843/844/845 Algebra Notes. Table of Contents
Roy Smith

843: Galois' necessary criterion for solvable polynomials

B43 notes part 2:
§11) The problem of existence of solution formulas for polynomial equations.

Galois theory provides the final step in the analysis of solution formulas for polynomial equations. The general formulas solving polynomials of degrees 2, 3, 4, which had been known since the 16th century, were thoroughly analyzed by LaGrange in 1770 with a view to solving the riddle of extending them to higher degrees. Proofs of the impossibility of such extensions followed by Ruffini in 1799, and Abel in 1826, the latter one apparently satisfying all objections. After the resolution of the question of existence of general solution formulas (valid for all equations of a given degree), it remained for Galois to clarify the existence of solution formulas valid for particular equations of higher degree. His theory completely reveals the "reason" for the existence or non existence of solution formulas involving radicals, for any polynomial equation, and allows one in principle to distinguish solvable equations of any degree from unsolvable ones. It works not only over **Q** but also over any other field of coefficients, including variable coefficients, thus handles general equations as well as particular ones. To understand Galois' formulation and solution of the problem, first we look at the known solution formulas for equations of degrees 2 and 3.

For the solutions x_1, x_2 of the quadratic equation $x^2+px+q = 0$, we have from antiquity (at least since 825 AD) the solution formula $x = (-p+D^{1/2})/2$, in terms of the coefficients p, q, where $D = (x_1-x_2)^2 = p^2-4q$, and the two solutions are obtained by taking the two square roots of D. For the cubic equation $x^3+px+q = 0$, years of toil and some intrigue led to the publication, by Cardano in 1545, of the following formula. [Fix $(-3D)^{1/2}$, where $D = (x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2 = -4p^3-27q^2$, and vary the cube root to get all three solutions.] $x =$

$$(1/3)[\{(-27q/2)+(3/2)(-3D)^{1/2}\}^{1/3} - 3p/\{(-27q/2) + (3/2)(-3D)^{1/2}\}^{1/3}].$$

For example, in the equation $x^3-1 = 0$, $p = 0$, $q = -1$, $D = -27$, so we get $x = (1/3)(27/2 + 27/2)^{1/3} = (1/2 + 1/2)^{1/3} = 1^{1/3}$, as hoped.

Indeed, for $x^3-a = 0$, we have $p = 0$, $q = -a$, $D = -27a^2$, and hence

$x = (1/3)\{27a/2 + (3/2)(81a^2)^{1/2}\}^{1/3} = (1/3)\{27a\}^{1/3} = a^{1/3}$.

For $x^3 - 4x = 0$, we get $p = -4$, $q = 0$, $D = 256$, and so

$x = (1/3)\left[\{(3/2)(-768)^{1/2}\}^{1/3} + 12/\{(3/2)(-768)^{1/2}\}^{1/3}\right]$

$= (1/3)\left[\{(-27)(64)\}^{1/6} + 12/\{(-27)(64)\}^{1/6}\right]$

$= (1/3)\left[2\sqrt{3}\, i^{1/3} + 12/\{2\sqrt{3}\, i^{1/3}\}\right] = (2/\sqrt{3})(i^{1/3} + i^{-1/3})$

$= (4/\sqrt{3})\mathrm{Re}(i^{1/3})$. Varying the cube roots gives $(4/\sqrt{3})(\cos(\pi/6)) = (4/\sqrt{3})(\sqrt{3}/2) = 2$, $(4/\sqrt{3})(\cos(5\pi/6)) = (4/\sqrt{3})(-\sqrt{3}/2) = -2$, and $(4/\sqrt{3})(\cos(9\pi/6)) = (4/\sqrt{3})(0) = 0$.
Of course, factoring $x^3-4x = x(x-2)(x+2) = 0$ confirms these answers. (Notice a point which fascinated earlier workers, who were not entirely happy with "imaginary" numbers: the solution formula involves imaginaries even though the final answer it gives is real! It can be proved that this cannot be avoided.)

As far as our examples tell us, the formula is even correct! But we have a different goal in mind, we want to understand what the existence of such a formula says about expressing the solutions of a polynomial in terms of the coefficients. Looking at the symbols that are used in the formula, we see three kinds of symbols in the formula, numerals standing for numbers, the letters p, q for the coefficients of the polynomial, and operational symbols standing for the algebraic operations, addition, subtraction, multiplication, division, and the extraction of roots or formation of "radicals". If we want to make a statement that would apply to any formula anyone might ever come up with, we should concern ourselves not with what the specific numbers are in these formulas, but rather with what operations the solutions are formed out of the coefficients.

Specifically, in this formula $(-3D)^{1/2} = (12p^3+81q^2)^{1/2}$ occurs, which means we have taken the arithmetic combination $(12p^3+81q^2)$ of the coefficients, and then taken its square root. Then we have $3p/\{(-27q/2) + (3/2)(-3D)^{1/2}\}^{1/3}$, which shows we have formed the arithmetic combination $\{(-27q/2) + (3/2)(-3D)^{1/2}\}$, involving both the coefficients and that square root, and then we

have taken the cube root of this expression; and finally we have divided by the cube root. To repeat, to get the solution x_1, we have allowed the operations +, −, ·, /, on the coefficients. Then we have added in one new element, the square root $(-3D)^{1/2}$ and allowed arithmetic operations on this new set of elements. Then we have adjoined another new element, the cube root $\{(-27q/2) + (3/2)(-3D)^{1/2}\}^{1/3}$, and finally we have allowed arithmetic operations on this new larger set of elements. Let's try to say this more abstractly, and consequently more simply.
Call the collection of all elements that can be obtained from a given set, using the operations of +, −, ·, /, the "field" generated by those elements. [More precisely a field is a set F with two binary operations +, ·, such that (F,+) is an abelian group, (F−{0},·) is an abelian group, and multiplication is distributive over addition.] If F denotes any field let $F(\alpha)$ denote the field generated over F by "adding in" the new element α. Then the formula above says x_1 belongs to the field formed in the following stages: First form the field F generated over the rational numbers by the coefficients of the polynomial, and let A be a suitable element of F. Then let $F_1 = F(A^{1/2})$ be the field generated over F by the square root of A. Finally, let B be a suitable element of F_1, and put $F_2 = F_1(B^{1/3})$ = the field generated over F_1 by adding in the cube root of B. Then the solution x_1 given by the cubic formula above, lies in F_2.
Thus the field containing the solution was obtained by two extensions of the field of the coefficients, each extension being made by adjoining a single nth root of an element from the previous field.

This suggests the following way to formulate the statement that a polynomial has such a formula for its solutions. If f is a polynomial, let F be the field generated by its coefficients, and let K be the field generated by its solutions. Then there is a formula of the previous kind for the roots of f, iff the "solution field" K is contained in a field which can be formed in a finite number of steps, starting from F, and such that each successive field is formed by adding in a root or "radical" of an element of the previous field. I.e. K must be a subfield of a field of form F_n, where $F_0 = F$, $F_1 = F(A_1^{1/r_1})$ = the field obtained by adjoining to F a root of an element A_1 in F, $F_2 = F_1(A_2^{1/r_2})$ = the field obtained by adjoining to F_1 a root of an element A_2, etc,....., $F_n = F_{n-1}(A_n^{1/r_n})$ = the field obtained by

adjoining to F_{n-1} a root of the element A_n, where A_n is in F_{n-1}. We will say that such a field F_n is a "radical" extension of F.

Thus in order for a polynomial with rational coefficients to have a solution formula in terms of radicals, the solutions must be contained in a "radical extension of $\mathbb{Q}$", i.e. in some subfield of $\mathbb{C}$ of form $\mathbb{Q}(a^{1/n}, b^{1/m}, c^{1/k}, \ldots)$ where a is in $\mathbb{Q}$, b is in $\mathbb{Q}(a^{1/n})$, c is in $\mathbb{Q}(a^{1/n}, b^{1/m})$, etc....

§12) The Galois group of a field extension: Galois' answer to the problem of existence of solution formulas for polynomial equations.

Now that we have posed the problem of existence of a solution formula, how can we study it? I.e. how can we tell whether a given field, such as a solution field for a polynomial, is or is not contained in a radical field extension of another field? More generally, when is an inclusion of fields $K \subset L$ possible? Let's try using the "functorial" approach of changing this question into one we can answer more easily. We do know a bit more about groups than we do about fields, so maybe we can change the question into one about groups. I.e. suppose we concoct a suitable functor from fields to groups, taking say F to G(F). Then an inclusion of fields, $K \subset L$ will yield a homomorphism $G(K) \to G(L)$ if our functor is covariant, or $G(L) \to G(K)$ if contravariant. If moreover either $G(K) \to G(L)$ is injective, or $G(L) \to G(K)$ is surjective, it would follow that $\#(G(K))$ divides $\#(G(L))$. But the condition found and exploited by Galois is much subtler than these numerical conditions.

Let's sketch briefly the impressive attack that Galois carried out. We have seen a natural construction that associates a group Bij(S) to a set, and we can try something similar, associating the group of field automorphisms to a given field. In order to measure only the extension, i.e. the *change* from the original field to the new field, let's associate to a field extension $k \subset K$, the "Galois" group G(K/k) or $G_k(K)$ of "relative automorphisms", i.e. those field automorphisms of K that act as the identity on k.

Hence to the extension F of $\mathbb{Q}$ we associate the group $G_{\mathbb{Q}}(F)$ of those field automorphisms of F that are the identity on $\mathbb{Q}$, or that leave $\mathbb{Q}$

(pointwise) "fixed". We might hope also that we could understand the group $G(F_n/F_0)$ of a sequential field extension consisting of several steps $F_0 \subset F_1 \subset F_2 \subset \ldots\ldots \subset F_n$, by understanding each of the groups $G(F_j/F_{j-1})$. Then the group associated to a radical extension like $Q(a^{1/n}, b^{1/m}, c^{1/k}\ldots\ldots, h^{1/r})$, should be understandable step by step from studying the group of a single extension like $F(a^{1/n})$, where a is in F. What is one of these groups? If a=1, and we look at the complex roots of $x^n-1 = 0$, we see they consist of the points on the unit circle (in the complex plane) which have angles (measured from z=1) which are multiples of 360/n degrees. Hence if ω denotes the first of these (after 1), the full set of them has form ω, $\omega^2, \omega^3, \ldots, \omega^n = 1$. Moreover if $a^{1/n}$ is one solution of the equation x^n-a, then the full set of solutions is $\omega a^{1/n}$, $\omega^2 a^{1/n}$, $\omega^3 a^{1/n}, \ldots\ldots$, $\omega^n a^{1/n} = a^{1/n}$. Now these sets of solutions look sort of "cyclic" in nature, and it might not be too wild to assume these groups $G_F(F(a^{1/n}))$ are all cyclic, (although in fact things are not quite that simple, but almost).

While we are hypothesizing, suppose indeed that all these individual radical extensions have cyclic automorphism groups, it should perhaps mean that the group of the full radical extension $Q(a^{1/n}, b^{1/m}, c^{1/k}\ldots\ldots, h^{1/r})$ should be "made up" of cyclic subgroups. I.e. the group of this field should have a sequence of subgroups whose quotients are all cyclic! Best of all, perhaps the group of a radical extension would have a decomposition series all of whose simple constituents are of prime order! Since we know there are many simple groups which are not of prime order, this would say it is entirely possible for a root field *not* to be of the form $Q(a^{1/n}, b^{1/m}, c^{1/k}\ldots\ldots, h^{1/r})$. Moreover if we can show that an inclusion $Q \subset K \subset L$ would lead to a surjective homomorphism $G_Q(L) \rightarrow G_Q(K)$, it would follow from one of our extra credit problems that the simple constituents of $G_Q(K)$ are a subsystem of those of $G_Q(L)$. Consequently a solution field could not be contained in a radical extension unless all the simple constituents of the Galois group of the solution field are also of prime order. This in fact is the theorem that Galois proved. Since we know the group S_5 has as simple constituents Z_2 and A_5, only one of which has prime order, it would follow that a solution field with Galois group S_5 could not be contained in a radical extension, and the solutions of the

corresponding polynomial could thus not be expressed by a formula like those which exist for all polynomials of degrees 2, 3 and 4.

Definition: A finite group G is called "solvable" if the simple constituents of a composition series for G are all of prime order.

Theorem(Galois): If the solutions of a polynomial can be expressed in terms of its coefficients by field operations and radicals, the Galois group of the field generated by the solutions is a solvable group.

With this insight we can indicate already why there is no universal formula for the solutions of all fifth degree polynomials. For let $f(x) = x^5+\sigma_1x^4+\sigma_2x^3+\sigma_3x^2+\sigma_4x+\sigma_5$ be a general 5th degree polynomial, i.e. a polynomial whose coefficients are "variables". If we had a formula for the solutions $a_1,\ldots,a_5$, of this polynomial, in terms of the coefficients $\sigma_1,\ldots,\sigma_5$, it would mean that the field extension $\mathbb{Q}(\sigma_1,\ldots,\sigma_5) \subset \mathbb{Q}(a_1,\ldots,a_5)$ would have solvable Galois group. We can get a good idea of what this group is by noticing that one always has an easy expression for the coefficients of a polynomial in terms of the solutions, i.e. the opposite problem to that of finding solution formulas is easy. For if $a_1,\ldots,a_5$ are the solutions of $f(x)=0$, it means we can factor $f(x) = \Pi(x-a_j) =$
$x^5 + \sigma_1x^4+ \sigma_2x^3+\sigma_3x^2+\sigma_4x+\sigma_5$. Actually multiplying out this expression, we see that $\sigma_5 = \Pi(-a_j)$ and $\sigma_1 = \Sigma(-a_j)$, with a bit more thought that $\sigma_2 =$
$a_1a_2 + a_1a_3 + a_1a_4 + a_1a_5 + a_2a_3 + a_2a_4 + a_2a_5+ a_3a_4+ a_3a_5+ a_4a_5$, and in general that σ_j is the sum of all different products formed from j of the elements $(-a_1,\ldots,-a_5)$. It follows that the coefficients σ_j are always in the field generated by the solutions, so there is always an inclusion $\mathbb{Q}(\sigma_1,\ldots,\sigma_5) \subset \mathbb{Q}(a_1,\ldots,a_5)$.

Now suppose we ask what the group of this field extension is. I.e. what are the automorphisms of the field $\mathbb{Q}(a_1,\ldots,a_5)$ which leave fixed all elements of the field $\mathbb{Q}(\sigma_1,\ldots,\sigma_5)$? Remembering that the coefficients $\sigma_1,\ldots,\sigma_5$ are independent variables, it follows (from the theory of transcendence degree) that the solutions $a_1,\ldots,a_5$ are also independent variables. In particular the field $\mathbb{Q}(a_1,\ldots,a_5)$ just consists of quotients of polynomials in the letters $a_1,\ldots,a_5$. Consequently any permutation of those letters changes one

polynomial into another, and gives a field automorphism of $\mathbf{Q}(a_1,\ldots,a_5)$. Moreover by looking at the formulas for the σ_j, you can see that permuting the a's does not change any of the σ's. Consequently the whole group S_5 of permutations of the a's leaves the field $\mathbf{Q}(\sigma_1,\ldots,\sigma_5)$ pointwise fixed. Thus the Galois group of the extension $\mathbf{Q}(\sigma_1,\ldots,\sigma_5) \subset \mathbf{Q}(a_1,\ldots,a_5)$ at least contains S_5. We will see later that the group of this field extension cannot have more than 5! elements, and thus S_5 is exactly the Galois group. Consequently Galois' theorem above implies there can be no universal formula in radicals that solves all fifth degree polynomials, (nor higher degree polynomials either).

Of course we have not fully proved any of our speculations, but we have identified a number of important questions needing answers.
Questions:
1) What is the Galois group of a field extension of form $F(a^{1/n})$? In particular is it cyclic? solvable? What about the case a = 1?
2) If $F = F_0 \subset F_1 \subset F_2 \subset F_3 \subset \ldots F_n = L$, is a sequence of field extensions, what is the relation between the big Galois group $G = G(L/F)$ and the intermediate groups $G(F_j/F_{j-1}) = G_j$? Is there a sequence of normal subgroups of G such that the G_j are the quotients?
3) In particular, given an inclusion of fields $F \subset K \subset L$, how is $G(K/F)$ related to $G(L/F)$? For instance when does an inclusion of fields $F \subset K \subset L$, induce a homomorphism of groups between $G(K/F)$ and $G(L/F)$? I.e. is the Galois group always a functor? If not, for which field extensions is it a functor?

§13) Review of rings, fields, and p.i.d.'s such as $\mathbf{Z}$ and $k[X]$
To be complete we review some elementary concepts which are probably familiar from previous courses.

A <u>commutative ring</u> (with identity), in this course simply called a "ring", is a set R with two binary operations, +, ·, "addition" and "multiplication", such that (R,+) is an abelian group, and multiplication is associative, commutative, and has an identity. Multiplication is also distributive over addition.

Note: In any ring $0x = 0$ for every x; i.e. $0x = (0+0)x = 0x + 0x$, so subtracting $0x$ from both sides gives $0 = 0x$. Thus if $1 = 0$, then $0 = 0x = 1x = x$, so every element of the ring is 0. Thus in every ring except the trivial ring $\{0\}$, we have $1 \neq 0$.

$\mathbb{Z}$ is an example of a (commutative) ring (with identity).

A ring homomorphism is a map of rings $f:R \to S$ such that $f(x+y) = f(x)+f(y)$, for all x,y in R, and such that $f(1) = 1$, where 1 denotes (both) the multiplicative identities. The "kernel" of such a map is $\ker(f) = f^{-1}(0) = \{x \text{ in } R : f(x) = 0\}$. Then f is injective iff $\ker(f) = \{0\}$.

An isomorphism of rings is a homomorphism with an inverse homomorphism. A homomorphism is an isomorphism iff it is both injective and surjective. An automorphism of a ring R is an isomorphism of R with itself.

