GALOIS THEORY.

Paul Taylor.
Trinity College
September 1983.

1. Field Extensions

The most notable elementary fact about fields is that every homomorphism is a monomorphism (injective map). The second observation is that, given two fields $K \subseteq L$, the larger is a vector space over the smaller.

A field extension, $L:K$, is simply a pair of fields, one included in the other. We may wish to say this formally, ie it is a triple (i, K, L) where $i: K \hookrightarrow L$. One usually thinks of K as the "ground field" and L as something constructed on top of it. The degree of the extension, written $[L:K]$ is the dimension of L considered as a vector space over K. For our purposes, $[L:K] = \infty$ is quite bad enough without considering infinite cardinals.

Given an extension $L:K$, an element $\alpha \in L$ is algebraic if there's a nontrivial polynomial

$$p(t) = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_0$$

with coefficients in K such that $p(\alpha) = 0$ in L. If $[L:K] < \infty$, every element is algebraic since the powers cannot be linearly independent. An extension in which every element is algebraic is called an algebraic extension. An element which is not algebraic is called transcendental. An algebraic extension need not be finite: consider $A:\mathbb{Q}$ where $A \subseteq \mathbb{C}$ consists of the algebraic numbers (exercise: show such a thing to be a field.)

We may consider a tower $M:L:K$ of fields. In this case one may verify by elementary but tedious linear algebra that $[M:K] = [M:L][L:K]$, remembering also to check the infinite cases. [Stewart pp. 50-52 or exercise]

A simple extension $L:K$ is one for which there is an element $\alpha \in L$ which generates L as a field over K, so L is the smallest subfield of L containing both K and α. We write $L = K(\alpha)$. If α is transcendental we have a simple transcendental extension and L consists of the rational functions in α over K, ie formal quotients of polynomials: $f(\alpha)/g(\alpha)$ with $g \neq 0$.

Given a nontrivial irreducible polynomial f over K we may construct a field extension $L:K$ for which f has a root in L. This is the quotient $K[t]/\langle f(t)\rangle$ which is a field since f is prime in $K[t]$ (which is a PID). See Stewart p.40. [<u>exercise</u>]

Transcendental extensions are relevant in Algebraic Geometry but not in this course. If $L:K$ is a (transcendental) extension, the <u>transcendence degree</u>, $\text{tr.deg.}(L:K)$, is the smallest cardinality of a set $X \subset L$ such that $L : K(X)$ is algebraic. We have $\text{tr.deg.}(M:K) = \text{tr.deg.}(M:L) + \text{tr.deg.}(L:K)$. [<u>exercise</u>] In particular if $M:L$ and $L:K$ are algebraic so is $M:K$.

2. <u>Polynomials and Splitting Fields</u>.

A polynomial over a given field is said to <u>split</u> if it can be expressed as a product of linear factors. It's clear that if it does split, it must do so essentially uniquely (ie up to order and scalar factors) [<u>exercise</u>]. A <u>splitting field</u> for a polynomial f over K is an extension $L:K$ such that f splits over L and not over any smaller field which also contains K. We aim to show that splitting fields exist and are unique.

First consider again adjoining one root, α, of an irreducible polynomial f to a field K. If we have a diagram

$$\begin{tikzcd} K(\alpha) \arrow[r, dashed, "j"] & L \\ K \arrow[u] \arrow[r, "\cong"'] & K' \arrow[u] \end{tikzcd}$$

where f has a root, β, in L, then there is a unique map $j : K(\alpha) \to L$ making the square commute (ie we embed $K(\alpha)$ in L in such a way as to identify K with K') such that $j : \alpha \mapsto \beta$. For the proof [<u>exercise</u>] observe that the elements of $K(\alpha)$ may be written uniquely as $a_{n-1}\alpha^{n-1} + \ldots + a_0$ with $a_i \in K$ and $n = \deg f$. The same argument also applies to transcendental extensions. By applying the lemma the other way round we see that $K(\alpha)$ is unique up to isomorphism.

Now a straightforward induction argument shows that we may construct a finite extension to split any polynomial, and by choosing the minimal subextension (ie subfield containing K) in which the polynomial does split we have a splitting field. Thus we require now to show it's unique.

Suppose we have a diagram

$$\begin{tikzcd} L \arrow[r, dashed, "j"'] & L' \\ K \arrow[u, hook] \arrow[r, phantom, "\cong"] & K' \arrow[u, hook] \end{tikzcd}$$

and a polynomial f (not necessarily irreducible) over K which splits in L and L' (nb in $L':K'$ we consider it to have coefficients $i(a_r)$ where $i:K \cong K'$ and a_r are the coefficients of f in K), such that $L:K$ is a splitting field for f. Put $K_0 = K$ and, given K_i, consider the factorisation of f into irreducibles over K_i (which is unique up to order and scalar factors : <u>exercise</u> from IB Rings & Modules); choose such a factor of degree $\geqslant 2$ and let K_{i+1} be an extension by a root α_i of it. Then $L = K_n$ for some n, so $L = K(\alpha_0, \dots, \alpha_{n-1})$ where α_i are the roots of f in L.

Now perform the corresponding construction in $L':K'$. Given $j_i : K_i \to K'_i$ choose a root $\beta_i \in L'$ of the corresponding factor under j_i and put $K'_{i+1} = K'_i(\beta_i) \subseteq L'$. The map j_i then extends uniquely to one for which $\alpha_i \mapsto \beta_i$ (although it does depend on the choice of β_i) and $j = j_n$ is the required map $j : L \to L'$. Thus the uniqueness (up to isomorphism) of the splitting field follows.

It is actually true that a finite separable extension is simple, ie $L = K(\alpha)$ for some (single) $\alpha \in L$. This is the <u>theorem of the primitive element</u> [see later].

3. <u>Separability</u>

Separability is a concept about which one only needs to know when dealing with infinite fields of nonzero characteristic. It is essentially the condition that there is the full complement of "independent" roots of a polynomial and hence of permutations of them so that the Galois group can "resolve" subfields as it should.

Given that one knows what it means for a root to be repeated, an irreducible polynomial is <u>separable</u> if its roots in a splitting field are distinct. A general polynomial is separable if all its irreducible factors are; an element is separable if its minimal polynomial is and an extension is separable if all its elements are.

We shall shortly find a simple criterion for separability and hence show that it's automatic in characteristic zero (and also for finite fields), but we need an example of an inseparable polyn. Let $K = \mathbb{F}_p(t)$, a simple transcendental extension of a finite field (of p elements, where p is prime). Then the polynomial $x^p - t$ is irreducible and inseparable since all its p roots coincide; see Stewart, pp. 93-94.

