Algebra Notes
Math 123 — Harvard University
Spring 2002

Varieties and divisibility.

Theorem 0.1 *Let $f, g \in \mathbb{C}[t_1, \ldots, t_n]$ satsify $V(f) \subset V(g)$, and suppose f is irreducible. Then f divides g.*

Proof. By the definition of irreducibility, f is neither zero nor a unit. Thus f has positive degree in some variable, say $z = t_n$. Let $t = (t_1, \ldots, t_{n-1})$, and regard f and g as elements $f(t, z)$ and $g(t, z)$ of $R[z]$ where $R = \mathbb{C}[t_1, \ldots, t_{n-1}]$. Let F denote the field of fractions of R, i.e. the rational functions in $(t_1, \ldots, t_{n-1})$.

Suppose we have $V(f) \subset V(g)$ but f does not divide g. We will obtain a contradiction.

By Gauss's Lemma, f is irreducible in $F[z]$, and f does not divide g in $F[z]$. Since $F[z]$ is a PID, the ideal $(f, g) = (1)$. Thus there are $r, s \in F[z]$ such that

$$fr + gs = 1$$

in $F[z]$. (These r and s are obtained using the division algorithm, and they implicitly involve the resultant of f and g.)

Now choose t_0 such that the denominators appearing in r and s (which belong to F and are hence polynomials in t) do not vanish at $t = t_0$, and also such that the leading coefficient $a_0(t)$ of $f(t, z) = a_0(t)z^d + \cdots + a_d(t)$ does not vanish at $t = t_0$. Then $f(t_0, z)$ is a polynomial of positive degree in z, so $f(t_0, z_0) = 0$ for some point z_0. Since we have $V(f) \subset V(g)$, we also have $g(t_0, z_0) = 0$. Moreover r and s assume finite values at (t_0, z_0), so we cannot have $fr + gs = 1$.

Thus $f|g$ in $F[z]$ and hence in $R[z]$. ∎

Class number 1 and almost identities.

Let $f(x) = (e^{\pi\sqrt{x}} - 744)^{1/3}$. Then $f(d)$ is pretty close to an integer when $\mathbb{Q}[\sqrt{-d}]$ has class number one (i.e. when its integers form a UFD.

For example, $f(163) = 640319$ to an error of less than 10^{-24}!

Explanation: it is known that the value of the j-function from the theory of elliptic curves is an algebraic integer at points $\tau \in \mathbb{H}$ such that $\mathbb{Z}[\tau]$ is an ideal in the ring of integers for $K = \mathbb{Q}(\sqrt{-d})$. In fact the degree of $j(\tau)$ over $\mathbb{Q}$ is the class number h of

K. In particular, if $h = 1$ (as is the case for $d = 163$), then $j(\tau)$ is an integer. This holds when τ generates the full ring of integers, e.g. when $\tau = (1 + \sqrt{-163})/2$.

Now the j-function has an expansion

$$j(q) = q^{-1} + 744 + O(q)$$

where $q = \exp(2\pi i\tau)$. Setting $\tau = (1 + \sqrt{-163})/2$, we obtain $q = -\exp(-\pi\sqrt{163})$. Plugging into the power series of j above, we have that $j(q)$ is an integer, and at the same time $j(q)$ is very close to $1/q + 744$. This explains why $\exp(\pi\sqrt{-163})$ is very nearly an integer. The cube root is subtler.

Class group examples. What is the class group of the ring of integers R in $K = \mathbb{Q}(\sqrt{-10})$?

Solution. Since $-10 = 2 \bmod 4$, the ring R is $\mathbb{Z}[\sqrt{-10}]$. Thus $\Delta(R) = \sqrt{10}$. By the Minkowski bound $\mathcal{C}$ is generated by factors of primes less than $\mu = (4/\pi)\Delta(R)$ which is itself less than $4/3\sqrt{10}$ which is less than 5. Thus we only have to factor (2) and (3).