An ideal in a ring is a subgroup for $+$, which is also closed under multiplication by *all* elements of the ring, not just those in the ideal. I.e. a non empty subset $I \subset R$ is an ideal iff for every x,y, in I we have $x-y$ in I, and for every x in I, and y in R, xy is in I. In every ring R, both $\{0\}$ and R are ideals. R is the only ideal containing 1, hence an ideal $I = R$ iff I contains 1, iff I contains an invertible element (for multiplication). [If I contains x, and x^{-1} is in R, then $1 = xx^{-1}$ is in I, and then for every y in R, $y \cdot 1 = y$ is in I.]
To repeat, a proper ideal never contains an invertible element.

The kernel of a ring homomorphism is always an ideal in the domain. I.e. if $f:R \to S$ is a ring map with $\ker(f) = \{x \text{ in } R : f(x) = 0\}$, we know from group theory that $\ker(f)$ is an additive subgroup, and for any z in R, $f(zx) = f(z)f(x) = f(z) \cdot 0 = 0$, so zx is in $\ker(f)$.

Conversely, every ideal is the kernel of some homomorphism. To show this we use a quotient construction analogous to the one for groups. I.e. given any ideal I in R, define an equivalence relation by equating two elements iff their difference lies in the ideal. Write R/I for the set of equivalence classes. The class $[x]$ of x is the additive coset $x+I$ of all sums $\{x+y: \text{ for all } y \text{ in } I\}$. Then we can define $[x] + [y] = [x+y]$, $[x][y] = [xy]$, and check this is well defined and gives R/I a commutative ring structure with $[1]$ as multiplicative identity.

Indeed from group theory we know R/I is an additive group with [0] as additive identity. Moreover, if $[x_1] = [x_2]$, and $[y_1] = [y_2]$, i.e. if $x_2 = x_1+g$, and $y_2 = y_1+h$, with g,h, in I, then $x_2y_2 = x_1y_1 + g(y_1+h) + x_1h = x_1 +$ (element of I). Hence $[x_1y_1] = [x_2y_2]$, and multiplication is well defined in R/I, by setting $[x][y] = [xy]$. Now everything else is easy to check. In particular, the map R to R/I taking x to [x] is a ring homomorphism with I as kernel.
Cor: If $f:R \to S$ is a ring map and $J \subset S$ is an ideal, then $f^{-1}(J) \subset R$ is an ideal, since $f^{-1}(J)$ is the kernel of the composition $R \to S \to S/J$.
Notice: In general we will try not to consider the trivial ring {0}, but that means we must check whether I = R in each particular quotient construction R/I.

Exercise #50) Prove, if $I \subset R$ is an ideal and $f:R \to S$ is a ring map such that $I \subset \ker(f)$, there is a unique ring map $\bar{f}: R/I \to S$ such that the composition $R \to R/I \to S$ equals f.

The intersection of any collection of ideals in R is again an ideal in R. If S is a subset of R, the ideal (S) "generated by" S, is the intersection of all ideals of R which contain S. It is therefore the smallest ideal of R containing S, in the sense that for any ideal I, if $S \subset I$ then $(S) \subset I$.

Specifically (S) = {all linear combinations of form $x_1y_1+....x_my_m$: where the x's are in R and the y's are in S}. In particular, if S = {y} contains only one point, then the ideal generated by y, called a "principal ideal", has form (y) = Ry = {xy: for all x in R}.

For example, for each integer n, the "principal ideal generated by n" = (n) = {set of all integral multiples of n}. The quotient ring $\mathbf{Z}/(n) = \mathbf{Z}_n$ is the ring of "integers mod n".

In fact in **Z**, all ideals are principal. [Certainly {0} and **Z** are principal. If n is the smallest positive element of a non trivial ideal I, then dividing any other element of I by n yields a non negative remainder which is also in I, hence is zero. QED.]

Exercise #51) If S is a non empty subset of **Z**, the ideal (S) generated by S is equal to (n), where n = gcd of the elements in S.

Exercise #52) The element [x] is invertible in $\mathbf{Z}_n$ iff x is relatively prime to n, i.e. iff gcd(x,n) = 1.

A field is a commutative ring in which the non zero elements form a commutative group under multiplication, in particular they are a non empty set, so $1 \neq 0$ in a field, which thus has $\geq$ two elements. A homomorphism of fields is a homomorphism as rings.

Examples of fields, include $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$; and $\mathbf{Z}_p$ is a field iff p is prime, (by exercise #52 above).
Fields have two simple but important properties: they have no "zero divisors" and no non trivial ideals:
To see the only ideals in a field F are the trivial ones {0} and F, recall that proper ideals never contain invertible elements. On the other hand, if R is a ring but not a field, and $x \neq 0$ is not invertible, then (x) is a non trivial ideal, so fields are the only rings with no nontrivial ideals.

Every ring homomorphism $f: F \to R$ where F is a field, and $R \neq \{0\}$, is injective. I.e. $f(1) = 1 \neq 0$, so $\ker(f) \neq F$, but the only other ideal of F = {0}, and thus f is injective.

Definition: A "maximal" ideal in a ring R, is a proper ideal $I \neq R$ such that the only ideals J with $I \subset J \subset R$ are J = I and J = R.

Cor: A quotient ring R/I is a field iff $I \subset R$ is a maximal ideal.

Definition: A "domain" or "integral domain" is a ring with no "zero divisors", i.e. in which xy=0 implies either x = 0 or y = 0.

Every field is a domain, since if xy = 0 and $y \neq 0$, then $0 = (xy)y^{-1} = x1 = x$. Consequently every subring of a field is a domain.

Exercise #53) Every domain is a subring of a field.
(Hint: Given a non trivial domain R, define $F_1 = \{(a,b)$ in $R \times R$, s.t. $b \neq 0\}$, and define $(a, b) \sim (c, d)$ in F_1 iff $ad-bc = 0$. Show this is an equivalence relation, and let $F = F_1/\sim$, the set of equivalence classes. Prove F is a field, with the operations $(a,b) + (c,d) = (ad+bc, bd)$ and $(a, b)(c, d) = (ac, bd)$, and F contains a subring isomorphic to R consisting of the elements (a, 1) for a in R. Replacing (a, 1) by a

gives the subring $R \subset F$. This field F is called the "quotient field" or "field of fractions" of R.]

Exercise #54) Prove the "quotient field of R", F = qf(R), is the smallest field containing R, in the sense that if K is any field containing R, there is an injective homomorphism $\varphi: F \to K$ such that φ is the identity on R.

Remark: The definition of $\mathbf{Q}$ shows that $\mathbf{Q} = qf(\mathbf{Z})$. Hence every field containing an isomorphic copy of $\mathbf{Z}$ also contains $\mathbf{Q}$.
Exercise #55) If R is any ring, there is a unique ring map $\mathbf{Z} \to R$. A field F is said to have "characteristic zero" iff the unique ring map $\mathbf{Z} \to F$ is injective.

Exercise #56)/Definition: If F is a field and the map $\mathbf{Z} \to F$ is not injective, then $\ker(f) = (p)$, for some prime p. We say then that F has characteristic $p > 0$.

Exercise #57)/Definition: If F is any field, the "prime field" of F is the intersection of all subfields of F. It is always isomorphic either to $\mathbf{Q}$ or to some $\mathbf{Z}_p$.

Definition: If $S \subset L$ is a subset of a field L, then "the subfield of L generated by S" is the intersection of all subfields of L which contain S. If $R \subset L$ is a subring, the subfield of L generated by R is $\cong qf(R)$. If $F \subset L$ is an inclusion of fields, and $S \subset L$ is a subset of the larger field, then F(S) = "the subfield of L generated over F by S" is the intersection of all subfields of L which contain both F and S. This is the smallest subfield of L which contains the field F and the set S.

Definition: Another very important example of a ring, is the ring k[X] of polynomials in one variable X over the field k. We can define these naively, by taking the field k and any symbol X not in the field, and constructing the set of all finite expressions of form $a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$, where the a_i are all in k. Define multiplication of monomials by $(aX^n)(bX^m) = (ab)(X^{n+m})$, and extend that definition to all polynomials by the distributivity and commutativity laws. We decree that two polynomials are different iff they "look different", i.e. $a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 = 0$ iff all

the a_i are zero, and consequently $a_nX^n + a_{n-1}X^{n-1}+...+a_1X + a_0 = b_mX^m + b_{m-1}X^{m-1}+...+b_1X + b_0$ iff $n = m$ and for all i, $a_i = b_i$. [To compare two polynomials with a different number of terms we can add higher powers of X, with coefficient zero, to one of them. I.e. all missing powers of X are thought of as having coefficient zero.] $k[X]$ is a commutative ring with identity. If R is any ring, we can define $R[X]$ similarly.

The degree of a polynomial is the highest exponent of X occurring with a non zero coefficient. The degree of the 0 polynomial is "minus infinity". If R is a domain and f,g are polynomials over R, we have $Deg(fg) = Deg(f) + Deg(g)$, so $R[X]$ is an integral domain if R is. In particular if k is a field, we can embed $k[X]$ in its quotient field.

Definition: If k is a field, denote the quotient field of $k[X]$ by $k(X)$, called the "field of rational functions" of one variable X. Thus an element of $k(X)$ can be represented in the form $f(X)/g(X)$ where f,g are polynomials in X and $g \neq 0$.

Definition: If k is a field, a "k-algebra" is any ring containing k. If R, S are both k algebras, a "k-algebra map" $R \to S$ is a ring map which is the identity map on k.

The polynomial ring $k[X]$ is a "free k-algebra" on one generator, in the sense of the following exercise:

Exercise #58: (i) The construction taking k to $k[X]$ is a functor from fields to algebras over fields.
(ii) Given a field k, if R is any k algebra, and α any element of R, there is a unique k algebra map $f:k[X] \to R$ such that $f(X) = \alpha$.

More generally, we define the polynomial ring $k[X,Y]$ over k on two variables X,Y to be $R[Y]$, where $R = k[X]$, and the polynomial ring $k[X_1,...,X_n]$ on n variables $X_1,...,X_n$ to be $R[X_n]$ where $R = k[X_1,...,X_{n-1}]$. Then for any sequence $\alpha_1,...,\alpha_n$ of elements of a k algebra S, there is a unique k algebra map $f:k[X_1,...,X_n] \to S$ such that $f(X_j) = \alpha_j$, for every $j = 1,...,n$. Just as in the case of the free abelian group generated by a set, it follows that these polynomial algebras give a "free" functor from finite sets to k algebras.

Definition: A "principal ideal domain" or p.i.d. is an integral domain in which every ideal is principal. All fields k, the integers $\mathbf{Z}$, and k[X], are p.i.d.'s. [To show k[X] is a p.i.d., imitate the argument for $\mathbf{Z}$. I.e. show that an ideal $I \subset k[X]$ is generated by an element f of smallest degree in I, since dividing any other element of I by f yields a remainder which is also in I, but of lower degree, hence zero.]

Remark: The slight difficulty encountered above in comparing two polynomials of different degrees, reveals that a careful definition of polynomials will admit the fact that terms of all orders are present, but that most of them have coefficient zero. A more precise definition of the polynomials in k[X] would be as infinite sequences $(a_n) = (a_0, a_1, a_2, \ldots)$ of elements of k, such that each sequence has only a finite number of non zero terms. Then one defines addition term by term, and multiplication by a rule that looks exactly like multiplication of polynomials. I.e. the k-th term in the product of $(a_n)\cdot(b_m)$ is the sum of all products of form $a_s b_t$ where $s+t = k$. Thus $(a_n)\cdot(b_m) = (a_0b_0, a_0b_1+a_1b_0, a_0b_2+a_1b_1a_2b_0, \ldots\ldots)$.

There are also important non commutative rings in nature, such as rings of matrices, but we will leave their study until later.

§14) Continuation of review of divisibility in $\mathbf{Z}$, k[X]:

Lemma: The greatest common divisor of two integers a,b can be written in the form an+bm for some n,m.
proof: The ideal (a,b) = {an+bm: for all n,m} = (d) where d is the gcd(a,b), by exercise #37. Hence d = an+bm, for some n,m. QED.

Definition: An element x of $\mathbf{Z}$ is <u>irreducible</u> iff $x \neq 0, 1, -1$, and whenever x = ab, for a,b in $\mathbf{Z}$, then either a or b equals 1 or -1.

Cor: If p is an irreducible integer and if p divides ab, then either p divides a or p divides b.
proof: If p does not divide a then gcd(a,p) = 1, so we can write 1 = np+ma, for some n,m in $\mathbf{Z}$. Multiplying by b gives b = bnp+bma. Notice that p divides the right hand side of this, since p divides ab. Hence p also divides the left hand side, i.e. p divides b. QED.

Definition: The invertible integers 1, -1 are called units.

Cor(Unique factorization of integers): If n is an integer, neither zero nor a unit, then n can be written as a (finite) product of irreducible integers $n = \Pi p_i$. Moreover, if $\Pi q_j = n = \Pi p_i$, where all p_i, q_j are irreducible, then there are the same number of p's and q's, and after possibly renumbering the indices of the q's, we have $p_i = q_i$ or $-q_i$, for every i.
proof: [sketch]. Existence of a factorization is easy by induction. I.e. if n is itself irreducible we have a factorization into one factor, n itself. If n is not irreducible, then n = ab where a,b are smaller than n, hence by induction each of them has a factorization into irreducibles. Multiplying those two factorizations together gives a factorization of n. For uniqueness, we use the previous corollary. I.e. if $\Pi q_j = \Pi p_i$, then q_1 divides the left hence also the right. Since q_1 is irreducible and divides the product of the p_i, it must divide one of them. Since all p_i are irreducible, the one divisible by q_1 must equal either q_1 or $-q_1$. Then we can cancel q_1 from both sides. Now we are done by induction. I.e. we have an equation between two smaller products of irreducibles, so they must consist of the same factors, up to ordering and sign. **QED.**

The same argument just used for uniqueness proves also:
Cor: For n,m any two integers, n divides m iff every irreducible factor p of n appears also as an irreducible factor of m, and the exponent of p as a factor of m is at least as large as its exponent as a factor of n.
Cor: The gcd of two integers n, m can be found as follows from their prime factorizations: factor both n, m into irreducible factors. For each irreducible factor p of both n, m raise p to the *smaller* of its two exponents, i.e. of that occurring in the factorization of n, and that occurring in the factorization of m. Multiplying all these powers of the factors together gives the gcd of n, m. For example $\gcd(2^3 5^4 7, 2^5 3\ 5^2 7^3) = 2^3 5^2 7$.

Cor: A rational number n/m can be reduced to "lowest terms" in a unique way, up to multiplying by minus signs.
proof: Factor both n, m into irreducible factors, and cancel like factors from top and bottom. **QED.**

Cor: $\sqrt{2}$ is irrational.
proof: We can write any rational square root of 2 as a/b in lowest form. Then $a^2/b^2 = 2/1$, is also in lowest form, and by uniqueness then $b^2 = 1$, and $a^2 = 2$, so 2 is an integral square root of 2. But $1^2 \neq 2$, $2^2 = 4$, and all other integers have still larger squares, so there is no integral square root of 2. Hence there is no rational square root of 2 either. QED.

Similar arguments show $\sqrt{3}$ is irrational, and $\sqrt{n}$ is irrational, whenever n is not a square of an integer.
Since these divisibility arguments for **Z** used only that **Z** is a p.i.d., analogous arguments go through for the ring k[X], as follows:

Definition: In a ring R, gcd(a,b) = s iff s divides both a, b and any other common divisor of a, b divides s. [gcd(a,b) need not exist.]

Lemma: The greatest common divisor of two polynomials f, g in k[X] exists, and can be written in the form fh+gr for some h, r in k[X].
proof: The ideal (f,g) = {fh+gr: for all h,r in k[X]} = (s) for some s in k[X]. Thus f,g are both multiples of s, and also s = fh+gr, for all h,r in k[X]. Hence a polynomial that divides f,g also divides s. QED.

Definition: An element f of k[X] is <u>irreducible</u> iff f is not in k, and whenever f = gh, for g,h in k[X], then either g or h is in k.

Cor: If f is irreducible and f divides gh, then either f divides g or f divides h.
proof: If f does not divide g then gcd(f,g) = 1, so we can write 1 = fr+gs, for some r,s in k[X]. Multiplying by h gives h = hfr+hgs. Since p divides gh f divides the right hand side of this, hence f also divides the left hand side, i.e. f divides h. QED.

Definition: The invertible polynomials, those in k-{0}, are called units.

Cor(Unique factorization of polynomials): If f is in k[X], but not in k, then f can be written as a (finite) product of irreducible polynomials $f = \Pi f_i$. Moreover, if $\Pi f_i = f = \Pi g_j$ where all f_i, g_j are irreducible, then there are the same number of f_i and g_j, and after

possibly renumbering the indices of the g_j, we have $f_i = c_i g_i$, for every i, where c_i is a unit.
proof: [sketch]. Existence: If f is itself irreducible we are done. If not, f = gh where g,h have smaller degree than f, hence by induction each of them has a factorization into irreducibles. Multiplying those two factorizations together gives a factorization of f. For uniqueness, we use the previous corollary. I.e. if $\Pi f_i = \Pi g_j$, then f_1 divides the left hence also the right. Since f_1 is irreducible and divides the product of the g_j, it must divide one of them. Since all g_j are irreducible, the one divisible by f_1 must equal $c_1 f_1$ for some c_1 in k-{0}. Then we can cancel f_1 from both sides. Now we are done by induction. I.e. we have an equation between two smaller products of irreducibles, so they must consist of the same factors, up to ordering and unit factors. QED.

Cor: If k is a field, then k[X]/(f) is a field iff f is an irreducible polynomial.
proof: If f is irreducible, then any ideal I such that $(f) \subset I \subset k[X]$ must equal I = (g), where g divides f. Since f is irreducible, either g = cf for c in k-{0}, or g = c in k-{0}. In the first case (g) = (f)m, and in the second (g) = k[X]. Thus (f) is maximal, and k[X]/(f) is a field. If f is reducible, say f = gh where g,h have lower degree than f, then [g][h] = [0] in k[X]/(f), but neither [g], nor [h] is zero, so the quotient ring is not an integral domain, hence not a field. If f is a unit, then (f) = (1) = k[X] and the quotient is {0}, so not a field. If f is zero then the quotient is k[X], not a field. QED.