For polynomial functions $f: \mathbb{R} \to \mathbb{R}$ we know that f has a double zero at α iff $f(\alpha) = f'(\alpha) = 0$. Whilst we have no hope of extending the notion of "rate of change" to a general field, we may nevertheless define the derivative formally for polynomials using $D(x^n) = n x^{n-1}$. [Whilst for this purpose this is merely a trick, the notion of a <u>derivation</u> - an algebraic operation satisfying conditions similar to those satisfied by d/dx - is important in extensions of Galois theory, being the beginning of <u>Galois cohomology</u>]. An irreducible polynomial f is then separable iff f, Df have no common factor in a splitting field.

Let $L:K$ be a splitting field for the irreducible polynomial f over K and suppose $\alpha \in L$ were a common root of f and Df. Now f is the minimal polynomial for α over K so α satisfies no nontrivial polynomial of lower degree. Thus $Df = 0$. Now in characteristic zero, $\deg Df = \deg(f) - 1$, so how can Df manage to vanish? Only by the vanishing of its coefficients, which means that the degree of any term of f with a nonzero coefficient must be a multiple of p. Thus f must actually be a polynomial in x^p.

Now this is not possible in a finite field. For observe that $x \mapsto x^p$ is a field homomorphism [<u>exercise</u>] and so in the finite case it's an automorphism [it's called the <u>Fröbenius map</u>]; thus every element of a finite field of characteristic p is automatically a p^{th} power. Hence if f is irreducible and separable it's of the form

$$a_k{}^p x^{kp} + a_{(k-1)}{}^p x^{(k-1)p} + \ldots + a_1{}^p x^p + a_0{}^p$$

but this is equal to $(a_k x^k + \ldots + a_0)^p$ and so f is not irreducible.

A field every finite extension of which is separable is called <u>perfect</u>. Thus if $|K| < \infty$ or $\operatorname{char} K = 0$ then K is perfect.

4. Algebraic closures.

A field is said to be algebraically closed if every nonzero polynomial over it has a root in it, ie there are no nontrivial irreducible polynomials. L:K is an algebraic closure (of K) if L is algebraically closed but no intermediate field (ie M st. L:M:K) is; alternatively, L is algebraic over K.

Given the Axiom of Choice, every field has an algebraic closure, which is unique up to isomorphism. The proof is, however, technical, but not for any reason concerned with field theory.

First recall that if M:L and L:K are algebraic, so is M:K, that is, a root of a polynomial equation with algebraic coefficients is itself algebraic. Hence in constructing an algebraic closure we need only consider roots of polynomials over the ground field and not over any extension. This provides us with an (infinite) cardinal which bounds the size of any algebraic extension and hence of an algebraic closure. We also know how to perform the finite steps of adjoining missing roots and we have just shown that we need not carry on doing so "for ever". Thus we have shown all that is essentially required.

Unfortunately, putting all this data into a form suitable for an application of Zorn's lemma is quite complicated (and unenlightening). The trick is to take a set of suitable size and consider all possible ways of putting a field structure onto subsets of it (this is still only a set, not a proper class, since we may easily prescribe a bound for it) and all field monomorphisms between these fields. In other words we take the (small) category of fields which are algebraic extensions of the given field and have underlying sets within the given set. With a certain amount of "bit-picking" one can show how to construct finite extensions within this (in other words you perform the finite extension in the usual way and then re-name the elements as elements of the set) and that we have unions of chains of fields (called "filtered colimits" in category theory), whence (since we're working inside a set, not a proper class) Zorn's lemma applies and we have a maximal algebraic extension, which must be algebraically closed.

Uniqueness is more interesting; again it requires choice. We have a diagram

$$\begin{tikzcd}
L \arrow[r, dashed, "?"] & L' \\
K \arrow[u] \arrow[r, phantom, "\cong"] & K' \arrow[u]
\end{tikzcd}$$

where $L:K$ and $L':K'$ are algebraically closed and L is the algebraic closure of K. This time we can apply Zorn's lemma more directly. Consider all intermediate fields $L:M:K$ and maps $m: M \to L'$ extending the isomorphism. We order these so that $(M_1, m_1) \leq (M_2, m_2)$ iff $K \subseteq M_1 \subseteq M_2 \subseteq L$ and $m_2|_{M_1} = m_1$. Again we have a partially ordered set which has unions of chains (this is easy to check, <u>exercise</u>, because of the finitary nature of the field operations) and hence a maximal element which we claim to be (L, j).

For suppose (M, m) is maximal but $M \subset L$. Then there is some irreducible polynomial f over M which has a root α in M' where $M \subset M' \subseteq L$. Choosing a root β in L' for the corresponding polynomial $m(f)$ in L' we may extend m to $m_1 : M_1 \to L'$ with $(M_1, m_1) > (M, m)$ contradicting the maximality of (M, m).

In the case of a finite field we may actually construct the algebraic closure explicitly. Likewise, the algebraic closure of any subfield of $\mathbb{C}$ (such as $\mathbb{Q}$) may be found inside $\mathbb{C}$ since that is algebraically closed.

5. Normal extensions

A <u>normal</u> extension is one which may be expressed as the splitting field of a set of polynomials. Equivalently, every polynomial which is irreducible over the ground field but has a root in the extension splits in the extension.

Given an extension satisfying the latter condition, consider the set of minimal polynomials of elements of the extension field; by hypothesis these split in the extension (being irreducible) and there is clearly no intermediate field in which they all split.

Conversely given the splitting field extension $L:K$ of a set of polynomials and another irreducible polynomial f over K with a root α in L, we may restrict our attention to the splitting field L' of some finite subset of the given set of polynomials. Thus without loss of generality (by choosing suitable intermediate fields $K \subseteq K' \subseteq L' \subseteq L$) $L:K$ is the splitting field of a single irreducible polynomial g over K and hence finite.

Now let $M:K$ be a splitting field for fg and consider the following diagram of subfields of M:

$$\begin{tikzcd}
 & M & \\
L(\alpha) \arrow[ur, hook] \arrow[dr, phantom, "\cong" sloped] & & L(\beta) \arrow[ul, hook'] \\
 & L \arrow[ur, hook] & \\
K(\alpha) \arrow[uu, hook] \arrow[ur, hook] & & K(\beta) \arrow[uu, hook'] \\
 & K \arrow[ul, hook'] \arrow[ur, hook] &
\end{tikzcd}$$

Now $K(\alpha):K$ and $K(\beta):K$, where β is another root of f in M, are isomorphic as abstract field extensions, as are $L(\alpha):K(\alpha)$ and $L(\beta):K(\beta)$. Hence considering degrees (which are all finite so we can perform division)

$$\begin{aligned}
[L(\beta):L][L:K] = [L(\beta):K] &= [L(\beta):K(\beta)][K(\beta):K] \\
&= [L(\alpha):K(\alpha)][K(\alpha):K] && \text{by above} \\
&= [L:K(\alpha)][K(\alpha):K] && \text{since } \alpha \in L \\
&= [L:K]
\end{aligned}$$

Hence $[L(\beta):L] = 1$, ie $L(\beta) = L$, so $\beta \in L$.

