Field theory and Galois theory - Briefly !

B.Sury

Field theory happens to be the language in which a number of classical problems can be rephrased and solved. This includes the famous Greek problems of ruler and compass constructions which are more than 2000 years old. This represents a big success story for modern algebra as it also solves completely the problem of solvability by radicals.

• *Splitting fields and algebraic closure*
If $L \supset K$ are fields, L is called a field extension of K. L can be regarded as a K-vector space. The dimension of this vector space is called the degree of L over K and denoted by $[L : K]$.
A basic property that is ubiquitous in field theory is the simple observation that *any field homomorphism from a field K to a field L is injective unless it is the zero map.*
If $L \supset K$ is a field extension, an element $\alpha \in L$ is said to be algebraic over K if it satisfies a non-zero polynomial (in one variable) over K. If α is not algebraic over K, it is said to be transcendental over K. If $K = \mathbf{Q}, L = \mathbf{C}$, the algebraic elements and transcendental elements are simply called the algebraic numbers and the transcendental numbers.
One calls L an algebraic extension of K if each element of L is algebraic over K. It follows from the division algorithm in $K[X]$ that if $\alpha \in L$ is algebraic over K, then it satisfies a unique monic, irreducible polynomial (called its minimal polynomial).
If $\alpha \in L$, one denotes by $K[\alpha]$ and $K(\alpha)$, respectively, the subring and the subfield of L generated by K and α. Explicitly, these are $K[\alpha] = \{$ all finite sums $\sum a_i\alpha^i : a_i \in K\}$ and $K(\alpha)$ is the quotient field of $K[\alpha]$. Similarly, for any subset S of L :, the subring $K[S]$ and the subfield $K(S)$ are defined.
The first important (and easy to prove) result is:
If $L \supset K$ is a field extension and $\alpha \in K$, then the following are equivalent: (i) α is algebraic over K, (ii) $K[\alpha] = K(\alpha)$ i.e., $K[\alpha]$ is a field and, (iii) $[K(\alpha) : K] < \infty$.
Here is the proof. Suppose (i) holds and let α satisfy a nonconstant polynomial f over K. Now, the ring homomorphism $\theta : K[X] \to K[\alpha]$ which evaluates every polynomial at α is surjective. As f is in the kernel, the kernel

is a non-zero ideal. Also, since $K[\alpha] \subset L$, it is a domain and so, Ker(θ) is a non-zero prime ideal. As $K[X]$ is a PID, Ker(θ) is also a maximal ideal i.e, $Im(\theta) = K[\alpha]$ must be a field. This shows (ii) holds if (i) holds.

Assume that (ii) holds and we shall prove (iii). Once again, let us look at the *evaluation-at-*α homomorphism $\theta : K[X] \to K[\alpha]$. As we are given that $K[\alpha]$ is a field, the kernel of θ must be a non-zero maximal ideal. Write $Ker(\theta) = (f)$ say. If deg$(f) = n$, we shall show that $1, \alpha, \cdots, \alpha^{n-1}$ span $K(\alpha)$ (in fact, they form a basis but we do not need it here). But, this is clear from the division algorithm in $K[X]$ because for any $g \in K[X]$, $\theta(g) = \theta(h)$ for some $h \in K[X]$ of degree $< n$. Thus, we have proved that (ii) implies (iii).

Finally, suppose (iii) holds, say $[K(\alpha) : K] = n$. Then, the infinitely many elements $1, \alpha, \alpha^2, \cdots$ cannot be linearly independent over K. Any nontrivial linear relation shows that α is algebraic over K. This completes the proof.

Moreover, repeated applications of the above criterion yields:

If $K \subset L \subset M$, then (i) $[M : K] = [M : L][L : K]$ and, (ii) M is algebraic over K if, and only if, M is algebraic over L and L is algebraic over K.

The first part is proved trivially by verifying that any K-basis $\{v_i\}$ of L and L-basis $\{w_j\}$ of M give rise to the K-basis $\{v_i w_j\}$ of M.

For the second part, start with any $x \in M$. As x is algebraic over L, it satisfies a nonconstant polynomial $f = \sum_{i=0}^n a_i X^i \in L[X]$. Thus, x is algebraic over the field $K(a_0, \cdots, a_n)$. Hence $[K(x) : K(a_0, \cdots, a_n)] < \infty$. Since a_i are algebraic over K, one has $[K(a_i) : K] < \infty$ for all i. Inductively, it is easy to see that $[K(a_0, \cdots, a_n) : K] \leq \prod_{i=0}^n [K(a_i) : K] < \infty$. But, $[K(x) : K] = [K(x) : K(a_0, \cdots, a_n)][K(a_0, \cdots, a_n) : K] < \infty$. Hence, x is algebraic over K. This proves (ii).

As a consequence, it follows that if $L \supset K$ is a field extension, then $L_{alg} = \{\alpha \in L : \alpha \text{ is algebraic over } K\}$, is a subfield of L.

The reason is that if $x, y \in L_{alg}$, then all the elements $x \pm y, xy, x/y$ (if $y \neq 0$) are in $K(x, y)$ which is a finite extension of K.

Let K be a field and $f \in K[X]$ be of positive degree n. Let g be any irreducible factor of f in $K[X]$. Then, the ideal (g) is maximal in $K[X]$ and the quotient field $K_0 = K[X]/(g)$ is a finite extension of K of degree $\leq n$ in which g (and so f) has a root α viz., $X + (g)$. Thus, using the remainder theorem (this is a consequence of the division algorithm) in $K_0[X]$, one has $f = (X - \alpha) f_1$ where $f_1 \in K_0[X]$ has degree $n - 1$. Continuing with f_1 and repeating this procedure, it follows that *there is a finite extension L of K of degree at most $n!$ such that f splits into linear factors in $L[X]$.*

In the above situation, if $\alpha_1, \cdots, \alpha_n$ are all the roots of f (in L), then the field $K(\alpha_1, \cdots, \alpha_n)$ is said to be a splitting field for f.

Any two splitting fields are isomorphic.

We shall prove this soon. First, we show:

If $\sigma : K \to K'$ is an isomorphism of fields and $f = \sum_{i=0}^n a_i X^i \in K[X]$ is monic, irreducible, then $f^\sigma = \sum_{i=0}^n a_i^\sigma X^i \in K'[X]$ is monic, irreducible. Further, if L, L' are field extensions of K, K' respectively and α, α' are roots of f, f^σ in L, L', then there is an isomorphism $\tau : K[\alpha] \to K'[\alpha']$ which sends α to α' and restricts to σ on K.

The proof is as follows. The field $K[X]/(f)$ is isomorphic to $K[\alpha]$ under the map θ which is the evaluation of a polynomial at α. Similarly, $K'[X]/(f^\sigma)$ is isomorphic to $K'[\alpha']$ under the map θ' which evaluates at α'. Then, the isomorphism $\tau = \theta' \circ \sigma \circ \theta^{-1}$ does the job.