Recall from high school the useful
Remainder theorem: If f is a polynomial over a field k, and c is in k, then f(X) = g(X)(X-c) + f(c), for some polynomial g(X).
proof: After dividing f(X) by (X-c) the remainder has degree less than (X-c), i.e. less than one, hence belongs to k. So we have f(X) = g(X)(X-c) + r where r is in k. Substituting X = c gives r = f(c). QED.

Cor(Root/Factor theorem): An element c of a field k is a root of a polynomial f in k[X] iff (X-c) is a factor of f in k[X].
proof: The remainder after division of f(X) by (X-c), is f(c). QED.

Cor: A polynomial $f \neq 0$ in k[X], has at most deg(f) roots in k.

proof: This is true if deg(f) = 1, since a(X-r) has only r as a root. If deg(f) = n, and r is a root of f, then f(X) = g(X)(X-r), where deg(g) = n-1. But since k is a domain, f(c)=g(c)(c-r) = 0 implies either c = r or g(c) = 0, and by induction g has at most n-1 roots. QED.

Cor: A polynomial of degree 2 or 3 with no roots in k is irreducible over k.
proof: Any non trivial factorization would involve a factor of degree one, which must have a root. QED.

In particular, X^2+1 is irreducible over $\mathbb{R}$, as is X^2+c for every $c > 0$. Moreover, since we know $2^{1/2}$, $3^{1/2}$ are irrational, then X^2-2, X^2-3 are irreducible over $\mathbb{Q}$. The following theorem shows many other specific polynomials have no rational roots.

Rational Root Theorem: If the coefficients of $f(X) = a_nX^n+.....+a_0$ are integers, the only possible rational roots of f are the rational numbers of form c/d, where c is a factor of a_0 and d a factor of a_n.
proof: Assume c/d is in lowest form, i.e. c, d have no common factors, set f(c/d) = 0, and multiply through by d^n. This gives $0 = a_nc^n + da_{n-1}c^{n-1} + d^2a_{n-2}c^{n-2} + ...+d^{n-1}a_1c + d^na_0$. Putting the first term on the other side of the equation, gives $-a_nc^n = da_{n-1}c^{n-1} + d^2a_{n-2}c^{n-2} + ...+d^{n-1}a_1c + d^na_0$, so that d divides the right hence the left side, hence d divides the product a_nc^n. But since c, d are relatively prime, none of the prime factors of d occurs in c^n. Hence all prime power factors of d occur in a_n, i.e. d divides a_n. On the other hand if we put the last term d^na_0 on one side by itself we conclude similarly that c divides a_0. QED.

Terminology: A "monic" polynomial is a polynomial with leading coefficient = one.

Cor: The only possible rational roots of a "monic" polynomial with integer coefficients are the integer factors of the constant term.

Cor: X^3-2 has no rational roots, hence $2^{1/3}$ is irrational, and X^3-2 is irreducible over $\mathbb{Q}$.
proof: The only possible rational roots are the integers 1,-1,2,-2, but

those do not work. Since any factorization of a cubic would have a linear factor, a Q-factorization would lead to a rational root. QED.

Cor: If a is an integer but not the nth power of an integer, then $a^{1/n}$ is irrational. If a is an integer but not a cube of an integer, then X^3-a is irreducible over $\mathbb{Q}$.
proof: The same proof works again. QED.

Cor: The quotient rings $\mathbb{Q}[X]/(1+X^2)$, and $\mathbb{Q}[X]/(X^3-2)$ are fields.
proof: Irreducible polynomials generate maximal ideals. QED.

We have need also for the elementary theory of dimension of vector spaces so we review it next.

§15) Digression on dimension of vector spaces over fields.

Definition: A "vector space" over the field k, is an abelian group (V,+) together with a way to multiply elements of V by elements of k, such that if x,y are in k, and v,w are in V then $(x+y)v = xv+yv$, $1v = v$, $x(v+w) = xv+xw$, and $(xy)v = x(yv)$.

Remarks: A quick way to summarize these axioms is to say there is a ring map $k \to End(V) = Hom(V,V)$, from k into the (non commutative) ring of "endomorphisms" of V, i.e. additive homomorphisms from V to itself. [Recall that Hom(V,V) is a commutative abelian group under +, where $(f+g)(x) = f(x)+g(x)$, with additive identity the constant zero homomorphism, and where multiplication is composition, i.e. $(fg)(x) = f(g(x))$. The identity map is hence the multiplicative identity, but composition is not commutative. Since k is commutative however, the image of k in End(V) consists of homomorphisms that commute with each other. It follows too that not every abelian group V can be a vector space over k, since unless $V = \{0\}$ there must be an isomorphic copy of the field k inside the ring End(V). For example if $V \neq \{0\}$ is finite, and k is infinite there is no way this can happen. Indeed, it turns out that the only groups which can be "finite dimensional" vector spaces over k, are isomorphic to the product groups $k \times k \times \cdots \times k$ [products of copies of the additive group (k,+)].

Definition: A k-homomorphism of vector spaces $f:V \to W$ is a map such that $f(v+w) = f(v) + f(w)$, for all v,w in V, and such that $f(xv) = xf(v)$, for all x in k, v in V.

Exercise: A k homomorphism $f:V \to W$ is an isomorphism, i.e. has an inverse k-homomorphism, if and only if f is bijective.

The essential concept is that of "linear combination".
Definition: If V is a k vector space, and $S \subset V$ is a subset, a "linear combination" of elements of S is a finite expression of form $\Sigma a_j x_j$, where the a's are in k and the x's are in S. A "non trivial" linear combination is one in which at least one of the a_j is non zero.

Definition: If V is a k vector space, an element x of V "depends on" the subset $S \subset V$ iff x equals a linear combination of elements of S. Sometimes it is convenient to say the vector 0 depends on the empty set.

Definition: A set $S \subset V$ is "(linearly) dependent" iff the vector 0 is a non trivial linear combination of elements of S, iff some vector in S depends on the other vectors in S. For example if S contains 0, then S is dependent. An indexed system $S = \{w_j\}$ of vectors in V, where vectors with different indices need not be different, is dependent iff 0 can be written as a finite linear combination of form $\Sigma_j a_j w_j$ and some a_j is non zero. Hence if some vector occurs more than once in such a system, the system is dependent.

A set or system is "(linearly) independent" iff it is not dependent, iff the only way to write zero as a finite linear combination of the vectors in the set or the system is for all coefficients to be zero, iff no vector in the set or system can be written as a linear combination of the others.

Definitions: (i) The "(k-)dimension" of a k vector space V is the maximal number of elements in an independent subset of V.
(ii) A subset $S \subset V$ "spans" V iff every vector in V depends on S.
(iii) A "basis" of V is an independent subset that spans V.

The following Lemma is the main technical result on dimension:
Main Lemma: If $S = \{x_1,...,x_n\}$ is an independent set in V, and T =

$(y_1,\ldots,y_m)$ is a set of vectors in V each of which depends on S, where $m > n$, then T is a dependent set.
proof: (from Brauer's Galois Theory notes: by induction on n.)
If $n = 1$, then $m \geq 2$, so we have at least $y_1 = a_1x_1$, and $y_2 = b_1x_1$.
case i) If $a_1 = 0$, then $y_1 = 0$, so T is a dependent set, since $0 = 1 \cdot y_1 = 1 \cdot 0$, is a non trivial combination of elements of T, (non trivial since the first coefficient is 1, not zero).
case ii) If $a_1 \neq 0$, then $x_1 = (1/a_1)y_1$. Thus $y_2 = b_1x_1 = (b_1/a_1)y_1$, thus T is dependent, since $0 = y_2 - (b_1/a_1)y_1$ expresses 0 as a non trivial linear combination of elements of T (the coefficient of y_2 is 1).
If $n \geq 2$, we do the same thing, i.e. solve for one of the x's in terms of y_1 and the other x's. then we write the other y's in terms of y_1 and the other x's and use induction. Rather than give a general proof, we illustrate it for $n = 4$, assuming we have proved the theorem for $n = 3$. Then there are 4 or more y's, but we only need 4 of them.
I.e. say we have
$y_1 = a_1x_1+a_2x_2+a_3x_3$,
$y_2 = b_1x_1+b_2x_2+b_3x_3$,
$y_3 = c_1x_1+c_2x_2+c_3x_3$,
$y_4 = d_1x_1+d_2x_2+d_3x_3$.

case i) all a's $=0$. Then $y_1=0$, and T is dependent.
case ii) some $a \neq 0$, renumber until $a_1 \neq 0$.
Then $a_1x_1 = y_1-a_2x_2-a_3x_3$, so $x_1 = (1/a_1)y_1-(a_2/a_1)x_2-(a_3/a_1)x_3$.
Now if we substitute this for x_1 in each of the three equations for y_2,y_3,y_4, we get expressions which involve only y_1,x_2,x_3, i.e. say
$y_2 = r_1y_1+r_2x_2+r_3x_3$
$y_3 = s_1y_1+s_2x_2+s_3x_3$
$y_4 = t_1y_1+t_2x_2+t_3x_3$.

Now put the y_1 terms over on the left, to get
$y_2 - r_1y_1 = r_2x_2+r_3x_3$
$y_3 - s_1y_1 = s_2x_2+s_3x_3$
$y_4 - t_1y_1 = t_2x_2+t_3x_3$.

Here we have three vectors, the three on the left hand sides of these equations, $y_2 - r_1y_1$, $y_3 - s_1y_1$, and $y_4 - t_1y_1$, depending on the

two independent vectors x_2, x_3. Thus the inductive hypothesis applies and we conclude that the three vectors on the left are dependent. Thus for some elements γ_2, γ_3, γ_4 of k, not all zero, we have $0 = \gamma_2(y_2 - r_1y_1) + \gamma_3(y_3 - s_1y_1) + \gamma_4(y_4 - t_1y_1)$. Collecting the y_1 terms gives $0 = \gamma_1y_1 + \gamma_2y_2 + \gamma_3y_3 + \gamma_4y_4$ [where $\gamma_1 = -\gamma_2 r_1 - \gamma_3s_1 - \gamma_4 t_1$]. This is a non trivial linear combination since not all of γ_2, γ_3, γ_4, are zero. Hence T is dependent. QED.

Cor: If $S = \{x_1,\ldots,x_n\}$ is a basis for a subspace of V, then that subspace has dimension n.

The lemma above leads easily to the following properties:
Definition: A "subspace" of V is a subset which is also a vector space under the same operations as in V.

Theorem: If V has dimension n, then:
i) more than n vectors in V are always dependent;
ii) fewer than n vectors cannot span V;
iii) every basis of V has exactly n vectors;
iv) every set of n independent vectors in V spans V, hence is a basis;
v) every set of n vectors that spans V is independent, hence a basis;
vi) every maximal set of independent vectors in V has exactly n vectors in it;
vii) every minimal set of spanning vectors for V has exactly n vectors in it;
viii) every independent subset of V is contained in a basis;
ix) every spanning set for V contains a basis;
x) a subspace of V cannot have dimension greater than n;
xi) a proper subspace of V has dimension less than n;
xii) a k-isomorphism $f:V \to W$ carries a basis of V to a basis of W, hence W also has dimension n.
[Proofs of viii), ix) seem to require the axiom of choice.]

Advice: You should be able to prove all of these statements.

Remark: All vector spaces are examples of a "free" construction. I.e. a vector space V is "free" on the set S iff i) $S \subset V$, and ii) for any vector space W, every function $f:S \to W$ extends uniquely to a k-homomorphism $V \to W$.

Exercise #59) V is "free" on $S \subset V$ iff S is a basis for V.

Remark: Every k-algebra is a k-vector space. In particular, if $k \subset K$ is an extension of fields, then K is a k algebra and therefore also a k-vector space.

Definition: The k dimension of K is called the <u>degree of the extension</u> and denoted [K:k].

Theorem: Given $k \subset K \subset L$, the degree of successive extensions is multiplicative, i.e. [L:k] = [L:K][K:k].
proof: Assume $x_1,\ldots,x_n$ are k-independent elements of K, and $y_1,\ldots,y_m$ are K-independent elements of L.
Claim 1: The products $\{x_iy_j\}$ are k-independent elements of L.
proof of claim 1: If $\Sigma a_{ij}x_iy_j = 0$ in L, we must show all $a_{ij} = 0$. Rewriting the sum we have $\Sigma_j(\Sigma_i a_{ij}x_i)y_j = 0$. But the y_j are K-independent, and the coefficients $(\Sigma_i a_{ij}x_i)$ belong to K, so these coefficients are all zero. Then $\Sigma_i a_{ij}x_i = 0$, the x_i are k-independent, while the a_{ij} are all in k, so all $a_{ij} = 0$.

Assume $x_1,\ldots,x_n$ are elements of K which span K over k, and $y_1,\ldots,y_m$ are elements of L which span L over K.
Claim 2: The products $\{x_iy_j\}$ span L over k.
proof of claim 2: If z is in L then $z = \Sigma_j b_jy_j$ for some b_j in K. Then each $b_j = \Sigma_i a_{ij}x_i$ for some a_{ij} in k. Thus $z = \Sigma_j(\Sigma_i a_{ij}x_i)y_j = \Sigma_{ij} a_{ij}(x_iy_j)$. **QED theorem.**

Remarks: (i) This proves also that [L:k] is infinite iff one of the degrees [L:K] or [K:k] is infinite, since if there are arbitrarily many independent x's or y's, we have proved there are also arbitrarily many independent products xy.
(ii) The k-dimension of an extension $k \subset K$ will be very useful in understanding the extension, as we will see in the next section.

§16) Theory of algebraic field extensions

Definition: A field extension $k \subset K$ is called "algebraic" provided every element of K satisfies a polynomial equation f(x)=0, where f has coefficients in k. More generally an *element* of K is called

algebraic over k iff it satisfies such a polynomial, and then K is algebraic over k iff every element of K is algebraic over k. An element of k which is not algebraic over k is called "transcendental" over k.

Examples: The element $2^{1/3}$ of $\mathbb{R}$ is algebraic over $\mathbb{Q}$ since it satisfies the polynomial X^3-2 with rational coefficients. Indeed if a is any element of $\mathbb{Q}$, then any complex nth root $a^{1/n}$ of a is algebraic over $\mathbb{Q}$, since it satisfies $X^n-a=0$. It is not so easy to prove, but the element π of $\mathbb{R}$ is transcendental over $\mathbb{Q}$.
If you know about the theory of countable and uncountable sets, it is not very hard to show that the set of all elements of $\mathbb{R}$ which are algebraic over $\mathbb{Q}$ is countable. [For each n, there are only countably many polynomials of degree n over $\mathbb{Q}$, each with at most n roots, hence only countably many roots of polynomials of degree n. The union over all n, is a countable union of countable sets hence countable.] Since $\mathbb{R}$ is uncountable, there are uncountably infinitely many transcendental elements of $\mathbb{R}$ over $\mathbb{Q}$, but the hard part is to recognize one.
If L is a field containing k[X], such as the field of rational functions of X, then X is not algebraic over k, since a polynomial f(X) is never equal to zero unless all the coefficients are zero. It follows that the map $\mathbb{Q}[X]\to\mathbb{R}$ sending X to π, and f(X) to $f(\pi)$, is an isomorphism from $\mathbb{Q}[X]$ onto the $\mathbb{Q}$-sub algebra of $\mathbb{R}$ generated by π. I.e. the ring of polynomials in π over $\mathbb{Q}$, is isomorphic to the ring of polynomials in X over $\mathbb{Q}$!

Definition/Theorem: If α in K is algebraic over $k\subset K$, then there is a unique monic irreducible polynomial over k satisfied by α, called the "minimal polynomial of α over k". This is the unique monic polynomial of least degree satisfied by α over k.
proof: Consider the k algebra map $\varphi: k[X]\to K$ sending X to α, and thus f(X) to $f(\alpha)$. Since α is algebraic, some non trivial f goes to zero by this map, hence $\ker(\varphi)\neq 0$. Thus $\ker(\varphi) = (f)$ is a principal ideal generated by some unique monic f. Moreover $k[X]/(f) \cong \mathrm{Im}(\varphi)\subset K$ is a subring of a field hence an integral domain. Thus the product of two non zero elements of k[X]/(f) is again non zero. Since [g] = [0] iff f divides g, this means that if f divides neither g nor h in k[X], then f does not divide gh either. Consequently f is irreducible, since if f = gh then f divides f=gh, so f divides either g or h. Thus either h or g

is a unit, and f is irreducible. QED.

Cor: If α in K is algebraic over $k \subset K$, then $k(\alpha) \cong k[X]/(f)$ (isomorphic as k-algebras) where f is the minimal polynomial of α over k.
proof: We just saw that the k algebra map $\varphi: k[X] \to K$ induces an isomorphism $k[X]/(f) \cong Im(\varphi) = k[\alpha] \subset K$, of $k[X]/(f)$ onto the k algebra $k[\alpha]$ of all polynomials in α. Since $k[X]/(f)$ is a field, so is $k[\alpha]$, i.e. the ring $k[\alpha] = k(\alpha)$ is already a field, the subfield of K generated by α. QED.

Lemma: If f in k[X] has degree n, then the vector space k[X]/(f) has k-dimension n.
proof: Any polynomial g(X) in k[X] can be divided by f to leave a remainder of degree $< n$, i.e. $g = fh + r$ for some r of degree $< n$. Then in $k[X]/(f)$, $[g] = [r] = [a_0 + a_1X + \ldots + a_{n-1}X^{n-1}]$, so the n elements $[1]$, $[X]$, $\ldots [X^{n-1}]$, span the space k[X]/(f) over k. Moreover they are independent, since if $[0] = a_0[1] + a_1[X] + \ldots + a_{n-1}[X^{n-1}] = [a_0 + a_1X + \ldots + a_{n-1}X^{n-1}]$, then f divides $a_0 + a_1X + \ldots + a_{n-1}X^{n-1}$, which is impossible since degree(f) = n. QED.