Now $x^2 + 10 = x^2 + 1 \bmod 3$ has no roots in $\mathbb{F}_3$, so 3 is inert (it remains prime). On the other hand, $x^2 + 10 = x^2 \bmod 2$, so we have $(2) = P\overline{P}$ for some prime ideal P. In fact $P = (2, \sqrt{-10})$. Thus $P = \overline{P}$ and so P has order 1 or 2 in $\mathcal{C}$.

Can P be principal? If $P = (a + b\sqrt{-10})$ then $N(P) = 2 = a^2 + 10b^2$, which has no solutions. Thus P is not principal and we have shown that $\mathcal{C} = \mathbb{Z}/2$.

An example of a PID that is not a Euclidean domain. The ring of algebraic integers in $\mathbb{Q}(\sqrt{-19})$, namely $R = \mathbb{Z}[(1 + \sqrt{-19})/2]$, is a PID but not a Euclidean domain. For a proof, see Dummit and Foote, *Abstract Algebra*, p.278.

Fundamental units. Examples of fundamental units for real quadratic fields $K = \mathbb{Q}(\sqrt{d})$ have irregular size.

For $d = 2, 3, 5, 6$ we can take $\epsilon = 1 + \sqrt{2}, 2 + \sqrt{3}, (1 + \sqrt{5})/2$ and $5 + 2\sqrt{6}$. But for $d = 19$ a fundamental unit is $\epsilon = 170 + 39\sqrt{19}$; for $d = 67$ we have

$$\epsilon = 48842 + 5967\sqrt{67},$$

and for $d = 94$ we have

$$\epsilon = 2143295 + 221064\sqrt{94}.$$

Constructing the regular 65537-gon.

From Coxeter's *Introduction to Geometry*, 1980:

> Euclid's postulates imply a restriction on the instruments that he allowed for making constructions, namely the restriction to ruler (or straightedge)

> and compasses. He constructed an equilateral triangle (I.1 [Book I, sect. 1 of the Elements]), a square (IV.6), a regular pentagon (IV.11), a regular hexagon (IV.15), and a regular 15-gon (IV.16). THe number of sides may be doubled again and again by repeated angle bisections. It is natural to ask which other regular polygons can be constructed with Euclid's instrments. This question was completely answered by Gauss (1777-1855) at the age of nineteen. Gauss found that a regular n-gon... can be so constructed if the odd prime factors of n are distinct Fermat primes
>
> $$F_k = 2^{2^k} + 1.$$
>
> The only known primes of this kind are [3, 5, 17, 257, 65537].
>
> To inscribe a regular pentagon in a given circle, simpler constructions than Euclid's were given by Ptolemy and Richmond... [latter given]
>
> Richmond also gave a simple construction for the [17-gon]... [given].
>
> Richelot and Schwendenwein constructed the regular 257-gon in 1832. J. Hermes spent ten years on the regular 65537-gon and deposited the manuscript in a large box in the University of Goettingen, where it may still be found.

A quartic polynomial. A chain of Galois extension is not necessarily Galois. Consider the example:

$$F = \mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) = E$$

Each extension is quadratic, hence Galois, but E/F is *not Galois*. For example, the polynomial $X^4 - 2$ has a root in E but does not split completely there, since it lacks its complex roots.

To understand this polynomial in more detail, consider its splitting field $K = \mathbb{Q}(i, \sqrt[4]{2})$. Since K/E is quadratic, clearly $\deg(K/F) = 8$. The Galois group acts effectively by permutations of the 4 roots of $X^4 - 2$.

If we think of the roots as forming a diamond in the complex plane, then the action is by the dihedral group D_4 of order 8.

To see this, note that the extension $K/\mathbb{Q}(i)$ has degree 4 and is generated by $\sqrt[4]{2}$. Thus the polynomial $x^4 - 2$ is irreducible over $\mathbb{Q}(i)$, and so their exists an autmorphism ϕ of $K/\mathbb{Q}(i)$ sending $\sqrt[4]{2}$ to $i\sqrt[4]{2}$. Since this automorphism commutes with multiplication by i, it cyclically permutes the 4 roots of f.