Every field K has a unique algebraic closure Ω i.e., Ω is algebraic over K and all nonconstant polynomials in $\Omega[X]$ have roots in Ω. More generally, if $\sigma : K \to K'$ is an isomorphism of fields and Ω, Ω' are algebraic closures of K, K' respectively, there exists an isomorphism $\tau : \Omega \to \Omega'$ such that τ extends σ.

The proof follows by using the result quoted just before this along with an application of Zorn's lemma.

In fact, we prove:

Let L/K be an algebraic extension and let $\sigma : K \to E$ be an embedding of K into an algebraically closed E. Then, there exists an extension of σ to an embedding of L into E. Further, if L is algebraically closed and E is algebraic over $\sigma(K)$, then each extension of σ to L is an isomorphism onto E.

Proof.

Consider the set S of all pairs (M, τ) of intermediate fields between $L \supset M \supset K$ and extensions $\tau : M \to E$ of σ. This is non-empty as $(K, \sigma) \in S$. Clearly, there is a partial order $(M_1, \tau_1) \leq (M_2, \tau_2)$ if and only if $M_1 \subset M_2$ and $\tau_2|_{M_1} = \tau_1$. Each chain has an upper bound (union and the obvious extension). So, by Zorn's lemma, there is a maximal element (L_0, σ_0). If $\alpha \in L - L_0$, then look at $L_0(\alpha)$. There is an extension of σ_0 to $L(\alpha)$ which contradicts the maximality of L_0. Hence $L = L_0$.

Now, if L is algebraically closed, then so is $\sigma(L)$. If E is algebraic over $\sigma(K)$, it is algebraic over $\sigma(L)$ also which means $E = \sigma(L)$.

The algebraic numbers form an algebraic closure of $\mathbf{Q}$. They form a countable set.

• *Separable extensions and normal extensions*

If L is an extension of K, an isomorphism of L onto itself which is the identity map on K, is called a K-isomorphism of L.

Denote by $G(L/K)$, the group of all K-isomorphisms of L.

If Ω is an algebraic closure of a field K, then elements $\alpha, \beta \in \Omega$ are said to be conjugates if $\beta = \sigma(\alpha)$ for some $\sigma \in G(\Omega/K)$.

Let K be a field and Ω an algebraic closure. Then, $\alpha, \beta \in \Omega$ are conjugates if, and only if, they have the same minimal polynomial over K. In particular, an element has only finitely many conjugates.

To see this, first let $\beta = \sigma(\alpha)$ for some $\sigma \in G(\Omega/K)$. If f is $\min(\alpha, K)$, then $0 = \sigma(f(\alpha)) = f(\beta)$ which means $f = min(\beta, K)$ since f is monic and irreducible over K. Conversely, suppose α, β have the same minimal polynomial f. Then, we know that there are isomorphisms $K[X]/(f) \cong K(\alpha)$ and $K[X]/(f) \cong K(\beta)$ which are given by the evaluation maps at α and β. Thus, there is an isomorphism $\sigma : K(\alpha) \to K(\beta)$ which sends α to β and is the identity map on K. As Ω is also an algebraic closure for both $K(\alpha)$ and $K(\beta)$, the isomorphism σ extends to an automorphism of Ω i.e., an element of $G(\Omega/K)$. This proves that α and β are conjugates.

If Ω is an algebraic closure of K and $K \subset L \subset \Omega$, then L is said to be a normal extension of K if, $\sigma(L) = L$ for all $\sigma \in G(\Omega/K)$. This definition depends only on L and K and not on the choice of Ω. For, if Ω' is another algebraic closure of L, look at an L-isomorphism $\theta : \Omega \to \Omega'$. Then, for any $\tau \in G(\Omega'/K)$, the element $\sigma = \theta^{-1} \circ \tau \circ \theta \in G(\Omega/K)$ preserves L. Since $\theta(L) = L$, this gives $\tau(L) = L$ i.e., L is normal over K considered as an algebraic extension contained in Ω'.

The crucial property which characterises normal extensions is:

Let $K \subset L \subset \Omega$ be as above. Then, L is normal over K if, and only if, for any $\alpha \in L$, all roots of its minimal polynomial f over K are in L.

To prove this, first let us assume that L is normal over K. Let $\beta \in \Omega$ be another root of f. Then, the field extensions $K(\alpha)$ and $K(\beta)$ are isomorphic under an isomorphism which carries α to β and is the identity on K. As Ω is an algebraic closure of both these fields, the isomorphism extends to an element $\sigma \in G(\Omega/K)$. As $\sigma(L) = L$, $\sigma(\alpha) = \beta \in L$. For the converse, suppose that all roots of f are also in L. But, any element of $G(\Omega/K)$ must take α into another root of f and thus $G(\Omega/K)$ preserves L i.e., L is normal over K.

Splitting field of a polynomial is a normal extension. Conversely, any finite normal extension is the splitting field of a polynomial.

The proof goes as follows. Suppose $f \in K[X]$ has a splitting field L in an algebraic closure Ω. Without loss of generality, let us take f monic. Let $\alpha_1, \cdots, \alpha_n$ be the roots of f in L. Then, $f = \prod_{i=1}^n (X - \alpha_i)$ in $\Omega[X]$. If $\sigma \in G(\Omega/K)$, then $0 = \sigma(f(\alpha_i)) = f^\sigma(\sigma(\alpha_i)) = f(\sigma(\alpha_i))$. So, $\sigma(\alpha_i)$. Thus, $\sigma(\alpha_i)$ is a root of f in Ω i.e., $\sigma(\alpha_i) = \alpha_j$ for some $j \leq n$. Therefore, $G(\Omega/K)(L) \subset L$ i.e., L is normal over K. Conversely, suppose L is a finite, normal extension of K. Now, let $x_1, \cdots, x_n$ be a K-basis of L. If $f_i \in K[X]$ is the minimal polynomial of x_i over K for any i, then the fact that L is normal shows that all the roots of all the f_i's are in L. Evidently, L is the splitting field of $f_1 \cdots f_n$ over K.

Clearly, if $K \subset L \subset M \subset \Omega$ where Ω is an algebraic closure of K, then since $G(\Omega/L)$ is a subgroup of $G(\Omega/K)$, we have:

If M is normal over K, then M is normal over L.

It can happen that L is normal over K and M is normal over L but M is not normal over K.

Normal extensions are the origin of the notion of normal subgroups. We say more on this soon while discussing Galois theory.

Now, let us prove a statement we made earlier without proof viz.:

Any two splitting fields of a polynomial are isomorphic.

Let $f \in K[X]$ have two splitting fields L, L' in algebraic closures Ω, Ω'. Now, there is a K-isomorphism $\sigma : \Omega \to \Omega'$. Also, in $L[X]$, we have $f = \prod_{i=1}^n (X - \alpha_i)$ where $\alpha_i \in L$ and $L = K(\alpha_1, \cdots, \alpha_n)$. Similarly, in $L'[X]$, $f = \prod_{i=1}^n (X - \alpha'_i)$ with $L' = K(\alpha'_1, \cdots, \alpha'_n)$. But, in the field $\sigma(L) = K(\sigma(\alpha_1), \cdots, \sigma(\alpha_n))$, we have $f = f^\sigma = \prod_{i=1}^n (X - \sigma(\alpha_i))$. As the last two product expressions for f in L' and $\sigma(L)$ are in Ω', it follows that σ_i's and α'_j are permutations of each other. Thus, σ gives a K-isomorphism from L to L'.