Cor: If α in K is algebraic over $k \subset K$, with minimal polynomial f over k of degree n, then $k(\alpha)$ has k-dimension n.
proof: The isomorphism $k(\alpha) \cong k[X]/(f)$ is one of k-algebras [i.e. a ring isom. which is the identity on k], hence also of k-vector spaces. The elements $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ thus form a k-basis of $k(\alpha)$. QED.

Remark: It is not hard to show that $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2}$, for a,b, in $\mathbb{Q}\}$, $\mathbb{Q}(\sqrt{3}) = \{a+b\sqrt{3}\}$, for a,b, in $\mathbb{Q}\}$, $\mathbb{Q}(i) = \{a+bi$, for a,b, in $\mathbb{Q}\}$, are fields directly by "rationalizing" and thus writing down inverses of their elements. For example, if a,b, are rational but not both zero, $(a+bi)^{-1} = (a-bi)/a^2+b^2)$, $(a+b\sqrt{2})^{-1} = (a-b\sqrt{2})/a-2b^2$, where in the first case the denominator is positive, and in the second is non zero since 2 has no rational square root.

To show directly that $\mathbb{Q}(2^{1/3}) = \{a + b\,2^{1/3} + c\,2^{2/3}$, where a,b,c, are in $\mathbb{Q}\}$ is a field, one can solve some linear equations for the inverse formula $(a + b\,2^{1/3} + c\,2^{2/3})^{-1} =$
$\{(a^2-2bc) + 2^{1/3}(2c^2-ab) + 2^{2/3}(b^2-ac)\} / (a^3+2b^3+4c^3-6abc)$, but

this is not a proof that the element is invertible unless we prove that this denominator is non zero. Here is a proof by Ken Berenhaut by the "method of descent" [take a minimal answer and make it smaller]. So assume there is, a solution of $(a^3+2b^3+4c^3-6abc) = 0$, with a, b, c rational, not all zero. By multiplying through by a large integer, one can assume the solutions are all integers, and then by dividing out their gcd, one can assume the gcd of a, b, c is 1. The trick now is to show that all of them are even, a contradiction. Looking at the equation we see all terms but a^3 are even, hence a^3 is even, hence a is even, hence a^3 is actually divisible by 8. Looking again now we see that all terms but $2b^3$ are divisible by 4, hence so is this one, so b^3 is even, hence b is even, hence $2b^3$ is divisible by 16. Hence every term but $4c^3$ is divisible by 8, so c^3 is even and c is even. Thus a,b,c, are all even, a contradiction. Hence our formula has non zero denominator unless all three of a,b,c, are zero. QED. [You might try finding inverses of elements of $Q(e^{2\pi i/3})$ directly.]

Lemma: k[X] has infinite dimension over k.
proof: For any n, the elements $1, X, \ldots, X^n$, are independent over k, since a linear combination $a_0 + a_1X + \ldots + a_{n-1}X^n$ cannot be zero in k[X] unless all a's are zero, by definition of equality of polynomials. QED.

The MAIN POINT for proving an extension is algebraic:
Cor: Given $k \subset K$ and α in K, α is algebraic over k iff $k(\alpha)$ has finite dimension over k.
proof: We know α is algebraic over k iff $f(\alpha) = 0$ for some non trivial polynomial f over k, hence iff the map $\varphi: k[X] \to K$ sending f(X) to $f(\alpha)$ has non trivial kernel. But $\mathrm{Im}(\varphi) \subset k(\alpha)$ by construction, so if $k(\alpha)$ is finite dimensional, than since k[X] is infinite dimensional, the map φ cannot be injective. We have already seen above that if α is algebraic with minimal polynomial f, then $k(\alpha)$ has (finite) dimension = degree(f). QED.

Definition: A field extension $k \subset K$ is called finitely generated/k iff $K = k(\alpha_1, \ldots, \alpha_n)$, i.e. K is generated over k by a finite set.

Theorem: $k \subset K$ is finite dimensional, or simply "finite", iff K is both algebraic and finitely generated k.

proof: If K is finite dimensional, and α is any element of K, then, as above, the map $\varphi: k[X] \to K$ sending $f(X)$ to $f(\alpha)$ is never injective since $k[X]$ is infinite dimensional. Hence every α is algebraic over k. Moreover, if we choose any element α in K-k, and adjoin it to k, then $k(\alpha)$ has k-dimension ≥ 2. If $k(\alpha) \neq K$ then choose another element β in $K-k(\alpha)$, and adjoin β to $k(\alpha)$ getting $k(\alpha,\beta)$. Since $k(\alpha) \subset k(\alpha,\beta)$ is a proper subspace, dim. $k(\alpha) <$ dim. $k(\alpha,\beta)$. Proceeding in this fashion, we eventually get $k(\alpha,\beta,\ldots,\gamma) \subset K$ and dim. $k(\alpha,\beta,\ldots,\gamma) \geq$ dim. K. Then the dimensions must be equal, and hence $k(\alpha,\beta,\ldots,\gamma)=K$. Thus K is also finitely generated over k.

If on the other hand, K is finitely generated and algebraic over k, then $k(\alpha,\beta,\ldots,\gamma) = K$, where each element $\alpha,\beta,\ldots,\gamma$ is algebraic over k. Hence we have a tower of extensions $k \subset k(\alpha) \subset k(\alpha)(\beta) \subset \ldots \subset k(\alpha,\beta\ldots)(\gamma) = K$. Each intermediate field is finite dimensional over the previous one, so the degree of the top one over the bottom one is the product of the intermediate degrees, hence finite. QED.

Definition: If $k \subset K$, and α is in K, the k-subalgebra generated by α in K is by definition the image of the map $k[X] \to K$ taking $f(X)$ to $f(\alpha)$.

Important remark: Finitely generated extensions are not finite dimensional if they are not algebraic. I.e. If α in K is transcendental over k, then α generates an infinite dimensional k subalgebra: $K \supset k[\alpha] \cong k[X]$. On the other hand, even an algebraic extension is not finite dimensional if it is not finitely generated. Eg. if $\bar{\mathbf{Q}}$ denotes the set of all complex numbers algebraic over $\mathbf{Q}$, then $\mathbf{Q} \subset \bar{\mathbf{Q}}$ is algebraic, but infinite dimensional. Thus in order to use the previous corollary for proving an infinite extension is algebraic, one must reduce somehow to considering finitely generated subextensions.

<u>We will only consider Galois groups of finite extensions.</u>

Definition: If $k \subset K$ is a "finite", i.e. finite dimensional, extension of fields, define its Galois group $G_k(K) = G(K/k) = Gal_k(K) =$ (all field automorphisms of K which restrict to the identity on k) = the set of "k-automorphisms" of K, with composition as group operation.

Remark: If K, L are finite extensions of k and $f: K \to L$ is a field automorphism which is the identity on k then f is also a k-vector

space isomorphism, hence $[K:k] = [L:k]$. In particular, $G_k(K)$ is a subgroup of the group of k-vector space automorphisms of K.

§17) Examples of algebraic field extensions

Example: The extension $\mathbb{R} \subset \mathbb{C}$ is finite, hence algebraic.
proof: Since $\mathbb{C}$ is spanned over $\mathbb{R}$ by the two elements $\{1,i\}$, $\mathbb{C}$ is two dimensional over $\mathbb{R}$ hence algebraic. But we can also easily find polynomials satisfied over $\mathbb{R}$ by any given elements of $\mathbb{C}$ as follows. If $z = a+bi$ is any complex number, then $z\bar{z} = a^2+b^2$ is real, and $z + \bar{z} = 2a$ is real, so z is a root of the real polynomial $(x-z)(x-\bar{z}) = x^2 - 2ax+(a^2+b^2)$. Hence $\mathbb{C}$ is algebraic over $\mathbb{R}$. QED.

The previous argument suggests that complex conjugation plays an important role in understanding the extension $\mathbb{R} \subset \mathbb{C}$. One reason for this is the following result:
Theorem: The Galois group of $\mathbb{R} \subset \mathbb{C}$, is $G(\mathbb{C}/\mathbb{R}) = \{id, z \mapsto \bar{z}\} \cong \mathbb{Z}_2$.
proof: The map $z \mapsto \bar{z}$, complex conjugation, is an $\mathbb{R}$-automorphism of $\mathbb{C}$, i.e. it preserves addition, multiplication, leaves the reals fixed, and is its own inverse. So it does belong to the Galois group. But why are there no other elements? Recall the elementary result:

Fact: If $f(x)$ is a polynomial with real coefficients, and if z is a complex "root" of f [i.e. a solution of $f(x) = 0$], then $\bar{z}$ is also a root.
proof: If $f(x) = \Sigma\, a_j x^j$, and $0 = f(z) = \Sigma\, a_j z^j$, then $0 = \bar{0} = (\Sigma\, a_j z^j)^- = \Sigma\, a_j \bar{z}^j = f(\bar{z})$. Hence $\bar{z}$ is also a root. QED.

The proof of the Fact also proves the theorem. I.e. let φ be any $\mathbb{R}$ automorphism of $\mathbb{C}$: The argument just given shows that if z is a root of a polynomial with real coefficients, then $\varphi(z)$ is also a root. I.e. $0 = f(z) = \Sigma\, a_j z^j$, so $0 = \varphi(0) = \varphi(\Sigma\, a_j z^j) = \Sigma\, a_j \varphi(z)^j$. Applying this fact to the polynomial x^2+1, we see, since the only complex roots of x^2+1 are $\{i, -i\}$, that if φ is any $\mathbb{R}$ automorphism of $\mathbb{C}$ then we must have either $\varphi(i) = i$, or $\varphi(i) = -i$. Since every element of $\mathbb{C}$ has form $a+bi$, with a, b real, then $\varphi(a+bi) = a+b\varphi(i)$ and hence φ is one of the two automorphisms $\{id, z \mapsto \bar{z}\}$. QED.

Cor: Exactly the same proof shows $G(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}_2$.

The principle we have encountered here is so important we state it:
Theorem: If $k \subset K$ is a field extension, α is a root in K of a polynomial f with coefficients in k, and φ is an element of $G_k(K)$, then $\varphi(\alpha)$ is also a root of f in K.
Proof: We know this proof by now. QED.

Theorem: $G(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}2$.
proof: We can try to imitate the previous argument.
I.e. Since $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2}$, for a,b rational$\}$, if φ is in $G(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ then $\varphi(a+b\sqrt{2}) = \varphi(a) + \varphi(b)\varphi(\sqrt{2}) = a+b\varphi(\sqrt{2})$, so φ is determined by $\varphi(\sqrt{2})$. Next, since $\sqrt{2}$ is a root of X^2-2, $\varphi(\sqrt{2})$ must also be a root of that polynomial. Hence we must have $\varphi(\sqrt{2}) = \sqrt{2}$ or $-\sqrt{2}$. Thus there are at most two $\mathbb{Q}$ automorphisms of $\mathbb{Q}(\sqrt{2})$. We claim there are two of them, namely the identity taking $\sqrt{2}$ to $\sqrt{2}$, and the map taking $a+b\sqrt{2}$ to $a-b\sqrt{2}$. So we must check the latter is an automorphism. It preserves addition since if $\varphi(a+b\sqrt{2}) = a-b\sqrt{2}$, and $\varphi(c+d\sqrt{2}) = c-d\sqrt{2}$, then $\varphi((a+b\sqrt{2}) + (c+d\sqrt{2})) = \varphi((a+c) + (b+d)\sqrt{2}) = (a+c) - (b+d)\sqrt{2} = (a-b\sqrt{2}) + (c-d\sqrt{2}) = \varphi(a+b\sqrt{2}) + \varphi(c+d\sqrt{2})$.
It also preserves multiplication since $\varphi((a+b\sqrt{2})(c+d\sqrt{2})) = \varphi((ac+2bd) + (ad+bc)\sqrt{2}) = (ac+2bd) - (ad+bc)\sqrt{2}) = (a-b\sqrt{2})(c-d\sqrt{2}) = \varphi(a+b\sqrt{2})\,\varphi(c+d\sqrt{2})$. QED.

Of course $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2}$, for a,b rational$\}$ has dimension 2 over $\mathbb{Q}$, hence is algebraic, but suppose we look for polynomials satisfied by elements of the field $\mathbb{Q}(\sqrt{2})$. We might as well try to imitate the construction used for $\mathbb{C}$ over $\mathbb{R}$. I.e. let $z = a+b\sqrt{2}$, for a,b rational, be a given element of $\mathbb{Q}(\sqrt{2})$, let $z^* = a-b\sqrt{2}$, and notice that $z+z^* = 2a$, and $zz^* = a^2-2b^2$, are both in $\mathbb{Q}$. Hence z satisfies the polynomial $(X-z)(X-z^*) = X^2 - 2aX + (a^2-2b^2)$, which has coefficients in $\mathbb{Q}$.

Similarly, the Galois group of $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ is isomorphic to $\mathbb{Z}2$, generated by a conjugation automorphism taking $a+b\sqrt{3}$ to $a-b\sqrt{3}$, and the same trick works to find explicit polynomials satisfied by elements of $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$.

Remark: Since all three fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(i)$, have isomorphic Galois groups, it is conceivable that they are actually isomorphic fields, but this is in fact not the case.

Proposition: No two of $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(i)$, are isomorphic over $\mathbf{Q}$.
proof: I.e. suppose $f: \mathbf{Q}(\sqrt{2}) \to \mathbf{Q}(\sqrt{3})$ were a $\mathbf{Q}$ isomorphism. Since $(\sqrt{2})^2 = 2$, then also $(f(\sqrt{2}))^2 = f(2) = 2$. So $f(\sqrt{2}) = a+b(\sqrt{3})$ must be a square root of 2. However if $(a+b(\sqrt{3}))^2 = (a^2+3b^2) + 2ab\sqrt{3} = 2$, then $2ab\sqrt{3} = 2 - (a^2+3b^2)$ is a rational number. Since $\sqrt{3}$ is irrational, the only way $2ab\sqrt{3}$ can be rational is if $2ab = 0$. Hence either a or b is zero. But then we must have either $a^2 = 2$, or $3b^2 = 2$. We know $a^2 = 2$ is impossible since $\sqrt{2}$ is irrational, and if $3b^2 = 2$, then $b^2 = (2/3)$. This is also impossible, since for example if $b = n/m$ is rational in lowest terms, then $b^2 = n^2/m^2$ is also in lowest terms, so if $b^2 = n^2/m^2 = 2/3$, then by uniqueness of a lowest terms expression, we have $n^2 = 2$, and $m^2 = 3$, where n,m are integers But both equations are impossible.
A similar argument shows neither field is isomorphic to $\mathbf{Q}(i)$. You should carry out at least one of these arguments. QED.

Now consider $\mathbf{Q}(2^{1/3}) = \{a + b\cdot 2^{1/3} + c\cdot 2^{2/3}: a,b,c \text{ in } \mathbf{Q}\}$. This extension of $\mathbf{Q}$ in fact has *no* interesting $\mathbf{Q}$- automorphisms. I.e.:

Proposition: $G(\mathbf{Q}(2^{1/3})/\mathbf{Q}) = \{id\}$.

proof: Let f be any $\mathbf{Q}$ automorphism of $\mathbf{Q}(2^{1/3})$. Since $2^{1/3}$ is a root of the polynomial X^3-2, $f(2^{1/3})$ must also be root of the same polynomial. Unfortunately the other two roots of this polynomial are complex, while all elements of the field $\mathbf{Q}(2^{1/3})$ are real. Thus the only root of X^3-2 in $\mathbf{Q}(2^{1/3})$ is $(2^{1/3})$. Hence we must have $f(2^{1/3}) = 2^{1/3}$. We claim f is the identity on all of $\mathbf{Q}(2^{1/3})$. I.e. consider the subset of $\mathbf{Q}(2^{1/3})$ on which f equals the identity. If $f(a) = a$, and $f(b) = b \neq 0$, then $f(a-b) = a-b$, and $f(a/b) = a/b$, so this set is closed under subtraction and division. Since f is a $\mathbf{Q}$ automorphism, this set also contains $\mathbf{Q}$. Hence this set is a field. Since $f(2^{1/3}) = 2^{1/3}$, this set is a field containing both $\mathbf{Q}$ and $2^{1/3}$. By definition of $\mathbf{Q}(2^{1/3})$ as the intersection of all such fields, we get that $\mathbf{Q}(2^{1/3})$ is contained in the field where f is the identity. Thus f is the identity automorphism of $\mathbf{Q}(2^{1/3})$, and $G(\mathbf{Q}(2^{1/3})/\mathbf{Q}) = \{id\}$. QED.

Thus the Galois group of $\mathbf{Q}(2^{1/3})$ is absolutely no help in finding actual polynomials over $\mathbf{Q}$ satisfied by elements of this field. We can still do something with our bare hands though. At least we know $\mathbf{Q}(2^{1/3}) = \{a + b\cdot 2^{1/3} + c\cdot 2^{2/3}: a,b,c \text{ in } \mathbf{Q}\}$, is a 3 dimensional, algebraic extension of $\mathbf{Q}$. Thus every element in $\mathbf{Q}(2^{1/3}) = \{a + b\cdot 2^{1/3} + c\cdot 2^{2/3}: a,b,c \text{ in } \mathbf{Q}\}$, satisfies a polynomial of degree at most three over $\mathbf{Q}$. Of course $2^{1/3}$ satisfies the polynomial X^3-2 over $\mathbf{Q}$, but what about the elements $1+2^{1/3}$, $3+2^{1/3}$, $1+2^{1/3}+2^{2/3}$, $2-3\,(2^{1/3})+5\,(2^{2/3})$, or more generally $(a + b\cdot 2^{1/3} + c\cdot 2^{2/3})$?