This means that all of the roots of f in M lie in L. But we assumed that f splits into linear factors in M, these being of the form $(x-\beta)$ for β a root. Now these linear factors may be found over L so f splits over L. Hence $L:K$ is normal.

If $L:K$ is normal and M is an intermediate field then $L:M$ is also normal although there is no reason why $M:K$ should be. Also, it is not true that $L:M$, $M:K$ normal $\Rightarrow$ $L:K$ normal; consider $K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt[3]{2}, \omega)$, $L = \mathbb{Q}(\sqrt{2}, \omega)$ where ω is a complex cube root of unity. [exercises]

The idea behind normality is this. We already know that extensions by a root of an irreducible polynomial are isomorphic, so in some sense the roots are "indistinguishable". We shall see later that there are in fact automorphisms taking any root to any other, so in order to get the full complement of automorphisms we need all of the roots, which is exactly what normality says.

Given any extension we may always embed it in a normal extension. The algebraic closure of the larger field, for instance, provides such an extension, but in the finite case we may easily construct a suitable extension without using the Axiom of Choice. A minimal normal extension including a given one is called a **normal closure**.

6. The Galois Group.

During the eighteenth century, when it was first realised that the general quintic equation probably could not be solved by radicals (we shall prove this later), it became apparent that the relevant things to consider were permutations of the roots of a polynomial, and also expressions involving the roots which had rational values [Stewart pp. xiii - xv].

The methods which were known by the middle of the sixteenth century for solving (quadratics,) cubics and quartics involved (essentially) expressions in the roots which, whilst not rational, satisfied polynomial equations of lower degree. For the cubic, if the roots are α, β, γ and ω is a complex cube root of unity, α, β, γ may easily be found given $\alpha+\beta+\gamma$, $\alpha+\omega\beta+\omega^2\gamma$ and $\alpha+\omega^2\beta+\omega\gamma$, of which the first is already a coefficient of the polynomial. The cubes of the other two are then roots of a quadratic equation whose coefficients are rational functions of those of the cubic. We shall deal with the quartic later.

In modern terminology permutations of roots are replaced by field automorphisms (fixing the ground field) and expressions in the roots are replaced by intermediate fields. The fundamental theorem relates subgroups of the group of permutations to intermediate fields.

Thus if $L:K$ is a field extension (which we shall henceforward assume to be finite), the **Galois group**, $\Gamma(L:K)$, consists of the field automorphisms of L such that the elements of K remain fixed. The composition is of course the composition of maps and the identity and inverses are the obvious things.

Now if $L:K$ is generated by some of the roots of a polynomial f over K, it's clear that elements of $\Gamma(L:K)$ must permute these roots since f is fixed. Conversely, the permutation of the roots determines the automorphism uniquely. Finally, if $L:K$ is a splitting field extension for an irreducible polynomial, the Galois group acts transitively on the roots [**exercise**]

Now we set up the relationship between subgroups and intermediate fields. Notice first that these two form lattices. Considering subgroups and intermediate fields simply as subsets, there is an intersection (or meet) operation defined on them. Whilst the set-wise union of subgroups or subfields need not be a subgroup or subfield, we may nevertheless form the subgroup or subfield generated by the union and call this the join of them.

Now write $\mathcal{F}$ for the lattice of intermediate fields, ordered by inclusion, and similarly $\mathcal{G}$ for the subgroups. Given an intermediate field $M \in \mathcal{F}$ (so $L:M:K$) there is a subgroup $\Gamma(L:M)$ of $\Gamma(L:K)$ of automorphisms fixing the elements of M; this we shall call M^*. Conversely, given a subgroup H of $\Gamma(L:K)$ we may consider its set of fixed points, which may easily be verified to form an intermediate field, $H^\dagger$.

Thus we have two operations $*: \mathcal{F} \to \mathcal{G}$ and $^\dagger: \mathcal{G} \to \mathcal{F}$ and they are easily seen to be order-reversing [exercise]. Moreover for $H \in \mathcal{G}$ and $M \in \mathcal{F}$ we have $M \le H^\dagger$ iff $H \le M^*$; equivalently, $M \le M^{*\dagger}$ and $H \le H^{\dagger *}$. In general a pair of maps $(*, \dagger)$ between lattices with this property is called a Galois correspondence (since this was the first example to be found) and is a special case of a pair of adjoint functors between categories.

The fundamental theorem of Galois theory gives necessary and sufficient conditions for these maps to be bijective and hence the lattices of subgroups and intermediate fields to be (dually) equivalent. We may then exploit our knowledge of group theory to investigate the structure of fields.

7. Galois extensions

The Galois correspondence is not always a bijection, and the first place we might check for failure is at the ground field itself. An extension $L:K$ is said to be a Galois extension if $\Gamma(L:K)^\dagger = K$. We shall show that for a finite Galois extension the Galois correspondence is bijective, and also that a finite extension is Galois iff it is normal and separable.

We need a lemma due to Dedekind. Given fields K, L, every set of distinct monomorphisms $K \to L$ is linearly independent over L. For otherwise there is an expression $a_1\sigma_1(x) + a_2\sigma_2(x) + \ldots + a_n\sigma_n(x) = 0$ with $a_i \in L$ and $\sigma_i : K \to L$ distinct, for which n is least. We choose $y \in K$ for which $\sigma_1(y) \neq \sigma_n(y)$ and construct a relation $b_2\sigma_2(x) + b_3\sigma_3(x) + \ldots + b_n\sigma_n(x) = 0$ where $b_i = a_i(\sigma_1(y) - \sigma_n(y))$ which is nontrivial since $b_n \neq 0$ and which is shorter than the supposed minimal one.

Now using this, by a similar argument [Stewart pp 101-3; <u>exercise</u>] we may show that if $L:K$ is a finite Galois extension then $[L:K] = |\Gamma(L:K)|$. That $[L:K] \geqslant |\Gamma(L:K)|$ follows immediately from the lemma and elementary linear algebra; the other inequality uses another minimality argument. It now also follows that for any finite extension $L:K$ and subgroup $H \leq \Gamma(L:K)$ we have $[H^{\dagger}:K] = [L:K]/|H|$.