An element $\alpha \in \Omega$ is said to be separable over K if it is a simple root of its minimal polynomial. An algebraic extension of K is said to be separable over K if each of its elements is separable.

In this context, it is useful to note:

If f is a monic, irreducible polynomial in $K[X]$, then all roots of f in any algebraic closure of K have the same multiplicity.

To see this and, indeed, to check the separability of any algebraic element, there is a very useful criterion. To check the separability of an element α, it suffices to check $p'(\alpha) \neq 0$ where $p = \sum_{i=0}^n a_i X^i$ is the minimal polynomial of α over K and p' is the 'formal derivative' $\sum_{i=1}^n i a_i X^{i-1} \in K[X]$. This is sometimes called the derivative test for separability. Let us apply this to prove the above assertion. Let α, β be any two roots of f in an algebraic closure Ω of K. Now, $\sigma(\alpha) = \beta$ for some $\sigma \in G(\Omega/K)$. Then, writing $f = (X-\alpha)^r g$ with $g(\alpha) \neq 0$, we get $f = f^\sigma = (X-\beta)^r g^\sigma$. As $g(\alpha) \neq 0$, we have $0 \neq \sigma(g(\alpha)) = g^\sigma(\sigma(\alpha)) = g^\sigma(\beta)$. Thus, β also has multiplicity r in f. This proves the assertion made.

Another application of the derivative test is:

Let $K \subset L \subset M$ be algebraic extensions. Then, if $\alpha \in M$ is separable over K, it is separable over L also.

For, if $f = min(\alpha, K)$, $g = min(\alpha, L)$, then $f = gh$ for some $h \in M[X]$. So, $f' = g'h + gh'$ so that $f'(\alpha) = g'(\alpha)h(\alpha) \neq 0$. So, $g'(\alpha) \neq 0$.

If L, M are extensions of K, one calls a field homomorphism $\sigma : L \to M$ a K-algebra homomorphism if it is the identity on K. Note that the latter property implies that such a map is not the zero map. Further, note that the set $Hom_K(L, M)$ of K-vector space homomorphisms from L to M forms an M-vector space. If L is finite over K, then $\dim_M Hom_K(L, M) = [L : K]$.

(Dedekind's independence theorem)

Let G be any group, E any field and $\theta_1, \cdots \theta_n \in Hom(G, E^*)$ be distinct. Then, the θ_i's are K-linearly independent.

In particular, with K, L, M as above, the set S of all K-algebra homomorphisms from L into M is linearly independent over L. Thus, if L is a finite extension, then this set has at the most $[L : K]$ elements.

We prove the special case as the proof is the same any way. The idea of the proof is to show that given any dependence relation, one can get one of smaller length. Therefore, let us suppose, if possible, that S is a linearly dependent subset of $Hom_K(L, M)$ over M. Let $m_1, \cdots, m_n \in M$ and $\phi_1, \cdots, \phi_n \in S$ such that $\sum_{i=1}^n m_i \phi_i = 0$ in $Hom_K(L, M)$ and n is minimal possible. Then, obviously $n \geq 2$ as $0 \notin S$. Thus, for any $a, b \in L$, then $0 = \sum_{i=1}^n m_i \phi_i(ab) = \sum_{i=1}^n m_i \phi_i(a) \phi_i(b)$. Thus, for any $a \in L$, the element $\sum_{i=1}^n m_i \phi_i(a) \phi_i \in Hom_K(L, M)$ is the zero element. We shall choose $a \in L$ suitably to get a relation of length smaller than n. Multiplying the original relation by $\phi_1(a)$, we have $\sum_{i=1}^n m_i \phi_1(a) \phi_i = 0$.

Subtracting from this the relation $\sum_{i=1}^n m_i \phi_i(a) \phi_i = 0$,

we get $\sum_{i=2}^n m_i(\phi_1(a) - \phi_i(a))\phi_i = 0$.

Choosing $a \in L$ so that $\phi_1(a) \neq \phi_2(a)$ (which is possible as ϕ_1, ϕ_2 are two different elements), we get a dependence relation of length less than n. This contradicts the minimality of n and proves that S is a linearly independent subset of $Hom_K(L, M)$ over M.

Let Ω be an algebraic closure of K and L, a finite extension of K contained in Ω. Then, the index $[G(\Omega/K) : G(\Omega/L)] = |S|$ where S is the set of all K-algebra homomorphisms of L into Ω.

To prove this, consider the restriction map $\eta : Hom_K(\Omega,\Omega) \to Hom_K(L,\Omega)$. Using the extendability of isomorphisms, it is easy to see that $\eta(G(\Omega/K)) = S$. Further, note that $\eta(\sigma) = \eta(\tau) \Leftrightarrow \sigma^{-1}\tau \in G(\Omega/L)$. This proves the result.

The cardinality $|S|$ (which is at the most $[L : K]$), is denoted by $[L : K]_{sep}$ and is called the separability degree of L over K. The fact that subgroup index multiplies in towers implies that the separability degree multiplies in towers. The nomenclature of separability degree is justified by:

An algebraic element α over K is separable over K if, and only if, $[K(\alpha) : K] = [K(\alpha) : K]_{sep}$. More generally, a finite extension L of K is separable if, and only if, its separability degree equals $[L : K]$.

Let us prove the first statement first. Let Ω be an algebraic closure of $K(\alpha)$ and let f be $min(\alpha, K)$. We consider the map $\alpha \mapsto \sigma(\alpha)$ from $G(\Omega/K)$ to the set of conjugates of α. This is onto and two elements $\sigma, \tau \in G(\Omega/K)$ give the same conjugate of α if, and only if, $\sigma^{-1}\tau$ fixes α i.e., belongs to $G(\Omega/K(\alpha))$. In other words, the number of different conjugates of α equals the index $G(\Omega/K) : G(\Omega/K(\alpha))] = [K(\alpha) : K]_{sep}$. Now, recalling that an irreducible polynomial has all its roots to be of the same multiplicity, it follows that α is separable over K if, and only if, all roots of f are simple i.e., α has deg(f) number of conjugates. As deg$(f) = [K(\alpha) : K]$, it follows that α is separable if, and only if, the separability degree and the full degree of $K(\alpha)$ over K coincide.

Now, let us prove the second statement by the multiplicativity of the usual degree on using induction and the upper bound $[L : K]_{sep} \leq [L : K]$. If $[L : K] = 1$, then $L = K$ and there is nothing to prove. Assume $[L : K] > 1$ and that the assertion holds for smaller degree extensions. Let $\alpha \in L$, $\alpha \notin K$. Then, $[L : K(\alpha)] < [L : K]$. If L is separable over K, then α is separable over K and L is separable over $K(\alpha)$. So, by the induction hypothesis and the first assertion proved above, we have $[L : K] = [L : K(\alpha)][K(\alpha) : K] = [L : K(\alpha)]_{sep}[K(\alpha) : K]_{sep} = [L : K]_{sep}$.

