Notes for MA591U, Spring 2001
(Symbolic Computation)

Galois Theory of Polynomials

NOTATION: I use the following notation in these notes. The conventions come from various algebra texts.

(1) ι indicates the identity function, or the identity permutation, depending on the context.

(2) (1), $(1\ 2)$, $(1\ 3\ 2)$ denote permutations according to cyclic form.

(3) $H < G$ means "H is a subgroup of G."

(4) $N \lhd G$ means "N is a normal subgroup of G."

(5) S_n indicates the group of permutations of n objects.

(6) A permutation σ is *even* if $\sigma\left(\prod_{i<j}(x_i - x_j)\right) = \prod_{i<j}(x_i - x_j)$.

(6) A_n indicates the group of *even* permutations of n objects; e.g., $(\sigma \in A_n) \Rightarrow (\sigma(\alpha_1 - \alpha_2) = \sigma(\alpha_2 - \alpha_1$

Let $f \in \mathbb{Q}[x]$ be squarefree. We want to study the "symmetries" of the roots.

Given f, there is a *splitting field* $k = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ that is the smallest field that contains all the roots of f. Symmetries of the roots of f are automorphisms of k over $\mathbb{Q}$, say

$$\text{Gal}\left({}^{k}/_{\mathbb{Q}}\right) \doteq \{\varphi | \varphi\ k \to k \text{ is a bijective ring homomorphism and } \varphi|_{\mathbb{Q}} = \iota\}.$$

We also refer to this set as $\text{Gal}(f)$.

FACTS:

1. In fact, $\text{Gal}\left({}^{k}/_{\mathbb{Q}}\right)$ is a group under composition.
2. For any $\varphi \in \text{Gal}\left({}^{k}/_{\mathbb{Q}}\right)$ and any root α_i of f,

$$0 = \varphi(0) = \varphi(f(\alpha_i)) = f(\varphi(\alpha_i)),$$

so $\varphi(\alpha_i)$ is also a root of f. Hence φ is a permutation of the roots of f. Thus

$$\text{Gal}(f) < S_n.$$

DEFINITION: We say that f is *reducible* over a field k when it factors as $f(x) = (x-\alpha_1)(x-\alpha_2)$ with $\alpha_1, \alpha_2 \in k$. If f is not reducible over k, we say it is *irreducible* over k.

GENERAL FACT: If f is irreducible over $\mathbb{Q}$ and its splitting field is $k = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, then for any $i \in \{1, \ldots, n\}$, there exists some $\varphi \in \text{Gal}\left({}^{k}/_{\mathbb{Q}}\right)$ such that $\varphi(\alpha_1) = \alpha_i$.

EXAMPLES:

1. Let $f(x) = x^2 + ax + b \in \mathbb{Q}[x]$.

Suppose f is reducible over k. The splitting field of f is $k = \mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}$. Hence $\mathrm{Gal}(f) = \{\iota\}$, since there are no roots outside of $\mathbb{Q}$ to permute.

Now assume f is irreducible over $\mathbb{Q}$. Then we know from the general fact above that $(1\,2) \in \mathrm{Gal}(f) < S_2$. This tells us that $\mathrm{Gal}(f) = S_2 = \{(1), (1\,2)\}$.

2. Let $f(x) = x^3 + ax + b \in \mathbb{Q}[x]$. (As we will indicate later, we can actually write *any* cubic in this form.)

If f is reducible over $\mathbb{Q}$, it has a factor of degree one, and so it has a root in $\mathbb{Q}$: $f(x) = (x - \alpha_1) \cdot g(x)$ where $\alpha_1 \in \mathbb{Q}$ and $g \in \mathbb{Q}[x]$ is quadratic. Then the splitting field of f will be the same as the splitting field of g; that is,

$$\mathrm{Gal}(f) = \mathrm{Gal}(g) \in \{\{\iota\}, S_3\}.$$

If f is irreducible over $\mathbb{Q}$, let $k = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ be its splitting field. Then

$$\mathrm{Gal}(f) < S_3 = \{(1), (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}.$$

Since f is irreducible, $\exists \varphi_i \in \mathrm{Gal}(f)$ such that $\varphi_1(\alpha_1) = \alpha_2$ and $\varphi_2(\alpha_1) = (\alpha_3)$ and $\varphi_3(\alpha_2) = \alpha_3$. The only permutations that contain enough subgroups to satisfy this are S_3 or $A_3 = \{(1), (1\,2\,3), (1\,3\,2)\}$, which are both "cyclic".