Recall that $M \leq H^{\dagger}$ iff $H \leq M^{*}$ where $L:M:K$ and $H \leq \Gamma(L:K)$, $L:K$ being any (finite) extension. From this and the order-reversing properties of $*$ and $\dagger$ it follows easily that $H \leq H^{\dagger *}$, $M \leq M^{*\dagger}$, $H^{\dagger} = H^{\dagger * \dagger}$ and $M^{*} = M^{*\dagger *}$. Thus we have

$$|H| = [L:K]/[H^{\dagger}:K] = [L:K]/[H^{\dagger*\dagger}:K] = |H^{\dagger *}|$$

so $H \leq H^{\dagger *}$ are finite groups of the same order and are hence equal.

We have thus shown that for finite extensions the composite of the Galois maps one way round is always the identity, ie $H = H^{\dagger *}$.

The results of this course may be extended (with occasional Choice) to general algebraic extensions. In this case the preceding result breaks down, but the Galois group may be given a topology (called the <u>Krull topology</u>) rendering it a compact Hausdorff totally-disconnected topological group (a <u>profinite group</u>) in which the closed subgroups are exactly those of the form M^{*} for M an intermediate field. The operation $H \mapsto H^{\dagger *}$ is then the topological closure and the results of finite Galois theory go through with "subgroup" replaced by "closed subgroup".

8. The Fundamental Theorem

We have still to show that a finite extension is Galois iff it is normal and separable, and that for a Galois extension $M = M^{*\dagger}$ for all intermediate fields M.

We shall do this by again counting automorphisms.

We must look again at normality and separability. First we show the same result about normal closures as we did about extensions by a single root, splitting fields and algebraic closures. Thus given a diagram

$$\begin{tikzcd}
N \arrow[rr, dashed] & & M \\
L \arrow[u] \arrow[urr] & & \\
K \arrow[u] & \cong & K' \arrow[uu]
\end{tikzcd}$$

in which $M:K'$ is normal and $N:K$ is the normal closure of $L:K$ there is a map (not unique) extending the given one. The proof [exercise] is much the same as before. Uniqueness of normal closures follows.

Similarly if $L:K$ is finite normal and α, β are roots of the same irreducible polynomial, there's an element of the Galois group sending one to the other (ie it's transitive).

Under automorphisms of a large extension, $M:K$, any normal extension $N:K$ is stabilised (ie $\sigma(N) = N$ for $\sigma \in \Gamma(M:K)$). In fact the normal closure of an extension $L:K$ is essentially its orbit under automorphisms of larger extensions.

We aim to show that $|\Gamma(L:K)| \leq [L:K]$ with equality iff $L:K$ is normal and separable. It is then an easy corollary of the previous section that this happens (in the finite case) iff $L:K$ is Galois (ie $\Gamma(L:K)^{\dagger} = K$). Finally if these conditions hold and M is an intermediate field (so $L:M$ is also finite, normal and separable) then by the same argument [exercise] $M^{*\dagger} = M$, completing (the first part of) the fundamental theorem.

Let $L:K$ be finite and separable and let $N:K$ be a normal extension containing it. Then there are precisely $n = [L:K]$ distinct monomorphisms $L \rightarrow N$ fixing K. We already know the result for $L:K$ simple (ie $L = K(\alpha)$), so it's a corollary of the theorem of the primitive element, but we can argue inductively on n. Choose $\alpha \in L \setminus K$ so its minimal polynomial splits into distinct linear factors in N. One may now show [exercise; Stewart pp 109-110] that the maps $L \rightarrow N$ fixing K are then the composites of the $[K(\alpha):K]$ maps $K(\alpha) \rightarrow N$ with the $[L:K(\alpha)]$ (by induction) maps $L \rightarrow N$ fixing $K(\alpha)$.

Clearly if $L:K$ is inseparable the roots of the minimal polynomial of α will not be distinct, and if L:K is not normal some of the maps will take elements of L outside L.

9. Group-theoretical properties of $\Gamma(L:K)$

We are now in a position to find out why normality is important in Galois' theorem, by studying the Galois groups of finite separable extensions in relation to those of their normal closures. Separability we shall not study further: an account is in Cohn, Algebra II §6.4. As one might have guessed, the term "normal" was applied to field extensions as a result of the relationship with normal subgroups; conversely "soluble" groups were so called because of a later theorem.

First we need the easy lemma [exercise; Stewart p.116] that for L:K any extension with intermediate field M and $\tau \in \Gamma(L:K)$ we have $(M^\tau)^* = \tau^{-1}M^*\tau \leq \Gamma(L:K)$. The second part of Galois' theorem now follows [exercise]:

For L:K finite normal and separable and M an intermediate field, M:K is normal iff $M^* \trianglelefteq \Gamma(L:K)$. Moreover $\Gamma(M:K) \cong \Gamma(L:K)/\Gamma(L:M)$ where the natural quotient map is $\varphi: \Gamma(L:K) \to \Gamma(M:K)$ by $\tau \mapsto \tau|_M$.

It is this functorial relationship between groups and field extensions which provides the real power of Galois theory.

Now let's drop the condition of normality on L:K and see why in terms of group theory the theorem fails. Take N:K a normal closure and $G = \Gamma(N:K)$ its Galois group. Recall that the crucial question is whether $K_0 \equiv \Gamma(L:K)^\dagger = K$ where ($\dagger$) is the relevant Galois map for the extension L:K. Put $H = \Gamma(N:L) \leq G$ and $G_0 = \Gamma(N:K_0) \leq G$ (this is where we run out of sensible letters!).

Now $K \subseteq K_0 \subseteq L$ so $G \supseteq G_0 \supseteq H$. Moreover $L:K_0$ is Galois by construction and hence normal, as is the larger extension $N:K_0$, so by the second part of the fundamental theorem $H \trianglelefteq G_0$. Conversely, let $H \trianglelefteq E \leq G$ and let $K \subseteq F \subseteq L$ be the fixed field (in the extension N:K), so L:F is normal and hence Galois whence $K_0 \subseteq F$ and so $G_0 \supseteq E$. Thus G_0 is the largest subgroup of G which contains H as a normal subgroup of it, ie $G_0 = N_G(H)$, the <u>normaliser</u> of H in G. Clearly $K = K_0 \Leftrightarrow G = G_0 = N_G(H) \Leftrightarrow H \trianglelefteq G \Leftrightarrow$ L:K is normal.

How do we say in the language of group

theory that $N:K$ is the normal closure of $L:K$? Well if $M:K$ were normal with $L \subseteq M \subseteq N$ then $\Gamma(N:M)$ would be a normal subgroup of $\Gamma(N:K)$ containing $\Gamma(N:L)$, and conversely. Thus $\Gamma(N:L)$ contains no normal subgroups of $\Gamma(N:K)$. Given any normal extension $N':K$ containing $L:K$, N^* is the intersection of the conjugates of $\Gamma(N':L)$ in $\Gamma(N':K)$, corresponding to the fact that $N:K$ is generated by the "conjugates" of $L:K$.