Conversely, suppose these two degrees coincide. Then, $[L : K] = [L : K(\alpha)][K(\alpha) : K] \geq [L : K(\alpha)]_{sep}[K(\alpha) : K]_{sep} = [L : K]_{sep} = [L : K]$ which shows that equality holds in the intermediate step too. Hence, $[K(\alpha) : K] = [K(\alpha) : K]_{sep}$ i.e., α is separable over K. As α was an arbitrary element of L outside K, it follows that L is separable over K.

Unlike normal extensions, separable extensions have the following property: *If $K \subset L \subset M$ are algebraic extensions, then M is separable over K if, and only if, M is separable over L and L is separable over K.*
It has already been observed that if M is separable over K, then it is separable over L and also L is separable over K. Assume now that both L/K and M/L are separable extensions. Let $\alpha \in M$ and $f = \sum_{i=0}^{n} a_i X^i = min(\alpha, L)$. Then, evidently, $f = min(\alpha, K_0)$ where $K_0 = K(a_0, \cdots, a_{n-1})$. Now, α is separable over K_0, being a simple root of f. Thus, $[K_0(\alpha) : K_0] = [K_0(\alpha) : K_0]_{sep}$. On the other hand, $K_0 \subset L$ implies that K_0 is separable over K. It is also evidently, a finite extension of K. Thus, $[K_0 : K] = [K_0 : K]_{sep}$. By multiplicativity of both the usual degree and the separability degree, it follows that $K_0(\alpha)$ is separable over K. In particular, α is separable over K.

For a finite extension L/K, there is a notion of trace and one of norm. For any $a \in L$, one can regard the map $T_a : L \to L$ which sends b to ab. This is clearly a K-linear transformation of L. Its trace and determinant are called, respectively, the trace and the norm of a over K and denoted by $Tr_{L/K}(a)$ and $N_{L/K}(a)$. For a finite extension L/K, the bilinear form

$$L \times L \to K \ ; \ (x, y) \mapsto Tr_{L/K}(xy)$$

is called the trace form and if L is also separable, this form is non-degenerate. This result is very useful in number theory. We briefly discuss the trace and norm maps in the next section.

Let L_0, L_1 be extensions of K contained in a field L. Define L_0, L_1 to be *linearly disjoint over* K if a subset of L_i is K-linearly independent if and only if it is L_{1-i}-linearly independent for $i = 0, 1$.
Two linearly disjoint extensions L_0, L_1 over K must intersect only in K clearly, However, the converse is not true (because of the result below which says that linear disjointness implies degree multiplies).
Indeed, if L_0, L_1 are pure cubic extensions of $K = \mathbf{Q}$ generated by two cube roots of 2, then the composite has degree 6 while the intersection of the fields is $\mathbf{Q}$.

We have:
L_0, L_1 are linearly disjoint over K if, and only if, the canonical map of K-vector spaces $\theta : L_0 \otimes_K L_1 \to L_0L_1$ is an isomorphism.
Proof.

Indeed, if $\{v_i\}$ is any K-basis of L_0, then each element of the tensor product is uniquely expressible as $\sum_{finite} v_i \otimes w_i$ with $w_i \in L_1$. If L_0, L_1 are linearly disjoint over K, then any element of Ker θ is a sum as above which is zero, must already be zero (as all w_i's must be zero).
Conversely, if θ is an isomorphism, then look at any K-basis $\{v_i\}$ of L_0 such that $\sum_{finite} v_i \otimes w_i = 0$ for some $w_i \in L_1$. By the fact that θ is injective, the above sum is non-zero unless each $w_i = 0$.
As a consequence of the above result, we have:
The composite of two extensions L_0, L_1 of K has degree equal to the product of the degrees if, and only if, L_0, L_1 are linearly disjoint over K.

Define an algebraic element of L/K to be *purely inseparable* if char $K = p > 0$ and $\alpha^{p^n} \in K$ for some $n \geq 0$.
We have:
Let L/K be a finite extension, where char $K = p > 0$. Then, $[L : K]_{sep} = 1$ if, and only if, each $\alpha \in L$ is purely inseparable over K. These happen if, and only if, for each $\alpha \in L$, min $(\alpha, K) = X^{p^n} - a$ for some $a \in K$.
Proof.
Suppose $[L : K]_{sep} = 1$. Let $\alpha \in L$. Then, $[K(\alpha) : K]_{sep} = 1$ as it divides the former. Thus, the minimal polynomial of α over K has only one distinct root. So, $\min(\alpha, K) = (X - \alpha)^r$ for some r. Writing $r = p^n t$, we have

$$min(\alpha, K) = (X^{p^n} - \alpha^{p^n})^t = X^{p^n} - t\alpha^{p^n} X^{p^n(t-1)} + \cdots$$

So $t\alpha^{p^n} \in K$ which gives since $(t, p) = 1$, that $\alpha^{p^n} = a \in K$ for some a. Thus, the first property of the statement implies the second.
But then $X^{p^n} - a$ has α as a root which means this must be the minimal polynomial of α over K. Thus, the second statement implies the third.
Finally, the third statement implies that there is only one K-embedding of $K(\alpha)$ into an algebraic closure, as it must send α to a root of the minimal polynomial of α which has only one root. As this is true for each $\alpha \in L$, we have only one K-embedding of L; that is, $[L : K]_{sep} = 1$.

• *Trace and norm*
The definitions have been given above. The basic properties which follow immediately from their definitions are :
$K \subseteq L \subseteq M \Rightarrow N_{M/K} = N_{L/K} \circ N_{M/l}$.
$N_{E/F}$ *is multiplicative.*
A useful result is :

Let $[L:K]=n$. If $a \in L$ has $Min(a,K) = p(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0$, then

$$N_{L/K}(a) = (-1)^n a_0^{n/m} \ , \ tr_{L/K}(a) = -\frac{n}{m}a_{m-1}.$$

In particular, if L is purely inseparable over K, the trace map is the zero map.

The last statement follows from the first one since the minimal polynomial in the purely inseparable case is of the form $X^{p^n} - c$. The first statement is proved as follows. The map $a \mapsto L_a$ from L to $End_K(L)$ which defines the norm and trace, is a ring homomorphism. It is injective. Therefore, $p(X)$, the minimal polynomial of a, is also the minimal polynomial of the linear transformation L_a. But, the minimal polynomial of any linear transformation divides its characteristic polynomial and has the same irreducible factors. Since $p(X)$ is irreducible, this means that $\chi(L_a, X) = p(X)^{n/m}$. Compare coefficients to get the result.

One can also prove:

Let L/K be finite and let $\sigma_1, \cdots, \sigma_r$ be the distinct K-embeddings of L in $\bar{K}$. Then

$$N_{L/K}(a) = (\prod_{i=1}^{r} \sigma_i(a))^{[L;K]_{insep}},$$

$$tr_{L/K}(a) = [L:K]_{insep} \sum_{i=1}^{r} \sigma_i(a).$$

In particular, if L/K is separable, the trace map is not the zero map. Further, in particular, if L/K is Galois with Galois group G, the above expressions become

$$N_{L/K}(a) = \prod_{g \in G} g(a) \ , \ tr_{L/K}(a) = \sum_{g \in G} g(a).$$

• *Finite fields*

Any finite field has cardinality the power of a prime.