Complex conjugation, on the other hand, provides another automorphism ψ of K that fixes two roots of f and exchanges the other two. The automorphisms ϕ and ψ generate D_4, a group of order 8, which must coincide with the full Galois group since $8 = \deg(K/\mathbb{Q})$.

The subfield E is fixed by complex conjugation; that is, $G^E = \mathbb{Z}/2$. This subgroup is *not normal*, which explains why E/F is not Galois.

This example is also instructive for the construction of automorphisms of a splitting field. Let $L = \mathbb{Q}(\sqrt{2})$. There is an automorphism ϕ of L/F given by $\sqrt{2} \mapsto -\sqrt{2}$. But this autmorphism does *not* extend to E. The point is that E/L is the splitting field of $g(x) = x^2 - \sqrt{2}$. We have $\phi(g) = x^2 + \sqrt{2}$ which does *not* split in E. But g and $\phi(g)$ are both factors of $f(x) = x^4 - 2$, so $\phi(g)$ *does* split in the splitting field K, allowing the automorphism to extend.

Solvable Galois extensions.

Most books have some awkwardness about solvable extensions and solvability by radicals. Here we try to flesh out the details. All fields will have characteristic zero.

The main result is:

Theorem 0.2 *An irreducible polynomial $f(x) \in F[x]$ is solvable by radicals iff its splitting field has solvable Galois group.*

Here $f(x)$ is solvable by radicals if it has a root in some field K/F that can be reached by a sequence of radical extensions.

We begin with some remarks that are easily verified.

1. The Galois group G of $f(x) = x^n - 1$ over F is abelian. Indeed, G injects into $(\mathbb{Z}/n)^*$.

2. If F contains the nth roots of unity, then the Galois group of $x^n - a$ over F is also abelian. In fact, G is a subgroup of $\mathbb{Z}/n$.

3. If K/F is a solvable extension and E/F is an intermediate Galois extension, then E/F is also solvable. Just note that $\mathrm{Gal}(E/F)$ is a quotient of $\mathrm{Gal}(K/F)$.

4. If K/F is Galois, and we have $F = F_1 \subset F_2 \subset \cdots F_m = K$ where each F_{i+1}/F_i is solvable, then K/F is solvable.

Now we come to a central technical point.

Theorem 0.3 *Let E/F be a solvable extension, and let $g(x) = x^n - e$, $e \in E$. Then the splitting field of g over E is contained in a solvable extension K/F.*

Proof. To build K first choose $h(x) \in F[x]$ such that E is the splitting field of h. Now let $G = \mathrm{Gal}(E/F)$ and let $f(x) = \prod_G (x^n - g \cdot e)$. Then $f \in F[x]$. Finally let K be the splitting field of

$$f(x)(x^n - 1)h(x)$$

over F.

Now we can describe K as a succession of Galois extensions as follows. First, E is the splitting field of h. Next, K_0 is the splitting field of $x^n - 1$ over E. Then, writing $G = (g_1, \ldots, g_m)$, define K_i as the splitting field of $(x^n - g_i \cdot e)$ over K_{i-1}. We can regard E and all K_i's as subfields of K, and we have

$$F \subset E \subset K_0 \subset \cdots \subset K_m = K.$$

The Galois group of E/F is solvable and those of K_0/E and K_{i+1}/K_i are abelian. Thus K/F is solvable. ∎

Corollary 0.4 *If an irreducible polynomial $f(x)$ is solvable by radicals, then its Galois group is also solvable.*

Proof. Let $F \subset E_1 \subset \cdots \subset E_n$ be a chain of radical extensions such that $f(x)$ has a root in E_n. Applying the Theorem above inductively, we find each E_i is contained in a solvable extension K_i/F. Thus $f(x)$ has a root in a solvable extension K/F. Since f is irreducible, its splitting field L is a subfield of K, and hence L/F is also solvable. ∎

This completes the proof of Theorem 0.2 in one direction. The other direction is more straightforward, since it amounts to showing that a cyclic extension is a radical extension.

Corollary 0.5 *A quintic with Galois group S_5 or A_5 is not solvable by radicals.*

Proof. If it were, then S_5 or A_5 would be a solvable group. ∎