Remark: Our experience with computing inverses suggests that these computations may be lengthy, since the problem of finding polynomials satisfied by a given element contains the finding of the inverse of that element as a subproblem: i.e. if $a+b\alpha+c\alpha^2+d\alpha^3 = 0$, and $a\neq 0$, then we get the inverse of α as follows: first $a = -b\alpha-c\alpha^2-d\alpha^3$, so $1 = -(b/a)\alpha - (c/a)\alpha^2 -(d/a)\alpha^3 = \alpha\,[-(b/a) - (c/a)\alpha -(d/a)\alpha^2]$, and thus the second factor on the right hand side is the inverse of α. If $a = 0$, then $b\alpha+c\alpha^2+d\alpha^3 = \alpha(b+c\alpha+d\alpha^2] = 0$, and since $\alpha \neq 0$ (or else we would not be trying to find its inverse) we can repeat the argument with the equation $[b+c\alpha+d\alpha^2] = 0$. In other words, the point is to start with the polynomial of smallest degree satisfied by $\alpha \neq 0$, which is sure to have a non zero constant term.
Still the problem must only be one of linear algebra. Lets try finding a polynomial satisfied by $\alpha = 1+2^{1/3}$. The four elements $1,\alpha,\alpha^2,\alpha^3$ must be dependent in the 3 dimensional space $\mathbf{Q}(2^{1/3})$. We compute: $\alpha^2 = 1+2(2^{1/3})+2^{2/3}$, and $\alpha^3 = 3+3(2^{1/3})+3(2^{2/3})$. Now if we stop writing the actual basis vectors $\{1, 2^{1/3}, 2^{2/3}\}$ of $\mathbf{Q}(2^{1/3})$ and write instead only the coefficients, we can represent the vectors $1,\alpha,\alpha^2,\alpha^3$ as the coordinate vectors (1,0,0), (1,1,0), (1,2,1), (3,3,3). Then we can do row reduction or some such calculation on the matrix with these columns, and find that (3,3,3) = 3(1,2,1) - 3(1,1,0) + 3(1,0,0). Hence $\alpha^3 = 3\alpha^2-3\alpha+3$, and $\alpha^3 - 3\alpha^2 + 3\alpha-3 = 0$.

An easier solution by E. Croot and Scott: since we know that $\beta = 2^{1/3}$ satisfies X^3-2, then for $\alpha = 1+2^{1/3}$, we have $\beta = \alpha-1$, so $\alpha-1$ also satisfies $X^3-2 = 0$, i.e. $(\alpha-1)^3-2 = \alpha^3-3\alpha^2+3\alpha-3 = 0$, the same

answer as above. Using the easy way again, we can deal also with $\alpha = 3+2^{1/3} = 3+\beta$, where $\beta = 2^{1/3}$ again, hence $\beta = \alpha-3$, and thus $(\alpha-3)^3-2 = 0$, i.e. $\alpha^3-9\alpha^2+27\alpha-29 = 0$.

If $\alpha = 1+2^{1/3}+2^{2/3}$, a similar trick seems to work, i.e. let $\beta = 2^{1/3}$, so $\alpha = 1+\beta+\beta^2$, then multiply by $(1-\beta)$ to get $\alpha(1-\beta) = 1-\beta^3 = 1-2 = -1$, so $1-\beta = -1/\alpha$, and $\beta = (\alpha+1)/\alpha$. Thus $0 = \beta^3-2 = (\alpha+1)^3/\alpha^3 - 2$, so $(\alpha+1)^3 - 2\alpha^3 = 0$, i.e. $\alpha^3+3\alpha^2+3\alpha+1-2\alpha^3 = -\alpha^3+3\alpha^2+3\alpha+1 = 0$.

What about the general case, $\alpha = a+b(2^{1/3})+c(2^{2/3})$? [Much later], computing by hand I got $\alpha^3-3a\alpha^2+(3a^2-6bc)\alpha-(a^3+2b^3+4c^3-6abc) = 0$, which seems to work. Note it is monic, hence non trivial. Lets check it on the last case. I.e. for $\alpha = 2-3\,(2^{1/3})+5\,(2^{2/3})$, since $a = 2$, $b = -3$, $c = 5$, I get $\alpha^3-6\alpha^2+(102)\alpha-634 =$
$(8-54+500-360)-6(-56)+(204)\ -634\ +$
$\{(-36+270+300)\ -6(-12+50)\ -306\}2^{1/3}\ +$
$\{(60+54-450)\ -6(20+9)+510\}2^{2/3} = 0+0(2^{1/3})+\ 0(2^{2/3}) = 0$. Hooray!

Easier solution (by Gang Yu): If $x = a+b(2^{1/3})+c(2^{2/3})$, then
$(x-a)^3 = 2(b+c\cdot 2^{1/3})^3 = 2(b^3+4c^3+6b^2c\cdot 2^{1/3}+3bc^2\cdot 2^{2/3})$
$= 2b^3+4c^3+6bc(x-a)$. Hence, x satisfies $f(x) =$
$(x-a)^3-6bc(x-a)-2b^3-4c^3 = 0$.

We see that finding specific polynomials satisfied by individual elements is not trivial but it is possible, and we have a nice theoretical condition for when they exist. Moreover when we know the Galois group, at least in the case of quadratic extensions, the automorphisms seem to help us find the polynomials. When a field extension does not have enough automorphisms, i.e. when the Galois group is not big enough, there is still a problem.

Exercise #60) Compute the inverses in the form $a+b3^{1/3}+c3^{2/3}$, of the elements $2+3^{1/3}$, and $1-3^{1/3}+3^{2/3}$, of the field $\mathbf{Q}(3^{1/3})$; and of the element $2^{1/2}+3^{1/2}$ in the field $\mathbf{Q}(2^{1/2},3^{1/2})$

Exercise #61) Find polynomials over $\mathbf{Q}$ satisfied by the elements $2 + 3^{1/3}$, $1 - 3^{1/3} + 3^{2/3}$, and $2^{1/2} + 3^{1/2}$.

§18) Construction of the Galois group functor

We need to know more about Galois groups. We need to know when they are large enough to do us any good, but from our earlier discussion of Galois' ideas, and from general principles, we should have faith that the most fundamental issue is the following:
Question: Is the Galois group a functor? I.e. can we compare Galois groups of comparable fields? If $k \subset K$ and $F \subset L$ are field extensions, a homomorphism from $k \subset K$ to $F \subset L$ should surely be defined as a homomorphism $K \to L$ which maps k into F, but the main question is whether such a homomorphism induces a group homomorphism between the Galois groups $G_k(K)$ and $G_F(L)$.

To keep the analysis as simple as possible, we restrict attention to extensions of a fixed base field k, and since all field maps are injective, we don't lose any more generality by restricting attention further to inclusions of fields. Thus we assume we have a sequence of inclusions $k \subset K \subset L$, and ask whether there is an induced homomorphism of groups between $G_k(K)$ and $G_k(L)$. If we have an automorphism of K fixing k, to get a homomorphism of L we would have to extend the automorphism of K to one of the larger field L. It is unclear how to define such an extension, and even if we could see how to define it, there is no reason why such an extension should be unique. So let's try going the other way, from an automorphism of the larger field L to one of the smaller field K. Here the definition is almost automatic, simply restrict the automorphism $\varphi: L \to L$ to K. Since φ fixes k, so will the restriction. Still there is a problem, since there is no reason for the restriction $\varphi: K \to L$ to have image equal to K. I.e. the restriction $\varphi: K \to L$ will be an injection of K into L that fixes k, but why should it be an automorphism of K? There does not seem to be any reason it will be. Since we are stuck otherwise, we will agree to consider only those inclusions $k \subset K$ for which all k automorphisms of larger fields always restrict to k automorphisms of K. Since we are also interested primarily in fields obtained by adjoining solutions of polynomials, and we need to use concepts of finite dimensionality, we make the further restriction that our extension fields are finite.

Definition: A finite (hence algebraic) field extension $k \subset K$ is called "normal" provided for every inclusion $K \subset L$ in a larger field, every k-homomorphism $\varphi: K \to L$ maps K isomorphically onto itself.

Cor: If we consider the category of normal extensions of k, the Galois group is a functor from that category to the category of groups.

The trouble is we don't know yet whether there are any normal extensions of k other than $k \subset k$. We begin by producing one example.
Theorem: The extension $\mathbb{R} \subset \mathbb{C}$ is normal.
proof: This is almost the same argument we have used above. If $\mathbb{C} \subset L$ is any inclusion of fields, and $\varphi: \mathbb{C} \to L$ is any $\mathbb{R}$ homomorphism, then $\varphi(i)$ is a root of the polynomial x^2+1. Since x^2+1 factors as $(x-i)(x+i)$ over L, then for any element α of L we have $\alpha^2+1 = (\alpha-i)(\alpha+i) = 0$ iff $\alpha=i$ or $\alpha=-i$. Hence the only roots of x^2+1 in L are i,-i. Thus we know $\varphi(i) = i$ or $-i$. Hence $\varphi(a+bi)$ = either $a+bi$ or $a-bi$, and in particular, φ is an automorphism of $\mathbb{C}$. Also $[\mathbb{C}:\mathbb{R}] = 2$. QED.

Definition: If f is a polynomial of degree n over k, and $k \subset K$ is an extension field a set of elements $\{a_1,\ldots,a_n\}$ in K, not necessarily all different, is called a "full system of roots" of f provided f factors over K into linear factors as $f(x) = c\Pi(x-a_j)$, $j=1,\ldots,n$, where c is in $k-\{0\}$.

Remark: If $\{a_1,\ldots,a_n\}$ is a "full system of roots" of f in K, then f has no other roots in K, since $f(\beta) = c\Pi(\beta-a_j) = 0$ iff b = some α_j. If f has degree n, and if $\{a_1,\ldots,a_n\}$ is a set of n distinct roots then it is a full system of roots of f by the root/factor theorem.

Definition: If K is *generated* over k by a full system of roots for some k polynomial f, then K is called a "splitting field" for f over k, [f splits into linear factors over K, but not over any smaller field].

The next result provides plenty of normal field extensions:
Theorem: If $k \subset K$ and K is a splitting field for some polynomial f in k[X], then $k \subset K$ is normal.
proof: Assume $K \subset L$, and that $\varphi: K \to L$ is a k-homomorphism.
1) If $\{a_1,\ldots,a_n\}$ is a "full system of roots" of f in K, then f has no other roots in K. By our usual argument φ permutes the roots of f. Thus $\varphi(\{a_1,\ldots,a_n\}) = \{a_1,\ldots,a_n\}$. Consequently $\varphi(K)$ is a subfield of L containing k and $\{a_1,\ldots,a_n\}$. Since K is the smallest such field, $K \subset \varphi(K)$. On the other hand since $\varphi(k) \subset K$ and $\varphi(\{a_1,\ldots,a_n\}) \subset K$, $\varphi^{-1}(K)$ is a subfield of K containing k and $\{a_1,\ldots,a_n\}$. Since K is the smallest such field, $K \subset \varphi^{-1}(K)$. Hence $\varphi(K) \subset K$, so $\varphi(K) = K$ as desired.

2) Finally, since K is generated over k by $(a_1,\ldots,a_n)$, each of which is a root of f, K is algebraic and finitely generated/k hence finite. QED.

Cor: The extensions $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(i)$, $\mathbf{Q}(\omega)$, $\mathbf{Q}(2^{1/3}, \omega)$ are all normal /$\mathbf{Q}$, where $\omega = e^{2\pi i/3}$.
proof: These are respectively the splitting fields of X^2-2, X^2-3, X^2+1, X^3-1, X^3-2, over $\mathbf{Q}$. QED.

Exercise #62) Compute the Galois groups of $\mathbf{Q}(\omega)$, $\mathbf{Q}(2^{1/3}, \omega)$ over $\mathbf{Q}$, where $\omega = e^{2\pi i/3}$.

Exercise #63) Compute the Galois groups of (the splitting fields of) : (X^4-1), (X^5-1), (X^6-1), (X^7-1) over $\mathbf{Q}$. Can you guess $G_{\mathbf{Q}}(X^n-1)$?
Exercise #64) Prove that $\mathbf{Q}(2^{1/3})$ is *not* normal, over $\mathbf{Q}$.

Exercise #65) If α is a complex number, algebraic of degree n over $\mathbf{Q}$, i.e. its minimal polynomial over $\mathbf{Q}$ has degree n, then there exist n distinct $\mathbf{Q}$-homomorphisms of $\mathbf{Q}(\alpha)$ into $\mathbf{C}$.

§19) Extending field homomorphisms

Now we know that if $K \subset L$ are two (finite) normal extensions of k, there is a restriction homomorphism of Galois groups $G_k(L) \to G_k(K)$. We know nothing about this homomorphism however. For instance when is it injective or surjective? To answer such questions and others, we will study how to define a k-homomorphism out of a field $k(\alpha,\beta,\ldots\gamma)$, by extending the homomorphism from k to $k(\alpha)$, then to $k(\alpha,\beta)$, and so on until it is defined on all of $k(\alpha,\beta,\ldots,\gamma)$. This will be our primary tool for understanding field embeddings and field automorphisms.

First we do a warm-up exercise:
Proposition: $\mathbf{Q} \subset \mathbf{Q}(2^{1/3})$ is NOT a normal extension.

Remark: Recall we know that a field generated by a full system of roots of a polynomial over the base field is normal over the base field. Hence we would expect that to get a *non* normal extension we would adjoin some, but not all, of the roots of an irreducible polynomial. "Irreducible" is important here. For instance, adjoining

only the roots {i,-i} of the polynomial X^8-1, would still give a normal extension, since {i,-i} constitute a full system of roots for the polynomial X^2+1, a factor of X^8-1.

proof of Prop: We will show there are field homomorphisms $\mathbb{Q}(2^{1/3})\to\mathbb{C}$ with image not contained in $\mathbb{Q}(2^{1/3})$. First recall the basic result, that given $K\subset L$, and an element α in L, with minimal polynomial f in K[X], then $K(\alpha)\cong K[X]/(f)$. Note that α does not appear on the right side. Hence if α,β are two elements of L having the same minimal polynomial over K, then $K(\alpha)\cong K(\beta)$.
We will apply this to the three complex roots $2^{1/3}$, $\omega\cdot 2^{1/3}$, $\omega^2\cdot 2^{1/3}$, of the irreducible $\mathbb{Q}$ polynomial X^3-2, where $\omega = e^{2\pi i/3}$ is a primitive cube root of 1. This gives three distinct subfields of $\mathbb{C}$, all isomorphic to $\mathbb{Q}[X]/(X^3-2)$ hence to each other, namely $\mathbb{Q}(2^{1/3})$, $\mathbb{Q}(\omega\cdot 2^{1/3})$, and $\mathbb{Q}(\omega^2\cdot 2^{1/3})$. This gives three distinct embeddings of $\mathbb{Q}(2^{1/3})$ into $\mathbb{C}$:
1) id: $\mathbb{Q}(2^{1/3})\to\mathbb{Q}(2^{1/3})\subset\mathbb{C}$,
2) $\mathbb{Q}(2^{1/3})\to\mathbb{Q}(\omega\cdot 2^{1/3})\subset\mathbb{C}$ (taking $2^{1/3}$ to $\omega\cdot 2^{1/3}$), and
3) $\mathbb{Q}(2^{1/3})\to\mathbb{Q}(\omega^2\cdot 2^{1/3})\subset\mathbb{C}$ (taking $2^{1/3}$ to $\omega^2\cdot 2^{1/3}$).
Only the first of these is an isomorphism of $\mathbb{Q}(2^{1/3})$ with itself, hence $\mathbb{Q}(2^{1/3})$ is not normal. QED.

Next we turn to the more interesting case of normal extensions, more interesting since there is more symmetry, more automorphisms, and thus the automorphisms tell us more about the field extension. If $k\subset K\subset L$ are fields and $k\subset K$ is a splitting field, we know the restriction map $G_k(L)\to G_k(K)$ is well defined. We want to prove a criterion for this map to be surjective.

Recall that polynomial rings are another example of a functor, in particular if $K\cong L$, then $K[X]\cong L[X]$. In fact for any ring map $f:R\to S$ there is a naturally induced ring map $R[X]\to S[X]$ extending f, as follows: if $f(a) = a^*$, for a in R, then the induced map takes Σa_iX^i to $\Sigma a_i^*X^i$. It is easy to check this is a ring map. Moreover these induced ring maps respect compositions and identities, hence the association of R[X] to R is a functor from rings to rings (always commutative with identity). This easy remark will be very useful in proving the main Lemma on extending field homomorphisms.

Surjectivity Lemma: If $k \subset K \subset L$ are fields and both $k \subset K$ and $k \subset L$ are splitting fields, then the restriction map $G_k(L) \to G_k(K)$ is (well defined and) surjective.
proof: Assume $L = k(\alpha_1,\ldots,\alpha_n)$ where $(\alpha_1,\ldots,\alpha_n)$ is the full system of roots of a polynomial f in k[X]. Since $k \subset K \subset L$, f is also a K polynomial, and $L = k(\alpha_1,\ldots,\alpha_n) = K(\alpha_1,\ldots,\alpha_n)$. To show $G_k(L) \to G_k(K)$ is surjective, we will extend a k automorphism $\varphi: K \to K$ to a k automorphism $L \to L$, by first regarding it as an embedding $K \to L$, then extending it to an embedding $K(\alpha_1) \to L$, then to $K(\alpha_1,\alpha_2) \to L$, ..., and finally to $K(\alpha_1,\ldots,\alpha_n) \to L$. So assume $\varphi: K \to K \subset L$ is given, and let g denote the minimal polynomial over K satisfied by α_1. Since α_1 is a root of f, and f lies in $k[X] \subset K[X]$, we know that g is a factor of f in K[X]. By the remarks above the Lemma, we know the k-automorphism $\varphi: K \to K$ induces a k automorphism $\varphi: K[X] \to K[X]$, hence takes the irreducible factor g of f, to an irreducible polynomial $\varphi(g) = g^*$ which is a factor of $\varphi(f) = f^*$. In fact $f^* = f$ since φ is a k homomorphism and f is in k[X]. (The polynomial ring functor takes the identity map on k to the identity map on k[X].) Since L contains a full system of roots of f, these roots contain a full system of roots of g^*, so let α_1^* be any root of g^* in L. Then φ induces k isomorphisms $K(\alpha_1) \cong K[X]/(g) \cong K[X]/(g^*) \cong K(\alpha_1^*) \subset L$, and hence the composition is a k-embedding $K(\alpha_1) \to L$. Repeating the argument, we get a k embedding $K(\alpha_1,\alpha_2) \cong (K(\alpha_1))(\alpha_2) \to L$, and thus eventually a k-embedding $L = K(\alpha_1,\ldots,\alpha_n) \to L$. Since L is normal over k, this last map is a k automorphism of L. QED.