The reason is, it has to be of finite degree over the field $\mathbf{Z}_p$ for some prime p. Regarded as a field, $\mathbf{Z}_p$ is usually denoted by $\mathbf{F}_p$.

The multiplicative group $F^* = F \setminus \{0\}$ is a cyclic group.

This follows from the group-theoretic fact that a finite group in which for every d, there are at the most d elements satisfying $g^d = 1$, must be cyclic.

Any two finite fields of the same cardinality are isomorphic.

To see why, observe first that in an algebraic closure Ω of $\mathbf{F}_p$, the subset

$F = \{\alpha : \alpha^{p^n} = \alpha\}$ is clearly a field of cardinality p^n since the roots of the polynomial $X^{p^n} - X$ are distinct. Thus, F is the splitting field of this polynomial. Conversely, in any field of cardinality p^n, all the elements satisfy this polynomial. Thus, we have proved the stronger statement:
Up to isomorphism, the unique field with p^n elements is the splitting field over $\mathbf{F}_p$ of the polynomial $X^{p^n} - X$.

Here is an observation:
The norm and trace maps on finite extensions of finite fields are surjective.
Indeed, $E = \mathbf{F}_{p^{nd}} \supset F = \mathbf{F}_{p^n}$ have respective generators α and $\alpha^{|E^*|/|F^*|}$. Clearly, the norm of α is

$$\alpha^{1+p^n+p^{2n}+\cdots+p^{n(d-1)}}$$

which is $\alpha^{|E^*|/|F^*|}$.

The following provides a nice way to count of the number N_k of monic irreducible polynomials of a given degree k over a finite field $\mathbf{F}_q$.
As $\mathbf{F}_q[X]$ is a UFD, we have

$$\sum_{f\ monic} T^{deg(f)} = \prod_{g\ monic\ irred} \frac{1}{1 - T^{deg(g)}}$$

So,

$$\sum_n q^n T^n = \prod_k (1 - T^k)^{-N_k}$$

Adding 1 and taking log, we get

$$\sum_n \frac{q^n T^n}{n} = \sum_k N_k (\sum_r \frac{T^{rk}}{r} = \sum_d (\sum_{kr=d} \frac{N_k}{r}) T^d$$

Comparing like powers, we get

$$q^n = \sum_{k|n} k N_k.$$

• *Simple extensions*
An extension L of K is said to be simple (or primitive) if there is some $\alpha \in L$

such that $L = K(\alpha)$. One of the beautiful results proved by Galois is:
(Primitive element theorem)
Any finite, separable extension is simple.
The proof over a finite field is a consequence of the fact that the multiplicative group of such a field is cyclic. Over infinite fields, the proof is as follows. Let L be a finite, separable extension of K. Consider the set S of all the K-homomorphisms from L into an algebraic closure Ω. Write $S = \{\sigma_1, \cdots, \sigma_n\}$. Look at the vector K-subspaces $V_{ij} = \{x \in L : \sigma_i(x) = \sigma_j(x)\}$ for all $i \neq j$. Obviously, $n = [L : K]$ by separability and so V_{ij} is a proper subspace of L. Since K is an infinite field, the fact that the finite-dimensional vector space L cannot be the union of finitely many proper subspaces V_{ij} proves that there is some $\alpha \in L$ outside each V_{ij}. In other words, α has n different conjugates in Ω. Therefore, $[K(\alpha) : K] = n = [L : K]$. So $L = K(\alpha)$. This proves the theorem.

Corollary. *If L/K is separable algebraic, and if $[K(\alpha) : K] \leq n$ for each $\alpha \in L$, then L/K is finite (and hence simple) of degree $\leq n$.*
Here is the proof. If $\alpha \in L$ has the largest degree m, then if $K(\alpha) \neq L$, we would have some $\beta \in L - K(\alpha)$. But, then $K(\alpha, \beta)$ would be a finite (therefore, simple) extension of degree $> m$ over K, a contradiction.

Here is another criterion for simplicity of a finite extension.
Let L be a finite extension of K. Then, L is a simple extension if, and only if, there are only finitely many intermediate fields.
To prove this, we first suppose that L is a simple extension, say, $L = K(\alpha)$. If f is the minimal polynomial of α over K, then for any intermediate field K_0, the minimal polynomial of α over K_0 will be a divisor of f. As $L[X]$ is a UFD, the set S of irreducible factors of f is finite. Consider the map from the set S' of intermediate fields to the set S given by sending any K_0 to $\min(\alpha, K_0)$. We claim that this is a 1-1 map. This would establish that S' is finite. Suppose $min(\alpha, K_1) = min(\alpha, K_2) = g$ say. If $g = \sum_{i=0}^{n} a_i X^i$, then evidently, $g = min(\alpha, K_0)$ where $K_0 = K(a_0, \cdots, a_n)$. As K_0 is contained in K_1 and in K_2 and the degree of L over each of these fields is n, they are equal i.e., $K_1 = K_2 = K_0$.
Conversely, suppose that there are only finitely many intermediate fields. We may assume that K is infinite. Now $L = K(x_1, \cdots, x_n)$ for some elements x_i. We prove by induction on n that L is simple. It suffices to show for $n = 2$. Look at the extensions $K(x_1 + tx_2)$ as t varies over K. As K is infinite, the

finiteness assumption forces the existence of two (indeed, infinitely many) distinct elements $a, b \in K$ such that $K(x_1 + ax_2) = K(x_1 + bx_2) = K_0$ say. Thus, both $x_1 + ax_2, x_1 + bx_2$ belong to K_0. So, does their difference, which shows that both x_1, x_2 do too. Hence, $K(x_1, x_2) = K_0$ which is a simple extension.

Q 8, P. 216 from Jacobson's Basic Algebra I.
Let $K(t) \supset L \supset K$ where $L \neq K$. We claim that t is algebraic over L. More precisely, if $a \in L - K$, we write $a = f(t)/g(t)$ in reduced form and show that $[K(t) : K(a)] = max(deg(f), deg(g))$.
Now, the polynomial $h(X) := f(X) - ag(X) \in K(a)[X]$ has t as a root. This is not the zero polynomial; otherwise, a would be in K.
Indeed, the degree of the polynomial $h(X)$ is max(deg(f),deg(g)); otherwise, again we would have $deg(f) = deg(g)$ and $ab_n = a_n$ with a_n, b_n top coefficients of g, f respectively. This again gives a contradiction as $a \notin K$. So, we have shown that t is algebraic over $K(a)$ (and hence over $L \geq K(a)$ also).
Note that a is not algebraic over K; otherwise, the degree of $K(t)$ over K would be finite which is absurd.
So, $K[a]$ is isomorphic to the polynomial ring.
Now, $h(X) = f(X) - ag(X) \in K[X][a] \subset K(X)[a]$ is a degree 1 polynomial (in a) over $K(X)$. So, it is irreducible over $K(X)$.
As f, g are relatively prime in $K[X]$, $h = f - ag$ is primitive in $K[X][a]$ and, therefore, irreducible over $K[X]$.
So, $h = f - ag \in K[a][X] = K[X][a]$ is irreducible over $K[a]$ as a polynomial in X. Therefore, h is irreducible over $K(a)$. In other words, $h = min(t, K(a))$.