10. Finite Fields

We are now in a position to classify finite fields and their Galois groups. The additive group of a finite field is what the group theorists call an elementary Abelian p-group, the multiplicative group is cyclic and so is the Galois group of any extension between finite fields; however finite fields amply repay to group theory its contribution to Galois theory since their matrix groups (in particular the analogues of the special linear group, the orthogonal group and the symplectic group) provide a substantial proportion of the finite simple groups.

We have already made most of the relevant observations towards the classification of finite fields. The characteristic (the smallest number of times one has to add unity to itself to get zero) must be a prime (exercise) and so we have the prime subfield of order p (we also say that $\mathbb{Q}$ is the prime subfield of any field of characteristic zero). Any finite field is a vector space (say of dimension n) over its prime subfield and hence has order p^n. There is exactly one field of each possible order, called $GF(p^n)$ or $\mathbb{F}_{p^n}$. Put $q=p^n$.

Recall that the map $\varphi : x \mapsto x^p$ is an automorphism of finite fields and so, if we think of a finite field as a finite separable (and indeed normal) extension $K:P$ of its prime subfield, $\varphi \in \Gamma(K:P)$. In fact $\Gamma(K:P)$ is cyclic with generator φ.

By elementary group theory applied to the multiplicative group K^*, every element $x \in K$ satisfies $x^q - x = 0$, and so this polynomial splits in K (since it can only have q distinct roots) and K is clearly the splitting field for it. In particular P is the splitting field for $x^p - x = 0$ so $\langle\varphi\rangle^\dagger = P$. $K:P$ is then normal and $\Gamma(K:P)$ is cyclic and generated by φ [exercise].

By the theory of splitting fields we have proved the uniqueness of the field of order p^n. Its existence is now an easy exercise.

The one remaining result for us is that the multiplicative group of a finite field is cyclic, as is any finite subgroup of the multiplicative group of any field. The exponent of a finite group G is the smallest positive number e such that $g^e = 1$ for all $g \in G$; in a finite Abelian group there is always an element whose order is the exponent [exercise; also a counterexample for a non Abelian group], so if $e(G) = |G|$ the Abelian group is then cyclic.

Given a finite group $G \leq K^*$ of the multiplicative group of a field let $n = |G|$ be its order and $e = e(G)$ its exponent. Then $x^e = 1$ for $x \in G \leq K$, but this is a polynomial equation with at most e roots, so $e \geq n$, but clearly $e | n$ so $e = n$. Thus G is cyclic, being Abelian.

11. Criteria for irreducibility; cyclotomic polynomial.

We shall now turn to some "practical" Galois theory. We have frequently mentioned irreducible polynomials but we've given no means of determining whether a given polynomial is in fact irreducible. The first lemma is due to Gauss (with $R = \mathbb{Z}$ and $K = \mathbb{Q}$): let R be a unique factorisation domain and K its field of fractions; then any polynomial over R which is irreducible over R is also irreducible over K [exercise]

The second lemma is called Eisenstein's criterion. Given a polynomial $f(x) = a_n x^n + \ldots + a_1 x + a_0$ (over a UFD R) whose coefficients have no common factor (ie they generate R as an ideal), and a prime p in R, suppose $p \nmid a_n$ but $p | a_r$ $(0 \leq r \leq n-1)$ and $p^2 \nmid a_0$. Then f is irreducible over R. [exercise]

Finally we have what is essentially a piece of first order logic and it only works over $\mathbb{Z}$. Let p be a prime and $f = a_n x^n + \ldots + a_0$ a polynomial over $\mathbb{Z}$ with $p \nmid a_n$. Let $\bar{f}$ be the corresponding polynomial over $\mathbb{Z}_p$ under the quotient map $\mathbb{Z} \to \mathbb{Z}_p$, whose coefficients $\bar{a}_r$ are (a_r mod p). Then if $\bar{f}$ is irreducible over $\mathbb{Z}_p$, so is f over $\mathbb{Z}$ (but not conversely). [easy exercise]

Many Tripos questions are based on these three lemmas. It is of particular relevance to us that $f(x) = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1$ is irreducible over $\mathbb{Z}$ (and hence $\mathbb{Q}$) for p prime: apply Eisenstein to $f(x+1)$. This is the cyclotomic polynomial of order p. Its roots in $\mathbb{C}$ are the complex p^{th} roots of unity.

More generally we define $\Phi_n(x) = \Pi(x-\eta)$ where η runs over the primitive n^{th} roots of unity, ie those for which no r^{th} power with $0<r<n$ is unity. They are of the form ε^m with $(n,m)=1$ and $\varepsilon = \exp 2\pi i/n$, and there are $\varphi(n)$ of them, where $\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}) = p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\dots p_r^{\alpha_r}(p_r-1)$. Notice that $x^n-1 = \Pi_{d|n}\Phi_d(x)$. A straightforward application of Galois theory to $\mathbb{Q}(\varepsilon):\mathbb{Q}$ [exercise] shows that the coefficients are rational and since any irreducible factor of $\Phi_n(x)$ is also one of x^n-1, Gauss' lemma shows that the coefficients are in fact integers. We aim to show that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ (or $\mathbb{Z}$).

Consider first $n=p^k$ and put $\Phi_{p^k}(x+1) = x^{p^k-p^{k-1}}+g_k(x)$. Now $\Phi_{p^k}(x) = (x^{p^k}-1)/(x^{p^{k-1}}-1)$ so put $\Sigma_{0\le r<p^k}(x+1)^r = x^{p^k-1}+ph_k(x)$: we may see by an application of the binomial theorem that $h_k(x)$ has integral coefficients, since p divides the numerators but not the denominators of all of the relevant coefficients. Now we simply multiply out the equation

$$(x^{p^{k-1}-1}+ph_{k-1}(x))(x^{p^k-p^{k-1}}+g_k(x)) = (x^{p^k-1}+ph_k(x))$$

to see that the coefficients of $g_k(x)$ must be divisible by p. As to the constant coefficient, this is $\Phi_{p^k}(1) = (\Sigma_{0\le r<p^k}1^r)/(\Sigma_{0\le r<p^{k-1}}1^r) = p^k/p^{k-1} = p$. Eisenstein's criterion is then applicable with prime p.