How do we tell which is the Galois group of a particular f? We take a brief excursion into symmetric functions.

DEFINITION: Given $f(x_1, \ldots, x_n)$ and $\pi \in S_n$, we define $f^\pi(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)})$.

EXAMPLE: Let $f(x) = x_1^2 + x_2$ and $\pi = (1\,2)$. Then $f^\pi(x) = x_2^2 + x_1$.

THEOREM: If $f = f^\pi$ for every $\pi \in S_n$, then we can write f as a polynomial in

$$s_0 = 1 \quad s_1 = \sum_i x_i \quad s_2 = \sum_{i<j} x_i x_j \quad s_3 = \sum_{i<j<k} x_i x_j x_k \cdots \quad s_n = x_1 \cdots x_n.$$

PROOF:

See Cox, Little, O'Shea's *Ideals, Varieties, and Algorithms.* Their proof uses Gröbner bases.

FACT: If we define the s_i on the roots α_i of a monic polynomial f, then

$$f(x) = \sum_{i=0}^{n} (-1)^i s_i x^{n-i}.$$

(Simply multiply out $f(x) = \prod_i (x - \alpha_i)$ to demonstrate this.)

EXAMPLES:
1. $(x_1 - x_2)^2 = x_1^2 - 2x_1x_2 + x_2^2 = (x_1 + x_2)^2 - 4x_1x_2 = s_1^2 - 4s_2$.
2. $[(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)]^2 = s_1^2s_2^2 - 4s_2^3 - 4s_1^3s_2 - 27s_3^2 + 18s_1s_2s_3$.

Returning to the irreducible cubic f, let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f. We want to decide if $\text{Gal}(f) = S_3$ or $\text{Gal}(f) = A_3$. Consider $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$ and set $\Delta = \delta^2$. From the fact immediately above, we know that given our f, $a = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3$ and $b = -\alpha_1\alpha_2\alpha_3$ while $0 = -(\alpha_1 + \alpha_2 + \alpha_3)$. The second example tells us then that $\Delta = -4a^3 - 27b^2 \in \mathbb{Q}$.

CLAIM: For any irreducible $f \in \mathbb{Q}[x]$, $\text{Gal}(f) = A_3$ if, and only if, $\Delta = x^2$ for some $x \in \mathbb{Q}$; that is, if and only if $\delta \in \mathbb{Q}$.
PROOF:

Suppose $\delta \in \mathbb{Q}$. Then δ is invariant under all $\pi \in \text{Gal}(f)$. Hence all elements of $\text{Gal}(f)$ are even. So $\text{Gal}(f) < A_3$. Since $\text{Gal}(f) \neq \{(1)\}$ (as f is irreducible), and the only non-trivial subgroup of A_3 is A_3 itself, $\text{Gal}(f) = A_3$.

Conversely, assume that Δ is not square in $\mathbb{Q}$, so that $\delta \notin \mathbb{Q}$. A general fact: if k is the splitting field of a squarefree f, and $\gamma \in k \backslash \mathbb{Q}$, then $\exists \sigma \in \text{Gal}\left(k/\mathbb{Q}\right)$ such that $\sigma(\gamma) \neq \gamma$. Now, this means that since $\delta \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ and $\delta \notin \mathbb{Q}$, we have some $\sigma \in \text{Gal}(f)$ such that $\sigma(\gamma) \neq \gamma$. Hence $\sigma(\delta) = -\delta$, whence $\sigma \notin A_3$. Thus $\text{Gal}(f) \not< A_3$, and we conclude that $\text{Gal}(f) = S_3$, as there are no other possibilities.

EXAMPLES:
1. $f(x) = x^3 - x + 1$ has $\Delta = -4 \cdot -1 - 27 = -23 \notin \mathbb{Q}^2$. So $\text{Gal}(f) = S_3$.
2. $f(x) = x^3 - 3x + 1$ has $\Delta = -4 \cdot -27 - 27 \cdot 1 = 81 = 9^2$ so $\text{Gal}(f) = A_3$.

DEFINITION: We call Δ the *discriminant*. Note that Δ vanishes if, and only if, f has a repeated root. This makes it very useful.

DEFINITION: We say that $\text{Gal}(f)$ *acts transitively* on the roots of f if

$$\forall \alpha_i, \alpha_j, i \neq j \, (\exists \sigma \in \text{Gal}(f) \text{ such that } \sigma(\alpha_i) = \alpha_j) \, .$$

PROPOSITION: Let f be squarefree. $\text{Gal}(f)$ acts transitively on the roots of f if, and only if, f is irreducible.
PROOF:

The converse follows from properties of a splitting field. See Lang's *Algebra* for details.