Q 10, P.14 of Morandi.
Let L/K be an extension and let $a \in L$ have $[K(a) : K]$ odd. Then, we claim that $K(a) = K(a^2)$. Indeed,

$$[K(a) : K] = [K(a) : K(a^2)][K(a^2) : K]$$

is odd while the first degree is 1 or 2. This implies the first degree is 1.

Q 11, P.14 of Morandi.
If L/K is algebraic and $K \subset A \subset L$ is a subring, then we claim that A is a field. If $0 \neq a \in A$, then $a \in L$ and so, it is algebraic over K. Thus, $K(a) = K[a]$ is a field so that a has an inverse in $K[a] \subset A$.

Q 12, P.14 of Morandi.
If $m \neq n$ are square-free positive integers, then we claim that neither of the two fields $\mathbf{Q}(\sqrt{\pm m})$ is isomorphic to either of the two fields $\mathbf{Q}(\sqrt{\pm n})$.
This is clear because any non-zero homomorphism of fields is injective and

none of the four fields contains a square-root of any of one of the other three integers.

Q 19, P.14 of Morandi.
Consider $L_1 = \mathbf{Q}(\sqrt{2})$ and $L_2 = \mathbf{Q}(\zeta_8) = \mathbf{Q}(e^{i\pi/4})$. Then, L_1, L_2 have degrees 2 and 4 over $\mathbf{Q}$. However, $L_1 \subset L_2$ because

$$\sqrt{2} = \zeta_8 + \zeta_8^{-1}$$

Q 20, P.14 of Morandi.
We claim that there exist cubic extensions K of $\mathbf{Q}$ which are not pure cubic; that is, $K \neq \mathbf{Q}([3]\sqrt{n})$ for any integer n.
By the way, we note that unlike quadratic fields, pure cubic fields do not determine a cube-free n as above - cube-free integers ab^2 and a^2b give the same pure cubic field.
There are many examples of non-pure cubic fields but we give one example first.
If $K = \mathbf{Q}(\alpha)$ where α is a root of $X^3 - 3X + 1 = 0$. It is easy to see that it has three real roots in the intervals $(-2, 0), (0, \sqrt{2}), (\sqrt{2}, \sqrt{3})$. In fact, if $\theta < 0$ is the negative root, then the other roots are

$$\alpha = \theta^2 - 2 \ , \ \beta = 2 - \theta - \theta^2.$$

This is gotten from the equalities

$$\alpha + \beta = -\theta \ , \ \alpha\beta = \theta^2 - 3.$$

Therefore, K is a normal extension being the splitting field of $X^3 - 3X + 1$ over $\mathbf{Q}$. Note that a pure cubic field cannot be a normal extension. This gives our example.
More generally, we will prove later that the field automorphisms of a splitting field of an irreducible polynomial of degree n over $\mathbf{Q}$ is a subgroup of S_n which is contained in A_n if and only if, the discriminant of the polynomial is a perfect square.
A class of examples when this automorphism group is A_3 (that is, irreducible cubics for which discriminant is a square) is $X^3 - aX - a$ where a is an odd integer of the form $r^2 + r + 7$.
In fact, discriminant of $X^3 - aX - a$ is $4a^3 - 27a^2 = a^2(4a - 27)$. This is a square if $4a - 27 = b^2$; that is, $b^2 = 4(r^2 + r + 7) - 27 = (2r + 1)^2$.

Q 1, P.24 of Morandi.
If σ is an automorphism of $\mathbf{Q}$ it is clearly identity on $\mathbf{Z}$. So, for $n > 0$,

$$n\sigma(m/n) = \sigma(m) = m \Rightarrow \sigma(m/n) = m/n.$$

Q 2, P.24 of Morandi.
If σ is an automorphism of $\mathbf{R}$, then it is identity on $\mathbf{Q}$. Also, for any $t \in \mathbf{R}$,

$$\sigma(t^2) = \sigma(t)^2$$

which implies $\sigma(x - y) > 0$ whenever $x > y$.
Thus, σ is an order-preserving map on $\mathbf{R}$. But, then it is continuous - indeed, if c is real and $\epsilon > 0$ is given, choose $\delta \in \mathbf{Q}$ such that $0 < \delta < \epsilon$; then for each $c - \delta < x < c + \delta$, we have

$$\sigma(c) - \epsilon < \sigma(c) - \delta = \sigma(c) - \sigma(\delta) < \sigma(x) < \sigma(c) + \sigma(\delta) < \sigma(c) + \delta < \sigma(c) + \epsilon$$

Thus, σ is continuous and is the identity on the rationals. So, it is the identity map on the whole of reals.

Q 6,7 of P.37 of Morandi.
Clearly, the assertion of problem 6 implies that of 7. Let us prove 6.
Let $L = K(a)$ be of degree n over K and let F/K be of degree m coprime to n. We claim that $min(a, K)$ is irreducible over F. Equivalently, we claim that $[F(a) : F] = n$. Consider the composite $F(a)$ of F and $K(a)$. Then,

$$[F(a) : K] = [F(a) : K(a)][K(a) : K] = n[F(a) : K(a)]$$

$$= [F(a) : F][F : K] = m[F(a) : F].$$

So, n divides $[F(a) : F]$. However, a satisfies a polynomial of degree n over F (the minimal polynomial over K); so, the degree equals n.

Q 12 of P.38 of Morandi.
We show that if G is any subgroup of $Aut(L)$ for any field L and $K = L^G$, then K is a subfield and either L is not algebraic over K or, it is algebraic and normal over K.
Clearly, K is a subfield. If L/K is not algebraic, there is nothing to prove. Assume that L/K is algebraic. To prove that L is normal, we prove the equivalent property that whenever an irreducible polynomial $f \in K[X]$ has

a root in L, it splits completely in $L[X]$.
Consider any $a \in L$. We look at the orbit $G.a$ of a under G. Since elements of G act as the identity on K, the minimal polynomial $min(a, K) = \sum_{i=0}^n c_i X_i$ is fixed by any element $g \in G$ and so, we have:

$$0 = g(\sum_{i=0}^n c_i a^i) = \sum_{i=0}^n c_i g(a^i) = \sum_{i=0}^n c_i g(a)^i.$$

Thus, each element $g(a)$ of the orbit of $G.a$ is a root of $min(a, K)$ inside L. Thus, the orbits are finite. Write $G.a = \{\sigma_1(a), \cdots, \sigma_r(a)\}$ say. Then, the r symmetric polynomials in $\sigma_1(a), \cdots, \sigma_r(a)$ are fixed by G. But, then the polynomial

$$\prod_{i=1}^r (X - \sigma_i(a))$$

has coefficients which are fixed by G which means it is in $K[X]$. Therefore, the minimal polynomial $min(a, K)$ divides the above polynomial in $K[X]$; in particular, all its roots are in L.