Before we turn to the general case, consider what this says about the extension $\mathbb{Q}(\varepsilon):\mathbb{Q}$ (which splits $x^{p^k}-1$), namely it has degree $\varphi(p^k) = p^k-p^{k-1}$. It is clearly finite, normal and separable, so the Galois group $G = \Gamma(\mathbb{Q}(\varepsilon):\mathbb{Q})$ has order $\varphi(p^k)$. However its elements are determined by their action on ε, which can only be $\varepsilon\mapsto\varepsilon^m$ for some m with $(n,m)=1$. There are only $\varphi(n)$ such maps, so they must all be there. Moreover they form an Abelian group, U_n, the group of units modulo $p^k=n$.

For general n, G must still be an (Abelian) subgroup of U_n, and we must show that it is the whole of it, so $[\mathbb{Q}(\varepsilon):\mathbb{Q}] = |G| = |U_n| = \varphi(n) = \deg\Phi_n$, whence it follows that Φ_n is irreducible [exercise: why?]. Now each $m\in U_n$ (ie $m\in\mathbb{Z}$ with $(n,m)=1$) may be expressed modulo n as a product $m_1\dots m_r$ with $p_i^{\alpha_i}|(m_j-1)$ for $i\ne j$ [exercise: the Chinese Remainder theorem] and so (essentially) as a composite of automorphisms of $\mathbb{Q}(\varepsilon):\mathbb{Q}$ each of which, when restricted to the subextensions $\mathbb{Q}(\varepsilon_i):\mathbb{Q}$, moves only one of them.

Thus $[\mathbb{Q}(\varepsilon):\mathbb{Q}] = |\Gamma(\mathbb{Q}(\varepsilon):\mathbb{Q})| = \prod|\Gamma(\mathbb{Q}(\varepsilon_i):\mathbb{Q})| = \prod\varphi(p_i^{\alpha_i}) = \varphi(n)$. In fact $\Gamma(\mathbb{Q}(\varepsilon):\mathbb{Q}) \cong U_n \cong \bigoplus_i U_{p_i^{\alpha_i}}$. [<u>Exercise</u>: where in the proof did we need that U_n was Abelian?] It now follows as before that $\Phi_n(x)$ is irreducible and its Galois group is Abelian.

12. <u>Extraction of roots</u>.

Now that we have determined the nature of the extension $\mathbb{Q}(\varepsilon):\mathbb{Q}$, where ε is a (primitive n^{th}) root of unity, we may proceed to the splitting field of $x^n - a$ where a is any rational number. In fact our retreat to $\mathbb{Q}$ is really rather cowardly: we may deal with any field of characteristic either zero or a sufficiently large prime ($>n$ will do), but we may as well assume $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$.

The first thing to do when we come across an equation such as $x^n - a$ is to adjoin a primitive n^{th} root of unity. This is an extension of degree dividing $\varphi(n)$ with Abelian Galois group, as we have seen ("dividing" since it may already be there). Thus wlog $x^n - 1$ splits in K. Now let α be an n^{th} root of a in some extension (we may as well think of α as real and positive if possible); then $K(\alpha):K$ has degree dividing n.

Now taking the prime factorisation of n, we may construct α and $K(\alpha)$ as a result of a sequence of extractions of p^{th} roots with p prime. Since at every stage the relevant polynomials split (in the presence of a primitive n^{th} - and hence p^{th} - root of unity, $x^p - a = (x-\alpha)(x-\varepsilon\alpha)\dots(x-\varepsilon^{p-1}\alpha)$), we have normal extensions, and finiteness and separability are automatic. Thus the Galois groups of these extensions will be of order p and hence cyclic.

To sum up, we construct the splitting field of $x^n - a$ over a field possibly lacking in roots of unity by adjoining roots of unity and successive p^{th} roots. At every stage we have a normal extension with Abelian Galois group over the previous stage. The result is the splitting field of $(x^n - 1)(x^n - a)$ and is hence normal but (possibly) too big so we take a (normal) subextension.

Now consider the Galois groups of the extensions between the splitting field of $(x^n - 1)(x^n - a)$ and each stage in the construction. These form a decreasing sequence of groups, each of which is normal in the previous one with Abelian quotient. A group with such a sequence is said to be *soluble*. It's easy to see that an extension formed by adjoining roots of unity and n^{th} roots of elements of (possibly intermediate) fields is going to have a soluble Galois group as well.

Formally, we define a *radical extension* $L:K$ as a finite normal (and, restricting to characteristic zero, separable) subextension of one of the form $K(\alpha_1,\ldots,\alpha_n):K$ where $\alpha_r^{p_r} \in K(\alpha_1,\ldots,\alpha_{r-1})$ for some primes $p_1,\ldots,p_r$ and $K(\alpha_1,\ldots,\alpha_{r-1})$ has p_r^{th} roots of unity. A radical extension need not necessarily itself be of the form $K(\alpha_1,\ldots,\alpha_n):K$ for such $\alpha_1,\ldots,\alpha_n$. An extension which is of that form clearly has a soluble Galois group; the Galois group of a normal subextension is a quotient of it and hence also easily seen to be soluble.

Notice that in the case of splitting $x^n - a$ alone, the intermediate groups in the sequence were normal not only in their predecessors but also in the whole group. This is *not* necessary for a group to be called soluble: it in fact defines a stronger condition called *nilpotency*. Two major theorems in the Part II Group theory course are that a group of order $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ is nilpotent iff it's a direct product of groups of orders $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_r^{\alpha_r}$ and soluble iff it has subgroups of orders $n/p_1^{\alpha_1}, n/p_2^{\alpha_2}, \ldots, n/p_r^{\alpha_r}$. Every group of that order has subgroups of orders $p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}$.

13. *Solutions of equations by radicals*.

In the previous section we showed that a radical extension has soluble Galois group. We shall now show the converse, for which we need a lemma usually called *Hilbert's Theorem 90*.

Let $L:K$ be Galois with cyclic Galois group of order n generated by τ. Then $\alpha \in L$ satisfies $\alpha\alpha^{\tau}\alpha^{\tau^2}\ldots\alpha^{\tau^{n-1}} = 1$ iff its of the form δ/δ^{τ} for some $\delta \in L \setminus \{0\}$. Sufficiency is a trivial *exercise*. Conversely, let $\beta_0 = \alpha$, $\beta_1 = \alpha\alpha^{\tau}, \ldots, \beta_{n-1} = \alpha\alpha^{\tau}\ldots\alpha^{\tau^{n-1}} = 1$ and consider the K-linear map $\varphi: L \to L$ (as a K-vector space) by $x \mapsto \beta_0 x + \beta_1 x^{\tau} + \ldots + \beta_{n-1} x^{\tau^{n-1}}$. This is a nontrivial linear combination of distinct automorphisms of L fixing K and is hence nonzero by Dedekind's lemma (§7). In particular there's some $\gamma \in L$ with $\gamma^{\varphi} = \delta \neq 0$. Its easy to check that $\delta = \alpha\delta^{\tau}$ so δ satisfies the required property.