Assume $\text{Gal}(f)$ acts transitively on the roots of f. Let $f(\alpha) = 0$ and set $g \in \mathbb{Q}[x]$ to be the minimal polynomial of α. Then there exists some $h \in \mathbb{Q}[x]$ such that $f = gh$. Using transitivity and the fact that $0 = \sigma(g(\alpha)) = g(\sigma(\alpha))$, we see that all roots of f are roots of

g. So $\deg f = \deg g$ (since f is squarefree!). Hence $f = cg$ for some $c \in \mathbb{Q}$, and g's being minimal means g, and hence f, must be irreducible.

NOTATION: We will write Gal to indicate $\text{Gal}\left({}^{\text{K}}/_{k}\right)$ in what follows.

MAIN THEOREM OF GALOIS THEORY
For any subfield $\mathbb{F}$ of $\mathbb{K}$ so that $k \subset \mathbb{F} \subset \mathbb{K}$, write

$$G\left({}^{\text{K}}/_{\text{F}}\right) \doteq \{\sigma \in \text{Gal} | \sigma : \mathbb{K} \to \mathbb{K} \text{ is an automorphism, and } \sigma|_{\text{F}} = \iota\}.$$

For any subgroup H where $\{(1)\} < H <$ Gal, write

$$\mathbb{K}^H \doteq \{\alpha \in \mathbb{K} | \sigma(\alpha) = \alpha \, \forall \sigma \in H\}.$$

Then $H \mapsto \mathbb{K}^H$ is a bijection of subgroups of G onto subfields $\mathbb{F}$ of $\mathbb{K}$. The inverse of this map is $\mathbb{F} \mapsto G\left({}^{\text{K}}/_{\text{F}}\right)$; that is,

$$H \mapsto \mathbb{K}^H \mapsto G\left({}^{\text{K}}/_{\text{K}^H}\right) = H.$$

Furthermore, a subfield $\mathbb{F} \subset \mathbb{K}$ is a splitting field if, and only if, $G\left({}^{\text{K}}/_{\text{H}}\right)$ is normal in Gal, in which case $\text{Gal}\left({}^{\text{F}}/_{k}\right) \cong \text{Gal}\left({}^{\text{K}}/_{\text{F}}\right)$.

We present the following **DIAGRAM** as as indication of what is going on here:

$$\begin{array}{ccl}
\mathbb{K} & \to & G\left({}^{\text{K}}/_{\text{K}}\right) = \{\sigma : \mathbb{K} \to \mathbb{K} |\, \sigma|_{\text{K}} = \iota\} = \{\iota\} \\
\cup & & \cap \\
\mathbb{F} & \to & G\left({}^{\text{K}}/_{\text{F}}\right) = \{\sigma : \mathbb{K} \to \mathbb{K} |\, \sigma|_{\text{F}} = \iota\} \\
\cup & & \cap \\
k & \to & G\left({}^{\text{K}}/_{k}\right) = \{\sigma : \mathbb{K} \to \mathbb{K} |\, \sigma|_{k} = \iota\} = \text{Gal}\left({}^{\text{K}}/_{k}\right)
\end{array}$$

NOTE: This implies that $k \mapsto G\left({}^{\text{K}}/_{k}\right) \mapsto \mathbb{K}^{G\left({}^{\text{F}}/_{k}\right)} = k$; that is,

$$\left\{\alpha \in \mathbb{K} : \, \sigma(\alpha) = \alpha \, \forall \sigma \in \text{Gal}\left({}^{\text{K}}/_{k}\right)\right\} = k.$$

So if $\alpha \in \mathbb{K} \backslash k$, then there exists some σ such that $\sigma(\alpha) \neq \alpha$.

EXAMPLE: Recall that $f(x) = x^3 - x + 1$ has Gal $= S_3$. Then the diagram becomes

$$\begin{array}{ccl}
\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) & \to & \{\iota\} \\
\cup & & \cap \\
\mathbb{F} = \mathbb{Q}(\delta) = \mathbb{Q}\left(\prod_{i<j}(\alpha_i - \alpha_j)\right) & \to & \{\sigma |\, \sigma(\delta) = \delta\} = A_3 \\
\cup & & \cap \\
\mathbb{Q} & \to & S_3
\end{array}$$

RECALL: $\Delta = \delta^2 \in \mathbb{Q}$, so $\mathbb{F}$ is the splitting field of $x^2 - \Delta$. Since $\mathbb{F}$ is the splitting field of an irreducible quadratic, $\mathrm{Gal}\left(\mathrm{F}/\mathrm{Q}\right) = S_2 = \mathrm{Z}/_{2\mathrm{Z}} \cong^{S_3} /_{A_3}$.