Miscellaneous problem.
If L is an algebraically closed extension of a field K, then we claim that the algebraic closure of K in L is algebraically closed.
Indeed, if L_{alg} denotes the algebraic closure of K in L, then consider any monic, irreducible $f \in L_{alg}[X]$. As L is algebraically closed and as f can be regarded as a polynomial over L, it has a root $a \in L$. So, a is algebraic over L_{alg}. But then a is algebraic over K itself. So, $a \in L_{alg}$. Hence, $f(X) = X - a$.

Miscellaneous problem.
If K is an infinite field, then we claim that the additive subgroup of K is not finitely generated.
Indeed, if K is any field for which the additive subgroup K^+ is isomorphic to $\mathbf{Z}^n \times T$ for some finite abelian group T, then $2K^+$ is an ideal in K which means it must be 0 or K. If $n > 0$, clearly $2K^+$ is a proper, non-zero ideal of K. Hence, $K^+ = T$ in case it is finitely generated and, hence K is finite.

Miscellaneous problem.
Let $f = X^4 - 5X^2 - 6X + 3$ and $g = X^5 - 8X^3 + 9X - 3$. We claim that there is a unique quadratic field over which f, g have a common root. We

want to determine that field and the common roots there.
By the Euclidean algorithm, we can obtain $(f, g) = (X^2 - 3X + 1)$ in $\mathbf{Q}[X]$. The GCD polynomial has two roots $(3 \pm \sqrt{5})/2$ in $\mathbf{Q}(\sqrt{5})$.

Miscellaneous problem.
We wish to determine the characteristics of the field for which the polynomial $X^4 + X + 1$ can have multiple roots. In that case, we wish to determine the multiple roots also.
If θ is a multiple root, then

$$\theta^4 + \theta + 1 = 0$$

$$4\theta^3 + 1 = 0$$

So $4\theta^4 + \theta = 0$ and $4\theta^4 + 4\theta + 4 = 0$; these give

$$3\theta + 4 = 0.$$

So, characteristic is $\neq 3$ and $\theta = -4/3$.
Putting this value in $4\theta^3 + 1 = 0$, we have $229 = 0$. As 229 is a prime, this is the characteristic. Moreover, the second derivative $12\theta^2 \neq 0$, So, the characteristic is 229, the multiple root is $-4/3 = 4 \times 76 = 304$; it is a double root.

Miscellaneous problem.
Let char $K = p > 0$. Then, we claim that $E = K(X, Y)$ is a non-simple extension of degree p^2 over $F = K(X^p, Y^p)$. In fact, we can show that $E_i = F(X^{ip+1} + Y)$ are distinct intermediate subfields. Note that for a simple extension of degree n, there are at the most 2^n intermediate fields.

• *Galois theory*

A finite extension L of K is said to be Galois over K if it is separable and normal over K. Let us denote by $G(L/K)$, the K-automorphisms of L. It follows from the above discussion that:

If L is a Galois extension of degree n over K, then $|G(L/K)| = n$.

For, if Ω is an algebraic closure of L, then any $\sigma \in G(\Omega/K)$ leaves L stable and thus there is a well-defined homomorphism from $G(\Omega/K)$ to $G(L/K)$ viz., the restriction of an automorphism. Evidently, it is surjective and has kernel $G(\Omega/L)$. Thus, $|G(L/K)| = [G(\Omega/K) : G(\Omega/L)] = [L : K]_{sep} = [L : K] = n$.

In this case, the group $G(L/K)$ is called the Galois group of the Galois extension L of K.

Here is an equivalent definition due to Emil Artin of a finite extension to be Galois:

(i) *A finite extension L/K is Galois if, and only if, $L^{G(L/K)} = K$.*

(ii) *Let L be any field and G be a finite group of automorphisms of L. Then, L is Galois over L^G with Galois group G.*

Here is the proof of (i).

For (i), first assume that L/K is Galois. Now, $K \subseteq L^{G(L/K)}$ evidently. If $\alpha \in L - K$, we will show there exists $\sigma \in G(L/K)$ such that $\sigma(\alpha) \neq \alpha$ (which would imply $\alpha \notin L^{G(L/K)}$). Now, $\alpha \notin K$ implies its minimal polynomial over K has another root $\beta \neq \alpha$. The map $\sigma : \alpha \mapsto \beta$ clearly extends to an element of $G(\Omega/K)$; this $\sigma \in G(L/K)$ as L is normal.

Conversely, now suppose that $L^{G(L/K)} = K$. Let $\alpha \in L$ and let $\sigma_1(\alpha), \cdots, \sigma_r(\alpha)$ be the distinct elements of the $G(L/K)$-orbit of α. Then, the polynomial

$$f = \prod_{i=1}^{r} (X - \sigma_i(\alpha))$$

satisfies $\sigma(f) = f$ for each $\sigma \in G(L/K)$. This is because $\sigma\sigma_i(\alpha)$ are distinct for $i = 1, \cdots, r$ and are among the $\sigma_i(\alpha)$. So $f \in K[X]$ by the hypothesis. So, min (α, K) divides f. As f has distinct roots, so does min (α, K) and hence α is separable. So, L is separable. Also, the conjugates of α are among $\sigma_i(\alpha)(1 \leq i \leq r)$; so, they are in L. Thus, we have shown that L is normal also. So, L is a Galois extension. Thus, (i) is proved.

The proof of (ii) is exactly the same excepting the last assertion that $G(L/L^G) = G$. To see this, we put $K = L^G$ and note that the proof above shows for each

$\alpha \in L$ that $[K(\alpha) : K] \leq O(G)$. An earlier corollary shows then that L itself has degree $\leq O(G)$ and can be expressed as $K(\beta)$ for some β. But, clearly $O(G)$ is at the most the number of conjugates of β which is the degree of $L = K(\beta)$ over K. Hence, we have equality $O(G) = [L : K]$. As the latter has order $|G(L/K)|$ and as $G \leq G(L/K)$, we must have equality of groups.

Now, we can prove:

(Fundamental theorem of finite Galois theory)

Let L be a finite Galois extension of K with Galois group $G(L/K)$. Then, there is a bijection :

$$\{E : K \subset E \subset L\} \leftrightarrow \{H : H \leq G\}$$

given by $\phi : E \mapsto G(L/E)$ whose inverse is $\psi : H \mapsto L^H$. Here L^H denotes the fixed subfield under H.

Furthermore, an intermediate field E is Galois over K if, and only if, the subgroup $H := G(L/E)$ of $G := G(L/K)$ is normal; in this case the Galois group of E over K is isomorphic to the quotient group G/H.