Remark: Constructing splitting fields.
It is frequently helpful when working with polynomials over $\mathbb{Q}$ to use the fact that $\mathbb{Q} \subset \mathbb{C}$ and $\mathbb{C}$ is "algebraically closed", hence every polynomial over $\mathbb{Q}$ has a complete system of roots in $\mathbb{C}$. Since splitting fields provide the only examples known to us of normal extensions, we might as well point out that every polynomial has a splitting field. Indeed constructing splitting fields is very easy using our fundamental tool for studying algebraic field extensions, of forming the quotient of a polynomial ring by a maximal ideal.

Lemma: Let k be any field and f any polynomial over k. then there is a field K containing k, and in which f has a root.
proof: This is so easy, the hard part is psychological, i.e. believing

that it works. The field extension is just $K = k[X]/(g)$, where g is any irreducible factor of f in k[X]. We know $(g) \subset k[X]$ is a maximal ideal, so k[X]/(g) is a field, and since $k \cap (g) = 0$, the map $k \to k[X]/(g)$ is injective. Hence we can replace the image of k in $K = k[X]/(g)$ by k itself, so that then K contains k. But why does K contain a root of f? Since g is a factor of f, it suffices to see K contains a root of g, and here is the psychologically tricky part: Let h^* denote the image in $K = k[X]/(g)$, of a polynomial h from k[X]. I.e. h^* = the coset h+(g). Then the root of g in K is just X^*, the coset of X. Why? Well the map $k[X] \to k[X]/(g)$ is a k-algebra map, i.e. a ring map which is the identity on k, and it takes g to zero. Hence the image of $g(X) = \Sigma a_j X^j$ in k[X]/(g), is $0 = g^* = \Sigma(a_j^*)(X^*)^j = \Sigma a_j (X^*)^j = g(X^*)$. That says exactly that X^* is a root of g in $K = k[X]/(g)$, and hence also a root of f. In our old notation, where we used [h] for the coset of h, this says $[0] = [g(X)] = g([X])$, so [X] is a root of g, in K. QED.

Cor: Given any field k and any polynomial f in k[X], there is a field K containing k in which f has a full system of roots, hence there is also a splitting field $k \subset L$ for f in K.
proof: After constructing a field K_1 in which f has at least one root, then f factors over K_1 into factors at least one of which is linear. If all factors are linear, stop. If not, and g is a non linear factor of f over K_1, construct another extension field K_2 of K_1 in which g has a root. After at most n steps, where n = degree (f), we have a field extension K of k, in which f has a full system of roots. It seems to me that this K will be a splitting field of f, but at least the subfield $L \subset K$ generated over k by the roots of f is a splitting field for f over k. QED.

Indeed, up to k-isomorphism, a splitting field for f is uniquely determined by f. We prove a more general statement:
Lemma: Let $k \cong k^*$ be an isomorphism of fields inducing an isomorphism $k[X] \cong k^*[X]$ of polynomial rings. If f is a polynomial in k[X], and f^* the corresponding polynomial in $k^*[X]$, and if $k \subset K$, $k^* \subset K^*$ are splitting fields of f, f^* respectively, then the isomorphism $k \cong k^*$ extends to an isomorphism $K \cong K^*$.
proof: (Induction on degree of f.) If f is linear or factors into linear factors over k, then $k = K$, $k^* = K^*$. If f is irreducible quadratic,

then $k \cong k^*$ induces $K \cong k[X]/(f) \cong k^*[X]/(f^*) \cong K^*$. If f has higher degree, and g is an irreducible factor of f in k[X], corresponding to the irreducible factor g^* of f^* in $k^*[X]$, let α_1 be a root of g in K, and β_1 be a root of g^* in K^*. Then we have again $K \supset k(\alpha_1) \cong k[X]/(g) \cong k^*[X]/(g^*) \cong k^*(\beta_1) \subset K^*$. Now K can be viewed as the splitting field, over $k(\alpha_1)$, of the polynomial h in $k(\alpha_1)[X]$ obtained from f by dividing out the factor $(X-\alpha_1)$. Also the isomorphism $k(\alpha_1) \cong k^*(\beta_1)$ induces an isomorphism $k(\alpha_1)[X] \cong k^*(\beta_1)[X]$ which carries h to the polynomial h^* obtained by dividing f^* by $(X-\beta_1)$. Then we can apply induction to get an isomorphism $K \cong K^*$ between the splitting field of h and that of h^*. Moreover this isomorphism extends $k(\alpha_1) \cong k^*(\beta_1)$, hence also extends $k \cong k^*$. QED.

Now we can characterize (finite) normal extensions.
Prop: $k \subset K$ is a finite, normal, field extension, if and only if K is the splitting field of some polynomial over k.
proof: We have proved "if" above, so we prove "only if".
Lemma: If $k \subset K$ is a finite normal field extension, and α in k is any element, then the minimal polynomial of α over k splits completely into linear factors over K.
proof: Let α be any element of K, and let $K = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Then we can consider also $K = k(\alpha, \alpha_1, \ldots, \alpha_n)$. Now enlarge K to a splitting field L for the product $gg_1g_2 \ldots g_n$, where g is the minimal polynomial for α over k, and g_j is the minimal polynomial for α_j over k. If some root β of g is in L but not in K, we will define a k-isomorphism $K \to L$ which is not an automorphism of K, thus proving K is not normal over k. We begin by defining $k(\alpha) \cong k[X]/(g) \cong k(\beta) \subset L$. Then we continue as in the extension arguments above, to extend this to a k-embedding $k(\alpha, \alpha_1) \to L$, ... and finally $k(\alpha, \alpha_1, \ldots, \alpha_n) \to L$. To carry out this extension, all we need at each step is the knowledge that a certain polynomial has roots in L. In fact this is already guaranteed by our hypotheses, but if you have any doubt, just enlarge L further each time you need to, by adding the roots you need. This proves K is in fact not normal, since the map $k(\alpha, \alpha_1, \ldots, \alpha_n) \to L$ takes α to β, and β is not in K. QED lemma.
proof of Prop: Let $k \subset K = k(\alpha_1, \ldots, \alpha_n)$ be any finite normal extension. Then the minimal polynomial g_j of each α_j splits

completely in K by the Lemma. Thus K is a splitting field of the product Πg_j. QED prop.

Our old principle, that a k-homomorphism permutes the roots of any given k polynomial, has an important consequence for computing Galois groups which we need to state:
The Galois group of a polynomial is isomorphic to a subgroup of the group of permutations of the set of distinct roots of that polynomial

More precisely,
Lemma: Assume $L = k(\alpha_1,\ldots,\alpha_n)$, is a splitting field of a polynomial f in k[X], where $(\alpha_1,\ldots,\alpha_n)$ is the full system of roots of f. Then $G_k(L)$ embeds as a subgroup of S_d, where d is the number of distinct roots of f among the $(\alpha_1,\ldots,\alpha_n)$.
proof: We have seen many times that every k-automorphism φ of L must carry a root of f to another root of f, hence φ permutes the set of distinct roots, say $(\alpha_1,\ldots,\alpha_d)$. Since these roots also generate L over k this permutation determines $\varphi: L \to L$. Hence the restriction homomorphism $G_k(L) \to Bij(\alpha_1,\ldots,\alpha_d)$ [restricting φ from an isomorphism of L to a bijection of the set $(\alpha_1,\ldots,\alpha_d)$] is injective. Any ordering of the roots yields an embedding $G_k(L) \to Bij(\alpha_1,\ldots,\alpha_d) \cong S_d$. QED.

Cor: If $L = k(\alpha_1,\ldots,\alpha_n)$, is a splitting field of a polynomial f of degree n in k[X], then $\#G_k(L)$ divides n!. In fact $\#G_k(L)$ divides d!, where d is the number of distinct roots of f.
proof: This follows from Cauchy's theorem. QED.

Cor: If f is an *irreducible* polynomial in k[X] with d distinct roots, $(\alpha_1,\ldots,\alpha_d)$, and splitting field L, then $G_k(L)$ acts transitively on the set $(\alpha_1,\ldots,\alpha_d)$, and hence d divides $\#G_k(L)$.
proof: We have seen, at the first stage of the proof of the surjectivity Lemma, that we have a choice of mapping α_1 to any root of its minimal polynomial over k. Since f is irreducible over k, f itself is the minimal polynomial, so we can map α_1 to any other root of f. Since this extends to an element of $G_k(L)$, we see that indeed $G_k(L)$ acts transitively on the set of distinct roots. That means the set of d roots is an orbit of the $G_k(L)$ action, so d is the order of an orbit, hence also the index of an isotropy subgroup in

$G_k(L)$. By Cauchy's theorem, d divides $\#(G_k(L))$. QED.

The method of extending homomorphisms allows us to be still more precise about the order of the Galois group:
Lemma: Assume $L = k(\alpha_1,\ldots,\alpha_n)$, is a splitting field of a polynomial f in k[X], where $(\alpha_1,\ldots,\alpha_n)$ is the full system of roots of f in L. Then $\#G_k(L) \leq [L:k]$ = degree of L over k.
proof: Since every k-automorphism of L restricts to a k-homomorphism of each of the intermediate fields $k(\alpha_1,\ldots,\alpha_j)\to L$, we can obtain every such element of $G_k(L)$ in stages, by starting with the inclusion map $k\subset L$, extending it to a map $k(\alpha_1)\to L$, then extending it further to a map $k(\alpha_1,\alpha_2)\to L$, etc.....until we get a map $k(\alpha_1,\ldots,\alpha_n) = L\to L$. Moreover if there are say, two ways to extend the inclusion map $k\subset L$ to a map of $k(\alpha_1)\to L$, and then three ways to extend further to a map $k(\alpha_1,\alpha_2)\to L$, then there are altogether six extensions of $k\subset L$ to a map of $k(\alpha_1,\alpha_2)\to L$, since we have two choices for the image of α_1, and then three choices for the image of α_2. Reasoning in this way, one can see that the number of k-automorphisms of L equals the product of the number of possible extensions at each stage. From the proof above, we know the number of possible extensions to $k(\alpha_1)$ is just the number of distinct roots in L of the minimal polynomial g of α_1 over k, which is at most the degree of g over k. Moreover the degree of g over k equals the degree of the field extension $[k(\alpha_1):k]$. Hence the number of extensions to $k(\alpha_1)$ is at most the degree $[k(\alpha_1):k]$. Similarly, the number of further extensions to $k(\alpha_1,\alpha_2)$ is at most the degree of the field extension $[k(\alpha_1,\alpha_2):k(\alpha_1)]$. Consequently the number of extensions from $k\subset L$ to $k(\alpha_1,\alpha_2)\to L$ is at most the product of these degrees, $[k(\alpha_1):k]\cdot[k(\alpha_1,\alpha_2):k(\alpha_1)] = [k(\alpha_1,\alpha_2):k]$, (by multiplicativity of degrees of field extensions). Continuing, we get that the number of extensions of k-homomorphisms from $k\subset L$ to $L\to L$, i.e. the number of k automorphisms of L, is at most the product $[k(\alpha_1):k]\cdot[k(\alpha_1,\alpha_2):k(\alpha_1)]\cdot\ldots\ldots\cdot[k(\alpha_1,\ldots,\alpha_n):k(\alpha_1,\ldots,\alpha_{n-1})] = [L:k]$. QED.

It is helpful to know when this bound is an equality.
Definition: A "separable" polynomial is one whose roots are all distinct, in any splitting field.

For separable polynomials the bound above is an exact result.
Cor: If $k \subset L$ is a splitting field of a "separable" polynomial f in k[X], then $\#G_k(L) = [L:k]$.
proof: This is what was proved above, since the number of extensions at each stage was the number of distinct roots.
QED.

Fortunately, separable polynomials are quite common.
Prop: In a field of characteristic zero, all irreducible polynomials are separable.
proof: If one defines the derivative of a polynomial $\Sigma a_j X^j$ by the usual formula $\Sigma j a_j X^{j-1}$, then one obtains the usual product rule for derivatives. [The proof is in Brauer's notes.] Hence if a polynomial f has a repeated root a, then $f = g(X)\cdot(X-a)^2$, for some g, and a is also a root of the derivative $f' = g'\cdot(X-a)^2 + 2g\cdot(X-a)$. If f is irreducible, then f is the minimal polynomial of a, hence must divide every other polynomial satisfied by a. Thus if also f has a repeated root, then f must divide its own derivative. Since the derivative of f has lower degree than f, this can happen only if the derivative is identically zero. In characteristic zero this cannot happen for a non constant polynomial, and hence an irreducible polynomial cannot have a repeated root. QED.

Cor: Over a field k of characteristic zero (i.e. any field containing Q), if L is a splitting field of a k polynomial then $\#G_k(L) = [L:k]$.
proof: At each stage of the extension process in the Lemma above, the polynomial used was a minimal one, hence irreducible, hence separable. QED.

Remark: The non constant polynomial $\Sigma a_j X^j$ *can* have derivative zero in characteristic $p > 0$, if in the derivative formula $\Sigma j a_j X^{j-1}$ all the multipliers j are divisible by p, since multiplication by p does make everything zero. For example in characteristic 3 the derivative of X^3-1 is zero. The polynomial $X^3-1 = (X-1)^3$ thus has repeated roots in $\mathbb{Z}_3$ but it is not irreducible. [Cf. the next exercise.]

Exercise #66) If T is a variable, n is prime, and $\mathbb{Z}_n[T^n]$ = the ring of polynomials in T^n with coefficients in $\mathbb{Z}_n$, let $F = \mathbb{Z}_n(T^n)$ be its

quotient field, or "field of fractions". Prove (X^n-T^n) is irreducible over F, but splits as $(X-T)^n$ in the extension field $F(T) \cong Z_n(T)$.

Exercise #57) If the minimal polynomial g_j of each α_j over F is seperable, then the same is true for all elements of $F(\alpha_1,....,\alpha_n)$. [Hint: Arguing as above, calculate the number of F-embeddings $F(\alpha_1,....,\alpha_n) \to L$, where L is a splitting field for Πg_j.]

Exercise #58) (i) If f(X) is an irreducible polynomial over k all of whose roots are equal in the splitting field L, then prove $G_k(L) = \{id\}$, hence $\varphi(\alpha) = \alpha$ for all α in L and all φ in $G_k(L)$.
(ii) If $Q \subset L$ is a finite normal extension, and α is an element of L such that $\varphi(\alpha) = \alpha$ for all φ in $G_Q(L)$, then prove α is in Q.
(iii) If $Q \subset L$ is a finite normal extension, β is in L, and $G_Q(L) = \{\varphi_1,....,\varphi_n\}$, prove that $f(X) = \Pi_j (X-\varphi_j(\beta))$ is a polynomial with coefficients in Q, and such that $f(\beta) = 0$.
(iv) Deduce that $[Q(\beta):Q] \leq \#(G_Q(L))$.

Cor: If f is an irreducible polynomial of prime order p over Q, and if f has precisely two non - real roots, then $G_Q(f) \cong S_p$.
proof: We know G is isomorphic to a transitive subgroup of S_p, hence a subgroup whose order is divisible by p. Then G contains an element of order p, and since p is prime, a cycle of order p, which we might as well denote by (123....p). The splitting field L lies between Q and C. Since f has precisely two non-real roots, complex conjugation is a Q automorphism which transposes exactly two roots, hence G contains a transposition (ab). We know from a previous exercise that (123....p) and (ab) generate S_p, hence $G \cong S_p$. QED.

Cor: The Galois group of the polynomial X^4-2 over Q, has order 8.
proof: We can obtain the splitting field in two stages from Q, extending first to $Q(2^{1/4})$, then to $Q(2^{1/4}, i)$ [= the splitting field of X^4-2 over Q]. The first extension adjoins a root of the polynomial X^4-2. We claim this polynomial is irreducible over Q. We know the roots of the polynomial to be $\{2^{1/4}, -2^{1/4}, i2^{1/4}, -i2^{1/4}\}$. Hence there are no rational roots, and two imaginary roots. Since there are no roots in Q, there cannot be a linear factor over Q. Hence if

X^4-2 factors over $\mathbf{Q}$, it factors into quadratic factors. Since any factor with coefficients in $\mathbf{Q}$ must have imaginary roots in pairs, one quadratic factor must be a constant times $(X-i2^{1/4})(X+i2^{1/4}) = (X^2+2^{1/2})$. Hence the only possible (monic) quadratic factors are $(X^2+2^{1/2})(X^2-2^{1/2})$. But these do not have rational coefficients, so in fact (X^4-2) does not factor over $\mathbf{Q}$. Since X^4-2 is irreducible over $\mathbf{Q}$, the extension $\mathbf{Q}(2^{1/4})$ is isomorphic to $\mathbf{Q}[X]/(X^4-2)$, and thus the degree $[\mathbf{Q}(2^{1/4}):\mathbf{Q}] = 4$. Now $\mathbf{Q}(2^{1/4}, -2^{1/4}, i2^{1/4}, -i2^{1/4}) = \mathbf{Q}(2^{1/4},i)$, so we can achieve the full splitting field of X^4-2), by adjoining a root of X^2+1 to $\mathbf{Q}(2^{1/4})$. Since $\mathbf{Q}(2^{1/4})$ contains no imaginary numbers, X^2+1 is irreducible over $\mathbf{Q}(2^{1/4})$, and thus the degree $[\mathbf{Q}(2^{1/4}):\mathbf{Q}] = 2$. So the total degree $[\mathbf{Q}(2^{1/4}, i):\mathbf{Q}] = (4)(2) = 8$. QED.

Example: Explicit computation of the Galois group of X^4-2.
Notation: If f is a polynomial over k and L is a splitting field for f over k, let us denote the Galois group $G_k(L)$ by $G_k(f)$. We know the splitting field L depends only on the polynomial f, so this notation makes sense.