DIAGRAMS: The field extension diagram

$$\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$$

$$\mathbb{Q}(\alpha_1) \quad \mathbb{Q}(\delta) \qquad \mathbb{Q}(\alpha_2) \qquad \mathbb{Q}(\alpha_3)$$

$$\mathbb{Q}$$

corresponds to the subgroup diagram

$$\{(1)\}$$

$$\{(1), (2\,3)\} \quad A_3 \quad \{(1), (1\,3)\} \quad \{(1), (2\,3)\}$$

$$S_3$$

Now we consider the purpose of Galois theory, the question of the solvability of a polynomial by radicals. Recall that

$$\left(ax^2 + bx + c = 0\right) \Leftrightarrow \left(x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}\right).$$

In this vein, we say that a polynomial f is *solvable by radicals* if its splitting field $\mathbb{K}$ is contained in a field $\mathbb{E}$ admitting a tower

$$k = \mathbb{E}_o \subset \mathbb{E}_1 \subset \cdots \subset \mathbb{E}_m = \mathbb{E}$$

where, for each i, $\mathbb{E}_i = \mathbb{E}_{i-1}(\alpha_i)$ where $\alpha_i^{n_i} \in \mathbb{E}_{i-1}$ for some $n_i \in \mathbb{N}$. So $\mathbb{E}_0 = k$, $\mathbb{E}_1 = k(\sqrt[n_1]{\alpha_1})$, $\mathbb{E}_2 = k(\sqrt[n_1]{\alpha_1}, \sqrt[n_2]{\alpha_2})$, etc., where $\alpha_1 \in k$, $\alpha_2 \in k(\sqrt[n_1]{\alpha_1})$, etc.

EXAMPLES:
1. $f(x) = ax^2 + bx + c$ has splitting field $\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\sqrt{b^2 - 4ac})$. The ancient civilizations knew the quadratic formula, which gives us this.
2. Let $f(x) = x^3 + ax^2 + bx + c$.

Define $z = x - a_2/3$. We get a new polynomial $f(x) = z^3 + pz + q$. Then

$$\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \subseteq \mathbb{Q}\left(\sqrt{\Delta}, \sqrt{-3}, \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-2}\sqrt{\Delta}}\right).$$

The Italian Cardano gave an explicit formula for this during the middle ages.
3. There is also a formula for $x^4 + ax^3 + bx^2 + cx + d$, but not beyond that, as we show below.

For the explicit formulas of the cubic and the quartic, we refer the reader to van der Waerden's *Modern Algebra*, second edition, volume 1.

DEFINITION: A group G is solvable if there is a tower of normal subgroups

$$\{\iota\} = G_0 \lhd G_1 \lhd \cdots \lhd G_m = G$$

where each ${}^{G_i}/_{G_{i-1}}$ is cyclic.

EXAMPLES:

S_2 is cyclic, so it is solvable.

$S_3 \rhd A_3 \rhd \{(1)\}$ and ${}^{S_3}/_{A_3} \cong^{\mathrm{Z}} /_{2\mathrm{Z}}$, ${}^{A_3}/_{\{(1)\}} \cong^{\mathrm{Z}} /_{3\mathrm{Z}}$, so it is solvable.

S_4 is also solvable, but S_n is *not* solvable for $n \geq 5$. (The clown guilty for this gross inconvenience is actually A_n. For details, see an algebra text.)

THEOREM: f is solvable by radicals if, and only if, $\mathrm{Gal}(f)$ is solvable.

A proof of the theorem above is beyond the scope of this course. However, note that, from a computational point of view, when $n \leq 4$, the tower of solvable groups tells us how to find a formula for the roots.

OPEN PROBLEM: Let $f \in \mathbb{Q}[x]$ have degree n.

We know there exists an algorithm that calculates the generators of the Galois group of f in exponential time (on n and the bit size of the coefficients of f). Is there some algorithm that calculates the generators of the Galois group that has polynomial time?

We *do* know that we can decide in polynomial time whether the Galois group is solvable. For this result, see Susan Landau and Gary Miller in *Comp. Sys. Sci.*, vol. 30, 1985.