Now let L:K be cyclic of degree n (ie as before), of characteristic not dividing n and such that x^n-1 splits in K. Then for some $\theta \in K$, $x^n-\theta$ is irreducible over K but has L:K as splitting field extension, and if $\beta \in L$ is a root of $x^n-\theta=0$ then $L=K(\beta)$.

Let ε be a primitive n^{th} root of unity in K and let τ generate the Galois group $\Gamma(L:K)$. Then $\varepsilon\varepsilon^{\tau}\varepsilon^{\tau^2}\dots\varepsilon^{\tau^{n-1}}=1$ so $\varepsilon=\beta/\beta^{\tau}$ and $\theta=\beta^n=\varepsilon^n(\beta^{\tau})^n=(\beta^n)^{\tau}$ is in the fixed field of $\Gamma(L:K)$, ie K. The minimal polynomial of β divides $x^n-\theta$ but has n distinct roots $\beta, \beta^{\tau}, \dots, \beta^{\tau^{n-1}}$ (since $\beta^{\tau^i}=\varepsilon^{-i}\beta$), so it is $x^n-\theta$. The result follows.

Given an extension with soluble Galois group we may, by refining the series which demonstrates solubility to one with cyclic quotients of prime order, wlog assume it to be cyclic. We now require simply to show that a cyclic extension is radical. Where roots of unity are missing in some term we may adjoin them there and in succeeding terms and refine the sequence once more: the original extension will then be a proper subext^n of the last term, but we have accommodated that in the definition. Each stage is now an extension either by a p^{th} root of unity, or by a p^{th} root of something else in the presence of p^{th} roots of unity. Thus the given extension is radical.

14. The quadratic, cubic and quartic

It's easy enough to write down formulae for the roots of a polynomial equation of degree at most four as radical expressions in the coefficients, although it gets a bit tedious unless you make a few substitutions. Our purpose is to understand why it works: how to do it is then just calculation. Let us assume that our polynomial is of the form $x^n+a_{n-2}x^{n-2}+\dots+a_1x+a_0$ and irreducible over $\mathbb{Q}$.

The Galois group may be regarded as a transitive permutation group on the roots. It is thus a subgroup of S_n itself having a subgroup of index n. For $n=2$ it must then be (the cyclic group of order) 2, for $n=3$ it is either 3 or S_3, for $n=4$ it is 4, $V'=\langle(12),(34)\rangle$, $V=\{1,(12)(34),(13)(24),(14)(23)\}$, D_4 (the dihedral group of order 8), A_4 or S_4. For $n=5$ it has order 5, 10, 20, 60 or 120.

The first subgroup of S_n which comes to mind is A_n: what is its fixed field? Consider the expression $\delta=\prod_{i<j}(\alpha_i-\alpha_j)$ whose square is in the fixed field of the whole group

and is hence rational; indeed with some effort one can express it as a rational function of the coefficients. If $\delta \in K$ then the elements of the Galois group must permute the roots evenly, so it must be a subgroup of A_n, but not otherwise. Let us then adjoin δ to K. This already splits the quadratic.

For the cubic we are now left with a cyclic Galois group of order 3, so as in the previous section we must adjoin ω, a complex cube root of unity, and then a suitable cube root if necessary. The extension may now have degree up to 18. If the roots are α, β, γ we already know $\alpha+\beta+\gamma=0$, so let's consider $\lambda = \alpha+\omega\beta+\omega^2\gamma$ and $\mu = \alpha+\omega^2\beta+\omega\gamma$. The Galois group ($A_3$) permutes α,β,γ cyclically so multiplies λ,μ by a power of ω, hence it fixes λ^3, μ^3; if we were to take S_3 in stead, an odd permutation would swap these: thus they satisfy a quadratic equation over $\mathbb{Q}$ which we have essentially already solved. Adjoining a cube root of either λ^3 or μ^3 now solves the cubic.

Explicitly, if our cubic is $x^3+3px+2q$ we have $\lambda^3, \mu^3 = -q \pm \sqrt{p^3+q^2}$ and $\alpha,\beta,\gamma = \frac{1}{3}(\lambda+\mu), \frac{1}{3}(\omega^2\lambda+\omega\mu), \frac{1}{3}(\omega\lambda+\omega^2\mu)$. Over $\mathbb{R}$, we have three distinct roots if $p^3+q^2<0$, one single and one double if $p^3+q^2=0\neq q$, a triple root at zero if $p=q=0$ (obviously) and a single root (with a complex conjugate pair) if $p^3+q^2>0$.

For the quartic, extension by δ reduces the group from S_4, D_4, V' or 4 to A_4, V or 2 in the same way it reduced the cubic from S_3 to $3=A_3$. The interesting case is now A_4, which has a normal subgroup V of index 3. This corresponds to the subfield generated by $\lambda=(\alpha+\beta)(\gamma+\delta)$, $\mu=(\alpha+\gamma)(\beta+\delta)$, $\nu=(\alpha+\delta)(\beta+\gamma)$ where the roots are α,β,γ as before. The Galois group (whether S_4 or A_4) permutes these transitively, so they satisfy a cubic equation which may be solved as before.

15. The Quintic.

It is an exercise from elementary group theory that A_5 is simple (has no normal subgroups apart from itself and 1) and so A_5 and S_5 are not soluble. Thus a quintic equation with either of these as its Galois group cannot be solved by radicals. Such a quintic is x^5-6x+3, which satisfies Eisenstein's criterion and is hence irrational (so its Galois group is transitive, so has order a multiple of five, hence has an element of order five which must be a cycle, wlog (12345)). By curve-sketching [Analysis I Exercise] it has exactly three real (and two complex) roots, so the Galois group includes complex conjugation, which is wlog (12) as a permutation. Now $\langle(12),(12345)\rangle$ generates S_5.

Some quintics can of course be solved by radicals, namely those whose Galois group has order 5, 10 or 20. These are the subgroups, wlog, $\langle(12345)\rangle$, $\langle(12345),(25)(34)\rangle$ and $\langle(12345),(2453)\rangle$ of S_5. An example of the first is obviously x^5-2 over $\mathbb{Q}(\varepsilon)$, where ε is a root of $x^4+x^3+x^2+x+1=0$, but this will also do for the others with ground fields $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}$ respectively. [Exercise: there are no other transitive subgroups of S_5].