The method of extending homomorphisms allows us to compute the Galois group $G_{\mathbf{Q}}(X^4-2)$ completely, as follows. We know the splitting field can be achieved in two stages $\mathbf{Q} \subset \mathbf{Q}(2^{1/4}) \subset \mathbf{Q}(2^{1/4},i)$, but it is convenient to do this in the opposite order, $\mathbf{Q} \subset \mathbf{Q}(i) \subset \mathbf{Q}(2^{1/4},i)$, first adjoining i, a root of X^2+1, and then adjoining $2^{1/4}$, a root of the polynomial X^4-2, which is still irreducible over $\mathbf{Q}(i)$ [by the multiplicativity of degrees, $[\mathbf{Q}(2^{1/4},i):\mathbf{Q}] = [\mathbf{Q}(2^{1/4}):\mathbf{Q}][\mathbf{Q}(2^{1/4},i):\mathbf{Q}(2^{1/4})] = (4)(2) = 8 = [\mathbf{Q}(i):\mathbf{Q}][\mathbf{Q}(2^{1/4},i):\mathbf{Q}(i)] = (2)[\mathbf{Q}(2^{1/4},i):\mathbf{Q}(i)]$. Hence the minimal polynomial of $2^{1/4}$ over $\mathbf{Q}(i)$ still has degree 4.]Since this second polynomial X^4-2, has coefficients in $\mathbf{Q}$, it will not be changed by our choice of the homomorphism on $\mathbf{Q}(i)$.
We will obtain $G_{\mathbf{Q}}(\mathbf{Q}(2^{1/4}, i)$ by computing all ways to extend the inclusion $\mathbf{Q} \to \mathbf{C}$ to embeddings of $\mathbf{Q}(i) \to \mathbf{C}$, and then all ways to extend further to embeddings of $\mathbf{Q}(i,2^{1/4}) \to \mathbf{C}$. Since the minimal polynomial of i over $\mathbf{Q}$ has two roots, there are two ways to extend the inclusion $\mathbf{Q} \to \mathbf{C}$ to an embedding of $\mathbf{Q}(i) \to \mathbf{C}$; i.e. we can send i to

either i or -i. Since there are four roots of X^4-2, we can extend such an embedding in four ways to an embedding of $\mathbf{Q}(i,2^{1/4})\to\mathbf{C}$. I.e. we can send $2^{1/4}$ to any one of $\{2^{1/4}, -2^{1/4}, i2^{1/4}, -i2^{1/4}\}$. Finally we compute the Galois group by computing what permutation of the set of roots $\{2^{1/4}, -2^{1/4}, i2^{1/4}, -i2^{1/4}\}$ these homomorphisms give us. We carry this out fully next, numbering the homomorphisms as we go:

#1) Map i to i, and $2^{1/4}$ to $2^{1/4}$. This gives the identity map, i.e. the inclusion $\mathbf{Q}(i,2^{1/4})\subset\mathbf{C}$.
#2) Map i to i, and $2^{1/4}$ to $i2^{1/4}$.
#3) Map i to i, and $2^{1/4}$ to $-2^{1/4}$.
#4) Map i to i, and $2^{1/4}$ to $-i2^{1/4}$.
#5) Map i to -i, and $2^{1/4}$ to $2^{1/4}$.
#6) Map i to -i, and $2^{1/4}$ to $i2^{1/4}$.
#7) Map i to -i, and $2^{1/4}$ to $-2^{1/4}$.
#8) Map i to -i, and $2^{1/4}$ to $-i2^{1/4}$.

Next we compute the permutations each of these homomorphisms induces on the set of roots $\{2^{1/4}, i2^{1/4}, -2^{1/4}, -i2^{1/4}\}$, which we choose to order as they occur cyclically around the unit circle in the complex plane. So denote these roots as $2^{1/4}$ = "a", $i2^{1/4}$ = "b", $-2^{1/4}$ = "c", $-i2^{1/4}$ = "d".

#1) is the permutation id = (a)(b)(c)(d).
#2) sends $2^{1/4}$ to $i2^{1/4}$ and i to i, hence $i2^{1/4}$ to $-2^{1/4}$, $-2^{1/4}$ to $-i2^{1/4}$, and $-i2^{1/4}$ to $2^{1/4}$. This is the cycle (abcd).
#3) sends i to i, and $2^{1/4}$ to $-2^{1/4}$, hence $i2^{1/4}$ to $-i2^{1/4}$, $-2^{1/4}$ to $2^{1/4}$, and $-i2^{1/4}$ to $i2^{1/4}$. This is (ac)(bd).
#4) sends i to i, and $2^{1/4}$ to $-i2^{1/4}$, hence $i2^{1/4}$ to $2^{1/4}$, $-2^{1/4}$ to $i2^{1/4}$, and $-i2^{1/4}$ to $-2^{1/4}$. This is (adcb).
#5) sends i to -i, and $2^{1/4}$ to $2^{1/4}$, hence $i2^{1/4}$ to $-i2^{1/4}$, $-2^{1/4}$ to $-2^{1/4}$, and $-i2^{1/4}$ to $i2^{1/4}$. This is (bd).
#6) sends i to -i, and $2^{1/4}$ to $i2^{1/4}$, hence $i2^{1/4}$ to $2^{1/4}$, $-2^{1/4}$ to $-i2^{1/4}$, and $-i2^{1/4}$ to $-2^{1/4}$. This is (ab)(cd).
#7) sends i to -i, and $2^{1/4}$ to $-2^{1/4}$, hence $i2^{1/4}$ to $i2^{1/4}$, $-2^{1/4}$ to $2^{1/4}$, and $-i2^{1/4}$ to $-i2^{1/4}$. This is (ac).

#8) sends i to -i, and $2^{1/4}$ to $-i2^{1/4}$, hence $i2^{1/4}$ to $-2^{1/4}$, $-2^{1/4}$ to $i2^{1/4}$, and $-i2^{1/4}$ to $2^{1/4}$. This is (ad)(bc).

Looking at the subgroup of S_4 formed by the permutations above, we see that it consists exactly of the full group of symmetries of the square whose vertices are lettered counterclockwise as abcd. The first four are rotations, #5, #7 are reflections about the two diagonals, and #6, #8 are reflections about the two lines bisecting opposite pairs of sides. Thus $G_{\mathbb{Q}}(X^4-2) \cong D_4$, the (8 - element) dihedral group on four letters. QED.

Remark: This computation was made easier by choosing successive extensions for which the irreducible polynomials never change during any of the extensions of homomorphisms. The situation is different for the extensions $\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(i,2^{1/2}) \subset \mathbb{Q}(i,2^{1/4})$. It is perhaps worth doing this more complicated example to illustrate the full generality of the proof of the surjectivity Lemma, in particular to see why the irreducible polynomial g used there can become a different polynomial g*. We will be somewhat more brief.

#1) Map i to i, then $2^{1/2}$ to $2^{1/2}$, then $2^{1/4}$ to $2^{1/4}$, (the identity).
#2) Map i to i, then $2^{1/2}$ to $2^{1/2}$, then $2^{1/4}$ to $-2^{1/4}$.
#3) Map i to i, then $2^{1/2}$ to $-2^{1/2}$, which changes the minimal polynomial for the next extension from $X^2-2^{1/2}$ into $X^2+2^{1/2}$. Hence we must map $2^{1/4}$ to a root of $X^2+2^{1/2}$, say $i2^{1/4}$.
#4) Map i to i, then $2^{1/2}$ to $-2^{1/2}$, then map $2^{1/4}$ to the other root of $X^2+2^{1/2}$, that is $-i2^{1/4}$.
#5) Map i to -i, then $2^{1/2}$ to $2^{1/2}$, then $2^{1/4}$ to $2^{1/4}$.
#6) Map i to -i, then $2^{1/2}$ to $2^{1/2}$, then $2^{1/4}$ to $-2^{1/4}$.
#7) Map i to -i, then $2^{1/2}$ to $-2^{1/2}$, then $2^{1/4}$ to $i2^{1/4}$.
#8) Map i to -i, then $2^{1/2}$ to $-2^{1/2}$, then $2^{1/4}$ to $-i2^{1/4}$.

In terms of cycles, with the roots lettered as before, i.e. with $a=2^{1/4}$, $b = i2^{1/4}$, $c= -2^{1/4}$, $d = -i2^{1/4}$, we get:
#1) = (a)(b)(c)(d)
#2) = (ac)(bd)
#3) = (abcd)
#4) = (adcb).

#5) = (bd)
#6) = (ac)
#7) = (ab)(cd)
#8) = (ad)(bc)
Again we see that these permutations form the full group D_4 of symmetries of the square with vertices labeled cyclically a,b,c,d.

In the next section we consider the Galois group of an extension formed by adjoining a single nth root, the fundamental building block of a radical extension. This is the first step in understanding the Galois group of a "solvable" polynomial.

solvable

§20) Polynomials of form (X^n-a) have ~~abelian~~ Galois groups
Back when we introduced the ideas of Galois theory and the problem of solving polynomial equations we observed that the roots of the polynomial X^n-1 form a group, cyclic of order n, and we said it did not seem too outlandish to guess that the Galois group of this polynomial might be cyclic of order n. Unfortunately, a few calculations say otherwise. For instance, X^2-1, already splits over Q, so the Galois group $G_Q(X^2-1)$ is cyclic, but of order one, not two. Then for X^3-1, this polynomial is not irreducible, but factors as $(X-1)(X^2+X+1)$, hence the splitting field is obtained by adjoining a root of X^2+X+1. Since there is only one real cube root of 1, this polynomial is irreducible quadratic, so the Galois group over Q is Z_2, cyclic again but of order 2, not 3. We might guess now the group of X^n-1 over Q is always cyclic of order n-1, but first let's compute one more. The polynomial X^4-1 splits over Q into the irreducible factors $(X-1)(X+1)(X^2+1)$, and thus the splitting field is obtained by adjoining a root of X^2+1, also irreducible quadratic, hence the group is Z_2, not Z_3. For X^5-1, we can factor at least as $(X-1)(X^4+X^3+X^2+X+1)$, but it is not clear whether the second factor is irreducible over Q. If it is, then the Galois group has order 4, but what is it? The next case, of X^6-1, is easier since it factors as $X^6-1 = (X^3+1)(X^3-1)$, and since a primitive 6th root of 1 cannot be a root of (X^3-1), the primitive roots must all be roots of $(X^3+1) = (X+1)(X^2-X+1)$, hence of (X^2-X+1). Since this quadratic has no real roots it is irreducible over Q. Thus again the Galois group of X^6-1 over Q is Z_2. We really aren't getting

a clear picture this way, and all the groups we could compute have been cyclic. You might try to guess the general rule.
As an alternative, instead of trying to generalize these examples, just for fun let's use the "Zen" method of guessing, i.e. the answer must be something nice and simple, or else we would never guess it. And mathematics is part of creation and the natural world, so the answer must be something beautiful and natural anyway. (If you think no respectable scientist ever argues this way, read Galileo some time!) So try to think of a group naturally associated with the number n, but different from $\mathbf{Z}_n$. In case n = 2, it was $\mathbf{Z}_1 = \{0\}$; in case n = 3, it was $\mathbf{Z}_2$; in case n = 4, it was $\mathbf{Z}_2$; in case n = 5 we think it has order 4; in case n = 6 it was $\mathbf{Z}_2$. What other group can you think of associated to n that has those orders? Well you might recall that $\mathbf{Z}_n$ is a ring, i.e. multiplication makes sense as well as addition, and $\mathbf{Z}_n$ is a group only under addition. But for example in $\mathbf{Z}_3$ we get a group under multiplication if we look only at the non zero numbers {1,2}. I.e. $2^2 = 1$, and $1 \cdot 2 = 2$, and so on. Got the idea? Every ring has two groups associated to it, the whole ring is a group for addition, and the invertible elements are a group for multiplication. [In functor language, there are two "forgetful" functors from rings to groups, (i) $(R,+,\cdot) \mapsto (R,+)$, and (ii) $(R,+,\cdot) \mapsto (R^*,\cdot)$ where R^* denotes the invertible elements of R.] So $\mathbf{Z}_n$ has a group of units $\mathbf{Z}_n^*$, represented by the positive integers less than, and relatively prime to, n. These groups have the right orders, at least so far, assuming the polynomial $(X^4+X^3+X^2+X+1)$ in the case n = 5 is actually irreducible over $\mathbf{Q}$. So we might refine our previous guess and conjecture that the Galois group of X^n-1 over $\mathbf{Q}$, is isomorphic to $\mathbf{Z}_n^*$, the multiplicative group of units of the ring $\mathbf{Z}_n$. To find out we will simply write down the $\mathbf{Q}$ automorphisms of $\mathbf{Q}(X^n-1)$ as best we can, using what we know about the complex roots of these polynomials. Since it takes a bit of work to show irreducibility over $\mathbf{Q}$ of the polynomial whose roots are *all* primitive nth roots of unity, we will settle for something less at the moment.

Proposition: For every $n \geq 2$, if η is a primitive nth root of 1, then $\mathbf{Q}(\eta)$ is a splitting field for (X^n-1), hence normal over $\mathbf{Q}$. There is an injective homomorphism from $G_{\mathbf{Q}}(X^n-1) = G_{\mathbf{Q}}(\mathbf{Q}(\eta)) \to (\mathbf{Z}_n^*,\cdot)$, hence $G_{\mathbf{Q}}(X^n-1)$ is isomorphic to a subgroup of $(\mathbf{Z}_n^*,\cdot)$. In particular

$G_{\mathbf{Q}}(X^n-1)$ is abelian (but not necessarily cyclic).
proof of proposition: Let η be a primitive nth root of 1, and let f be its minimal polynomial over $\mathbf{Q}$. For any other root μ of f, there is a $\mathbf{Q}$ isomorphism of fields between $\mathbf{Q}(\eta)$ and $\mathbf{Q}(\mu)$ taking η to μ. Thus $\eta^k = 1$ iff $\mu^k = 1$, so if $(\eta=\eta_1, \eta_2, \eta_3,\dots,\eta_d)$ are the roots of f in $\mathbf{C}$, then all d of them are *primitive* nth roots of 1. Since every nth root of 1 is a power of η, the splitting field of X^n-1 over $\mathbf{Q}$ is simply $\mathbf{Q}(\eta)$. Hence $G_{\mathbf{Q}}(X^n-1)$ = the set of $\mathbf{Q}$ automorphisms of $\mathbf{Q}(\eta)$. By our usual principle, every $\mathbf{Q}$ automorphism of $\mathbf{Q}(\eta)$ takes one root of f to another, and conversely, for every root μ of f, there is a $\mathbf{Q}$ automorphism taking η to μ. [You might think that surely there is a $\mathbf{Q}$ automorphism of $\mathbf{Q}(\eta)$ taking η to any other primitive nth root of 1, but if you can prove it you will have proved the nth cyclotomic polynomial is irreducible. So you might try.] Thus $G_{\mathbf{Q}}(X^n-1)$ has exactly d elements, $\varphi_1,\dots,\varphi_d$, where $\varphi_j(\eta) = \eta_j$, for $j=1,\dots d$. Now since each η_j is itself a primitive nth root of 1, then $\varphi_j(\eta) = \eta_j = \eta^{r_j}$ for some integer r_j relatively prime to n. Now r_j is not well defined since $\eta^n = 1$, so $\eta^{r+n} = \eta^r$, but $\eta^r = \eta^s$ iff $r \equiv s \bmod n$. Thus we have a well defined, injective, function $G_{\mathbf{Q}}(X^n-1) \to \mathbf{Z}_n^*$, taking φ_j to $[r_j]$. We need to check whether this is a homomorphism, i.e. whether $\varphi_j \circ \varphi_k$ goes to $[r_j][r_k]$. Since $(\varphi_j\circ\varphi_k)(\eta) = \varphi_j(\varphi_k(\eta)) = (\eta^{r_k})^{r_j} = \eta^{r_j r_k}$, this is indeed a homomorphism. Thus $G_{\mathbf{Q}}(X^n-1)$ is isomorphic to a subgroup of $(\mathbf{Z}_n^*,\cdot)$, and in particular $G_{\mathbf{Q}}(X^n-1)$ is abelian for every $n \geq 1$. QED.

Remarks: i) As you may have realized, the proposition above can also be proved by the following reasoning: the n roots of the polynomial X^n-1 form a cyclic subgroup of the multiplicative group of the splitting field $K = \mathbf{Q}(\eta)$, hence the elements of $G_{\mathbf{Q}}(K)$ restrict to group automorphisms of $\mathbf{Z}_n$, i.e. to elements of $\mathrm{Aut}(\mathbf{Z}_n) \cong \mathbf{Z}_n^*$. Since the roots of X^n-1 generate K, the restriction map is injective. This shows too why the fact that the roots formed a cyclic group should have suggested that the Galois group was likely to be, not cyclic, but the *automorphism* group of a cyclic group.
ii) It can be proved that the nth "cyclotomic polynomial" $\Phi_n(X) = \prod(X-\eta)$, product over all primitive nth roots η of 1, has rational coefficients and is irreducible in $\mathbf{Q}[X]$. Consequently the two groups

$G_{\mathbb{Q}}(X^n-1)$ and $\mathbb{Z}_n^*$, both have the same order $\varphi(n)$, ("Euler's phi function" of n), and hence actually $G_{\mathbb{Q}}(X^n-1) \cong \mathbb{Z}_n^*$. A formula for $\varphi(n)$ is given in books on number theory, and it is known that $\mathbb{Z}_n^*$ is not always cyclic, but it is always a direct product of cyclic groups, and is actually cyclic for example when n is prime.

Next let's try the Galois groups of equations of form X^n-a, but not over $\mathbb{Q}$. Instead let's consider an extension of form $F \subset F(\alpha)$, where $\alpha^n = a$ is in F, and where F already contains a splitting field for X^n-1. Interestingly, the group $G_F(F(\alpha))$ is a subgroup of $(\mathbb{Z}_n,+)$.

