0, 1) \times (1, 1) = \sigma^{-1}((x + (x^2 + x + 1)) \times (x + 1 + (x^2 + x + 1))) = \sigma^{-1}(x^2 + x + (x^2 + x + 1)) = \sigma^{-1}(1) = (1, 0) = 1$.

5 Field Automorphisms

Let E be a field. An automorphism of E is an isomorphism of E onto itself. For example consider the field $\mathbb{C}$ of complex numbers. Then the map $\eta : \mathbb{C} \rightarrow \mathbb{C}$ defined as $\eta(a + bi) = a - bi, a, b \in \mathbb{R}$ is an automorphism of $\mathbb{C}$.

Let $\frac{E}{F}$ be a field extension. An automorphism of E/F is an automorphism of E that fixes every element of F. So the automorphism of $\mathbb{C}, \eta$, defined above, is also an automorphism of $\frac{E}{F}$.

Note that if $\frac{E}{F}$ is a field extension then the set of automorphisms of $\frac{E}{F}$ constitutes a group. We call this group the *Galois group* of $\frac{E}{F}$ and denote it $Gal(\frac{E}{F})$.

To be continued...

Stay tuned for part II!