The general quintic is the polynomial $x^5+s_1x^4+\dots+s_5$ over the transcendental extension $K(s_1,\dots,s_5)$ in the five independent "indeterminates" $s_1,\dots,s_5$. The splitting field of this polynomial is $K(t_1,\dots,t_5)$ and has Galois group S_5, acting as arbitrary permutations of $\{t_1,\dots,t_5\}$. This fixes the expressions $s_1=t_1+t_2+t_3+t_4+t_5$, $s_2=t_1t_2+t_1t_3+\dots+t_4t_5$, etc., and any other expression it fixes (such as $t_1^2+t_2^2+\dots+t_5^2$) must be a rational function of these, which are called the elementary symmetric polynomials in five variables (similarly for any other number).

It's clear that the general quintic (or sextic, ...) cannot be solved by radicals, ie there's no radical expression for the roots in terms of the coefficients. We have essentially already found such expressions for the general quadratic, cubic and quartic.

16. The theorem of the primitive element.

Recall that a simple extension is one of the form $K(\alpha):K$. We shall prove that every finite separable extension is simple as a corollary of the stronger result that an algebraic extension $L:K$ is simple iff there are only finitely many intermediate fields. Observe first that if K and L are finite fields, $L:K$ is trivially simple since the multiplicative group L^*, is cyclic. Alternatively we may count the elements in the subfields of $L=GF(p^n)$, which number at most Σp^d over the proper divisors d of n: this sum is clearly (much) less than p^n. A randomly chosen element of $GL(2^{12})$, for instance, generates it with odds of 10:1 on or better!

Now let $L:K$ have only finitely many intermediate fields but with K an infinite field. Clearly $L:K$ is finitely generated since otherwise there would be an infinite strictly ascending sequence of subfields. Choose $\alpha \in L$ with $K(\alpha):K$ a maximal intermediate simple extension (we dont need choice for this since there are only finitely many) and let $\beta \in L \setminus K(\alpha)$. Consider the fields $K(\alpha + k\beta)$ for $k \in K$; since there are only finitely many intermediate fields but infinitely many values of k, two of these must coincide, so $K(\alpha+k_1\beta) = K(\alpha+k_2\beta)$. These both contain $((\alpha+k_1\beta)k_2-(\alpha+k_2\beta)k_1)/(k_2-k_1)$ and $((\alpha+k_1\beta)-(\alpha+k_2\beta))/(k_1-k_2)$, ie α and β, contradicting the maximality of $K(\alpha)$. Thus $L:K$ is simple.

Conversely let $K(\alpha):K$ be a simple extension where α has minimal polynomial f over K. For an intermediate field L, the minimal polynomial of α over L is, say, g_L, where (considered as polynomials over $K(\alpha)$), $g_L | f$, and (up to scalar factors) there are only finitely many such g_L (fewer than $2^{\deg f}$ in fact). Thus we aim to show g_L determines L uniquely.

Let $g_L = x^r + a_{r-1}x^{r-1} + \ldots + a_1x + a_0$ be such an intermediate minimal polynomial over a field L. Then L must contain $a_{r-1}, \ldots, a_0$, which, we may suppose, generate a field $M = K(a_{r-1}, \ldots, a_0)$ over K. Thus $K \subseteq M \subseteq L \subseteq K(\alpha)$. Now g_L is irreducible over L and hence, ā fortiori, over M. But each has a root α in $K(\alpha)$, so $M(\alpha) = L(\alpha) = K(\alpha)$, but $L(\alpha):L$ and $M(\alpha):M$ both have degree $r = \deg g_L$ so $L:M$ has degree 1 by the tower law. Thus $M=L$ and these are then clearly determined by g_L.

Notice that we haven't used any Galois theory at all, so we could have proved this in §2 where we first mentioned it.

Now consider a finite separable extension $L:K$. Clearly if we can show that its normal closure $N:K$ has only finitely many intermediate fields then the same is true of $L:K$, so $L:K$ is simple. Now $N:K$ is finite, normal and separable [Exercise: why?] so Galois' theorem applies to classify the intermediate fields as in 1-1 correspondence with the subgroups of the (finite) Galois group $\Gamma(N:K)$, of which there are only finitely many.

Exercise: prove this corollary by a similar method as the theorem without using Galois theory.

17. Ruler and compass constructions

It is particularly apt that this is section 17 since it was Gauss' discovery of a ruler and compass construction for the heptadecagon that won him for Mathematics rather than philology. He was nineteen at the time; Galois, on the other hand, was only twenty at his death in a duel.

For ruler and compass constructions one is given two points at "unit" distance apart and allowed to (i) draw a staight line through any two given points or intersections of constructed lines or circles, (ii) draw a circle whose centre and one of the points on the circumference of which have been given or constructed. Exercise show that, if the given points are $(0,0), (1,0) \in \mathbb{R}$, the constructible points are exactly those whose coordinites lie in the smallest subfield of $\mathbb{R}$ which is closed under square roots.

Thus (exercise) if $K:\mathbb{Q}$ is a finite extension with every $x \in K$ constructible, $[K:\mathbb{Q}] = 2^s$ for some number s. In particular the roots of an irreducible cubic are not constructible and so nor are $\sqrt[3]{2}$ and $\cos 2\pi/9$. This solves two of the three classical problems of duplicating the cube and trisecting an angle (in this case $2\pi/3$); the third problem, of squaring the circle, depends on the transcendence of π.

Since we have now shown the nonagon (and similarly the septagon) not to be constructible, what regular polygons can be constructed with ruler and compasses alone? Clearly if n, m can and $(n,m)=1$ and $d|n$ then so can nm, $2^r n$ and d. Thus the problem reduce to consideration of odd prime powers, p^α, 2^r being trivial.

If the p^α-gon with $\alpha \geqslant 2$ can be constructed then so can the p^2-gon. But this involves constructing a primitive p^2 root of unity and thus an extension of degree $p(p-1)$ over $\mathbb{Q}$, which is never a power of 2. Hence we are left with the p-gon and, by the same argument, $p = 2^k+1$ for some k. Exercise: show that if 2^k+1 is prime then $k = 2^r$ for some r. The only known cases (the Fermat primes) are 3, 5, 17, 257 and 65537.

We shall now show that the Fermat primes give constructible polygons. Let ε be a primitive

pth root of unity where $p = 2^{2^r}+1$ is prime. Then $\mathbb{Q}(\varepsilon):\mathbb{Q}$ is a finite normal separable extension of degree 2^{2^r} and there is a sequence of subextensions $\mathbb{Q}(\varepsilon) = K_{2^r} \supset K_{2^r-1} \supset \ldots \supset K_1 \supset K_0 = \mathbb{Q}$ where each step $K_{i+1}:K_i$ is normal and separable of degree 2, and hence an extension by a root of a quadratic equation, ie wlog a square root. Thus $\mathbb{Q}(\varepsilon):\mathbb{Q}$ is constructible by ruler and compasses.