Proposition: If F is a subfield of $\mathbb{C}$ containing a splitting field for X^n-1, if α belongs to $\mathbb{C}$ and $\alpha^n = a$ is in F, then $F(\alpha)$ is a splitting field over F for X^n-a, and there is an injective homomorphism $G_F(F(\alpha)) \to (\mathbb{Z}_n,+)$. In particular the extension $F \subset F(\alpha)$ is normal and the Galois group $G_F(F(\alpha))$ is cyclic, hence abelian.

proof: If α is one solution of X^n-a, and η is any primitive nth root of 1, then $(\alpha\eta)^n = \alpha^n\eta^n = a \cdot 1 = a$, so $\alpha\eta$ is another solution of X^n-a. Thus if F contains a splitting field for X^n-1 and α is one root of X^n-a, then $F(\alpha)$ is a splitting field over F for X^n-a, with the complete set of roots $\{\alpha_1, \alpha_1\eta, \alpha_1\eta^2, \ldots, \alpha_1\eta^{n-1}\}$. In particular $F \subset F(\alpha)$ is a normal extension. The group $G_F(F(\alpha))$ of all F-automorphisms $F(\alpha) \to F(\alpha)$, corresponds precisely to the set of distinct roots of the minimal polynomial for α over F, which is some irreducible factor f of X^n-a. [Note that in $\mathbb{Q}(i)$, the splitting field for X^4-1, the polynomial X^4-4 has no roots, but $X^4-4 = (X^2-2)(X^2+2)$. Hence the minimal polynomial for $4^{1/4}$ is the irreducible quadratic (X^2-2), the splitting field of X^4-1 has degree 2 over $\mathbb{Q}(i)$, and the group $G_{\mathbb{Q}}(X^4-4)$ is isomorphic to $\mathbb{Z}_2$.]

So let a belong to F, let α be one complex solution of X^n-a, and let $\{\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d\}$ be the complete set of distinct complex roots of the minimal polynomial f of α over F. f is a factor of X^n-a, so if η is any primitive nth root of 1 in F, then the complete set of roots of f are $\alpha = \alpha_1 = \alpha_1 \cdot \eta^0$, $\alpha_2 = \alpha_1 \cdot \eta^{r2}$, $\alpha_3 = \alpha_1\eta^{r3}, \ldots$, $\alpha_d = \alpha_1\eta^{rd}$, for some integers r_j, where $r_1 = 0$.

We have observed that $F(\alpha)$ is a splitting field for X^n-a, and now we

see the group $G_F(F(\alpha))$ consists of $\varphi_1,\ldots,\varphi_d$, where $\varphi_j(\alpha) = \alpha\eta^{r_j}$. The exponents r_j are well defined and distinct mod n, so we get a well defined, injective map $G_F(F(\alpha))\to\mathbb{Z}_n$, sending φ_j to r_j.
Claim: This map is a homomorphism to $(\mathbb{Z}_n,+)$.
proof of Claim: We must show that $\varphi_j\circ\varphi_k$ goes to r_j+r_k. But $(\varphi_j\circ\varphi_k)(\alpha) = (\varphi_j(\varphi_k(\alpha)) = \eta^{r_j}(\eta^{r_k}\alpha) = \eta^{(r_j+r_k)}\alpha$, so this is true, and the map is a homomorphism. **QED Claim.**
Thus $G_F(F(\alpha))$ is isomorphic to a subgroup of $(\mathbb{Z}_n,+)$, and in particular is cyclic and abelian. **QED Prop.**

At last we are ready to prove Galois' necessary condition on the Galois group of a "solvable" polynomial. We do so in the next section.

§21) Galois groups of solvable polynomials have prime order simple constituents

First we make the following definition:
Definition: A finite group G is called "solvable" iff all the simple constituents of every (equivalently some) composition series for G are abelian, equivalently iff they are cyclic of prime order.

Definition: A field extension $K\subset L$ is called a "radical extension" iff L is a finite extension of K obtained by a sequence of extensions of the following form: $K\subset K(\alpha_1)\subset K(\alpha_1,\alpha_2)\subset\ldots\subset K(\alpha_1,\alpha_2,\ldots,\alpha_s) = L$, where for each j, some positive power of α_j lies in $K(\alpha_1,\alpha_2,\ldots,\alpha_{j-1})$.

Definition: A polynomial f over $\mathbb{Q}$ can be "solved by radicals" iff the splitting field F for f is contained in a radical extension of $\mathbb{Q}$.

Theorem(Galois): If a polynomial f over $\mathbb{Q}$ can be "solved by radicals", then the Galois group of its splitting field over $\mathbb{Q}$ is a solvable group.

This will follow from all the subsidiary results to come next.
We need one more ingredient, a simple "trick" we borrow from the discussion in Michael Artin's Algebra.

Definition: A "good" radical extension of $\mathbb{Q}$, is a radical extension K which is *normal* over $\mathbb{Q}$, and of the form

$\mathbb{Q} \subset \mathbb{Q}(\eta) \subset \mathbb{Q}(\eta,\alpha_1) \subset \mathbb{Q}(\eta,\alpha_1,\alpha_2) \subset \ldots \subset \mathbb{Q}(\eta,\alpha_1,\ldots,\alpha_s) = K$, where for some n, η is a primitive nth root of 1, and for every j, $(\alpha_j)^n$ belongs to $\mathbb{Q}(\eta,\alpha_1,\ldots,\alpha_{j-1})$.

Lemma: If f is in $\mathbb{Q}[X]$ and f is solvable (over $\mathbb{Q}$) by radicals, then the splitting field of f lies in some *good* radical extension of $\mathbb{Q}$. In fact every radical extension of $\mathbb{Q}$ lies in a good radical extension of $\mathbb{Q}$.
proof: Start with a radical extension of form
$\mathbb{Q} \subset \mathbb{Q}(\alpha_1) \subset \mathbb{Q}(\alpha_1,\alpha_2) \subset \ldots \subset \mathbb{Q}(\alpha_1,\ldots,\alpha_s)$, where some positive power r_j of each α_j lies in the previous field $\mathbb{Q}(\alpha_1,\ldots,\alpha_{j-1})$. If we take $n = \Pi r_j$, then the nth power of each α_j lies in the previous field also. Then we can take η to be any primitive nth root of 1, and adjoin η to $\mathbb{Q}$ first, giving us the sequence of fields
$\mathbb{Q} \subset \mathbb{Q}(\eta) \subset \mathbb{Q}(\eta,\alpha_1) \subset \mathbb{Q}(\eta,\alpha_1,\alpha_2) \subset \ldots \subset \mathbb{Q}(\eta,\alpha_1,\ldots,\alpha_s) = K$.
Now each field is a splitting field over the previous one, hence normal; [$\mathbb{Q}(\eta,\alpha_1,\ldots,\alpha_j)$ is the splitting field over $\mathbb{Q}(\eta,\alpha_1,\ldots,\alpha_{j-1})$ of $X^n - a_j$, where $a_j = (\alpha_j)^n$.] The problem is that the last field K may not be normal over $\mathbb{Q}$. I.e. the equation $X^n - a_j$ for α_j does split in K, but the coefficient a_j in this equation lies in $\mathbb{Q}(\alpha_1,\ldots,\alpha_{j-1})$, not in $\mathbb{Q}$. We have no reason to think that any equation over $\mathbb{Q}$ for α_j splits in K. The point of the next trick is that we can adjoin the other roots of such an equation without changing the fact that we have a radical extension.
We are simply going to enlarge the field $\mathbb{Q}(\eta,\alpha_1,\ldots,\alpha_s)$ until it is normal over $\mathbb{Q}$. The only technique needed is the one used in our proof of the fundamental surjectivity lemma for field automorphisms. We state it next in the form we will use.

Sublemma: If $\varphi: F \to \mathbb{C}$ is any field homomorphism, and β is any element algebraic over F, there is an extension of φ to a field homomorphism $\Phi: F(\beta) \to \mathbb{C}$. More generally, if $F \subset K$ is any finite field extension, there is an extension $\Phi: K \to \mathbb{C}$ of φ from F to K.
proof of sublemma: The embedding φ maps F isomorphically to a subfield L of $\mathbb{C}$, and the induced isomorphism $F[X] \cong L[X]$ carries the minimal F-polynomial g of β to an irreducible L-polynomial g^*. Then $F \subset F[X]/(g)$, and $L \subset L[X]/(g^*)$ are subfields, and the isomorphism $F[X]/(g) \cong L[X]/(g^*)$ extends φ. If β^* is any complex root of g^*, Φ can be defined as the composition $F(\beta) \cong F[X]/(g) \cong L[X]/(g^*) \cong L(\beta^*) \subset \mathbb{C}$.

The more general statement is proved by applying the argument repeatedly to a finite sequence of elements generating K over F. QED sublemma.

Back to the Lemma: Now consider again $\mathbf{Q}(\eta,\alpha_1,\ldots,\alpha_s) = K$, let h_j be the minimal polynomial of α_j over $\mathbf{Q}$, and let $h = \Pi h_j$. The elements $\alpha_1,\ldots,\alpha_s$ are some of the roots of h. To enlarge K to a normal extension of $\mathbf{Q}$, we claim it suffices to adjoin to K also all other roots of h. Since all roots of the minimal polynomial for η are already in K, the enlarged field will be the splitting field over $\mathbf{Q}$ of the polynomial $h(X)\cdot(X^n - 1)$. I.e.:

Claim: If $\varphi_1,\ldots,\varphi_d$ is the set of all $\mathbf{Q}$ homomorphisms $\varphi: K \to \mathbf{C}$, then $\{\alpha_1,\ldots,\alpha_s;\ \varphi_1(\alpha_1),\ldots,\varphi_1(\alpha_s);\ldots\ldots;\varphi_d(\alpha_1),\ldots,\varphi_d(\alpha_s)\}$ is a complete set of roots of h, some roots possibly occurring repeatedly.

proof of claim: If $\varphi: K \to \mathbf{C}$ is a $\mathbf{Q}$-homomorphism, and α is a root of h, then we know very well that since h has $\mathbf{Q}$ coefficients, $\varphi(\alpha)$ is again a root of h. In the opposite direction, if β is a root of h, then β is a root of some irreducible h_j, and we can define a $\mathbf{Q}$-isomorphism $\mathbf{Q}(\alpha_j) \to \mathbf{Q}(\beta) \subset \mathbf{C}$, taking α_j to β. By the sublemma above, this map extends to a $\mathbf{Q}$-homomorphism $\varphi: K \to \mathbf{C}$. Hence every root of h has form $\varphi_i(\alpha_j)$ for some φ_i and some α_j. QED claim.

By the Claim, the field extension
$\mathbf{Q}(\eta,\alpha_1,\ldots,\alpha_s;\ \varphi_1(\eta),\varphi_1(\alpha_1),\ldots,\varphi_1(\alpha_s);\ldots\ldots;\varphi_d(\eta),\varphi_d(\alpha_1),\ldots,\varphi_d(\alpha_s)) = L$ is normal over $\mathbf{Q}$. Moreover, since $(\alpha_j)^n$ is in $\mathbf{Q}(\eta,\alpha_1,\ldots,\alpha_{j-1})$, and φ_i is a $\mathbf{Q}$ -homomorphism of K, $\varphi_i(\alpha_j)^n$ is in $\mathbf{Q}(\varphi_i(\eta),\varphi_i(\alpha_1),\ldots,\varphi_i(\alpha_{j-1}))$. Thus each step in the extension L is a splitting field of a polynomial of form $X^n - c$, over the previous stage, and L is thus a good radical extension of $\mathbf{Q}$. Since $K \subset L$, we are done. QED lemma.

Remark: In the proof above, since $\mathbf{Q}(\eta) = \mathbf{Q}(\varphi_j(\eta))$ for all j, $\mathbf{Q}(\eta,\alpha_1,\ldots,\alpha_s;\varphi_1(\alpha_1),\ldots,\varphi_1(\alpha_s);\ldots\ldots;\varphi_d(\alpha_1),\ldots,\varphi_d(\alpha_s)) = L$, is also a good radical extension, and slightly simpler.

Exercise #69) Let f be an irreducible polynomial over $\mathbf{Q}$. Prove that if one solution of f can be expressed in terms of radicals and field operations, then all solutions of f can be so expressed.

Now we need only a simple group theoretic Lemma:

Lemma: If G is a finite group, and $K \subset G$ is a normal subgroup, then G is solvable iff both K and $H = G/K$ are solvable.

proof: Let $(e) = H_0 \subset H_1 \subset \ldots \subset H_n = H$ be a composition series for H, and $(e) = K_0 \subset K_1 \subset \ldots \subset K_m = K$ a composition series for K, and $\varphi: G \to H$ the canonical homomorphism. Then $(e) \subset K_0 \subset \ldots \subset K_m = \varphi^{-1}(H_0) \subset \ldots \subset \varphi^{-1}(H_n) = G$ is a composition series for G, and by the fundamental homomorphism theorems the set of simple components of this series is the union of the sets of simple components of H and of K. Thus the simple components of G are all of prime order iff those of both K and H are. QED lemma.

Cor: If $F_0 \subset F_1 \subset \ldots \subset F_n$ is a tower of fields, such that each extension $F_{j-1} \subset F_j$ is normal, and also $F_0 \subset F_n$ is (finite and) normal, and each Galois group $G(F_j/F_{j-1})$ is solvable, then $G(F_n/F_0)$ is solvable. In particular the Galois group of a good radical extension is solvable.
proof: By induction on n. If n=1 we are done. Let $n > 1$. Since it is trivial that each extension $F_j \subset F_n$ is also normal for $j > 0$, it follows from induction that the group of $F_1 \subset F_n$ is solvable. We know the restriction homomorphism $G(F_n/F_0) \to G(F_1/F_0)$ is well defined and surjective, and its kernel is by definition equal to $G(F_n/F_1)$. Thus we have an isomorphism $G(F_n/F_0)/G(F_n/F_1) \cong G(F_1/F_0)$, and $G(F_n/F_0)$ is solvable by the previous lemma. A good radical extension is a tower of precisely the form given in the corollary. QED.

Now at last we can prove Galois'
Theorem: If f in Q[X] is solvable by radicals, then the Galois group $G_Q(f)$ is a solvable group.
proof: If F is the splitting field of f, then we have $Q \subset F \subset L$ where L is some good radical extension. Then the surjective homomorphism $G_Q(L) \to G_Q(F)$ shows, by the previous corollary and lemma, that $G_Q(F)$ is solvable. QED theorem.

Proposition: The polynomial $f(X) = X^5 - 80X + 2$ has Galois group isomorphic to S_5, and hence is not solvable by radicals.
proof: We know already that an irreducible quintic polynomial over Q with exactly 3 real roots has group S_5. It follows from Eisenstein's criterion that this polynomial is irreducible, and a little max/min theory from calculus shows that it has precisely three real roots. Since we also know $(e) \subset A_5 \subset S_5$ is a composition series for S_5, in which A_5 is a simple group of order 60, S_5 is not solvable. QED.

Exercise #70) Apply Eisenstein's criterion (below) to prove $X^5 - 80X + 2$ is irreducible over $\mathbb{Q}$, and use calculus to prove that this polynomial has exactly 3 real roots.

Recall: "Eisenstein's criterion": If $f(X) = a_0+a_1X+.....+a_nX^n$, has integer coefficients, and if some prime number p exists such that p divides $a_0, a_1, ...,a_{n-1}$, but p does not divide a_n, and p^2 does not divide a_0, then f is irreducible over $\mathbb{Q}$.

Exercise #71: Prove that the hypothesis of Eisenstein's criterion implies that f is irreducible over $\mathbb{Z}$, except for possible integer factors. ("Gauss' Lemma", proved later, implies f is then irreducible also over $\mathbb{Q}$.)

Definition: Given an extension $k \subset L$, an element α of L is called separable over k if the minimal polynomial of α over k is separable (i.e. has distinct roots). The extension $k \subset L$ is separable if every element of L is separable over k.

Exercise #72) (i) Given $k \subset L$ (finite) normal, separable, and $k \subset F \subset L$, prove the subfield of elements of L left fixed by the subgroup $G_F(L) \subset G_k(L)$ is exactly F.
(ii) For any finite, normal, separable extension $k \subset L$, prove #(subfields F with $k \subset F \subset L$) $\leq$ #(subgroups of $G_k(L)$), in particular the number of intermediate fields F between k and L is finite.

Exercise #73) (i) If $\mathbb{Q} \subset L$ is finite, and α, β are in L, prove there exist $\lambda \neq \mu$ in $\mathbb{Q}$ such that $\mathbb{Q}(\alpha+\lambda\beta) = \mathbb{Q}(\alpha+\mu\beta)$. [Hint: Prove there are only finitely many fields between $\mathbb{Q}$ and L.]
(ii) If $\mathbb{Q} \subset L$ is finite, and α, β are in L, prove there is λ in $\mathbb{Q}$ such that $\mathbb{Q}(\alpha+\lambda\beta) = \mathbb{Q}(\alpha, \beta)$.
(iii) If $\mathbb{Q} \subset L$ is finite, prove $L = \mathbb{Q}(\gamma)$ for some γ in L.

Exercise #74) If p, q are distinct primes, prove $\mathbb{Q} \subset \mathbb{Q}(p^{1/2}, q^{1/2})$ is a normal extension, with Galois group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Exercise #75) Prove if f(X) is an irreducible cubic in $\mathbb{Q}[X]$, the Galois group $G_{\mathbb{Q}}(f)$ is isomorphic either to $\mathbb{Z}_3$ or S_3.

Exercise #76) Prove X^3+2 is irreducible, separable over $\mathbb{Z}_7$.

Exercise #77) If L is the splitting field of X^3+2 over $\mathbb{Z}_7$, compute the degree $[L\ \mathbb{Z}_7]$ and the Galois group $G(L/\mathbb{Z}_7)$.

Exercise #78) If n is an integer and p a prime, such that X^3+n is irreducible but X^2+3 is reducible in $\mathbb{Z}_p[X]$, prove $G(X^3+n/\mathbb{Z}_p) \cong \mathbb{Z}_3$.