The proof goes as follows. First, we show that $\psi \circ \phi$ is the identity map on the set S of intermediate fields. Let $E \in S$ and write H for $G(L/E) = \phi(E)$. Then, $\psi \circ \phi(E) = \psi(H) = L^H$. Now, obviously, since H fixes E, we have $E \subset L^H$. Thus, $H = G(L/E) \supset G(L/L^H)$. But, by definition, $H \subset G(L/L^H)$; hence we must have $H = G(L/L^H)$. On the other hand, L is a Galois extension of L^H as well as of E and the corresponding Galois groups $G(L/L^H)$ and $G(L/E)$ have orders equal to the corresponding degrees $[L : L^H]$ and $[L : E]$ respectively. Thus, $[L : L^H] = |G(L/L^H)| = |H| = |G(L/E)| = [L : E]$. Since $E \subset L^H$, we must have $E = L^H$ i.e., $\psi \circ \phi = Id_S$.

Conversely, let H be any subgroup of G and write E for $\psi(H) = L^H$. Then, $H \subset G(L/E)$. As L is separable over K, we may write $L = K(\alpha)$. Look at the polynomial $f(X) = \prod_{h \in H}(X - h(\alpha))$. This is a monic polynomial of degree $|H|$ such that $f(\alpha) = 0$. Furthermore, $\forall \sigma \in H$, $f^\sigma(X) = f(X)$. Therefore, $f \in E[X]$. Since $L = K(\alpha) = E(\alpha)$, we have $[L : E] \leq deg(f) = |H| \leq |G(L/E)| = [L : E]$. Thus, all these are equalities and we have $H = G(L/E) = \phi(E) = \phi(L^H) = \phi \circ \psi(H)$. This proves the converse.

Finally, let E be an intermediate field. Suppose E is Galois over K. Write H for $G(L/E)$.Then, for any $\sigma \in G(L/K)$, we have $\sigma(E) \subset E$ and hence we have a well-defined 'restriction' homomorphism $\theta : G(L/K) \to G(E/K)$. It is evident that $ker(\theta) = G(L/E) = H$ and so H is normal. Now, let us suppose that H is normal in G. Write $E = L^H$. We need to show that E is normal over K. Let $x \in E$ and $\sigma \in G(L/K)$. Then, we want to show that $\sigma(x) \in E = L^H$. So, suppose $h \in H$. Then, $h\sigma(x) = \sigma\sigma^{-1}h\sigma(x) = \sigma(x)$ since H is normal and fixes all of E. Thus, $\sigma(x) \in L^H = E$ i.e., E is normal over K. Thus, E is a Galois extension of K. In this case, the restriction map $\theta : G(L/K) \to G(E/K)$ has kernel $G(L/E)$ and is surjective because we can extend any element of $G(E/K)$ to an element of $G(L/K)$. The proof is complete.

It is not difficult to develop a little bit of group-theoretic machinery to prove a more general version valid for infinite Galois extensions. In that case, the Galois group which is an infinite group can be given a natural topology such that the correspondence is between subfields and closed subgroups.

One can prove also the fundamental theorem of algebra using the fundamental theorem of Galois theory as follows.
Let $L/\mathbf{C}$ be any finite extension. Observe two facts: (i) $\mathbf{R}$ has no proper odd degree extensions and (ii) $\mathbf{C}$ has no quadratic extension. The first follows by using the mean-value theorem of real analysis to show that every odd degree real polynomial has a real root. The second follows by our ability to explicitly write the roots of a quadratic complex polynomial by completing squares.
Now, let N be the normal closure of L over $\mathbf{R}$. Write $G = Gal(N/\mathbf{R})$. If P is a 2-Sylow subgroup of G, then $N^P = \mathbf{R}$ being an odd degree extension. Thus, by the fundamental theorem, $P = G$ i.e., G is a 2-group. Write $O(G) = 2^n$ with $n \geq 1$. If $n > 1$, then $H = Gal(N/\mathbf{C})$ would have order $2^{n-1} \geq 2$ and, subgroup of index 2 in it would give a quadratic extension of $\mathbf{C}$. Thus $n = 1$ i.e., $H = e$ i.e., $N = L = \mathbf{C}$.

Finally, here is a nice result using the fundamental theorem of Galois theory:
Let $\alpha \in \mathbf{C}$ be an algebraic number and let K be a subfield of the algebraic closure of $\mathbf{Q}$ which is maximal with respect to the property that $\alpha \notin K$. (Such a field exists by Zorn's lemma). Then, any finite extension of K is a Galois extension which is cyclic.
Proof.
Let L/K be any finite extension and let N be the normal closure of L over K. Call $G = Gal(N/K)$. Let $g \in G$. If the cyclic group $< g > \neq G$, then its

fixed field N^g is a proper extension of K in N. By the definition of K, this means that $\alpha \in N^g$ i.e., $g(\alpha) = \alpha$. So, if every g is such that $< g > \neq G$, this would give that $g(\alpha) = \alpha$ for all $g \in G$. Thus, we would have $\alpha \in N^G = K$, a contradiction. Hence, there does exist some $g \in G$ so that $< g >= G$ i.e., G is cyclic. Now, as $L \subseteq N$, we have $L = N^H$ for some subgroup H of G. As G is cyclic (and therefore abelian), H is a normal subgroup. But this means that L is Galois over K i.e. $N = L$. This proves that L/K is cyclic.

• *Ruler and compass constructions*
Two points are given on the plane as constructed. These are taken to be at unit distance and the line is taken to be the X-axis. Given a ruler (which cannot measure lengths but can only draw straight lines) and a compass which can draw circles, one wants to know what other points on the plane can be marked off and what figures can constructed by these implements alone. Such points and such distances which can be marked off in a finite number of steps are said to be constructible. The ancient Greeks asked :
(i) is it possible to trisect any given angle? (ii) given a cube is it possible to construct another with double the volume? (iii) given a circle, is it possible to construct a square with the same area? (iv) which regular polygons are constructible?
It turns out that these 2000-year old problems were solved only after the advent of field theory.
The following constructions can be recalled from high school geometry: (i) drawing a perpendicular through a given point on a given line, (ii) drawing a line through a given point parallel to a given line, (iii) given a segment, marking off a segment of the same length starting at a given point on another given line.
Thus, it is clear that a point (a, b) is constructible if, and only if, the distances $|a|$ and $|b|$ can be constructed. Notice that we can draw a triangle similar to a constructed triangle with two sides of already constructed lengths.
The main result is:
A real number α is constructible if, and only if, there is a tower of fields $\mathbf{Q} = K_0 \subset K_1 \subset \cdots \subset K_r$ with $\alpha \in K_r$ and $[K_i : K_{i-1}] \leq 2$. In particular, if a real number α is conctructible, then it is an algebraic number of degree a power of 2.
The proof is as follows. Let α be a real number which has been constructed after a finite number of steps. Then, $|\alpha|$ is the distance between two points of which either one or both appear as a point of intersection of two lines,

two circles or a circle and a line based at points which have been constructed earlier and with radii which are numbers constructed earlier. A circle based at a constructed point (a, b) and with a constructed radius r has an equation of the form $(x-a)^2 + (y-b)^2 = r^2$. A constructed line has an equation of the form $lx + my + n = 0$ where l, m, n are already constructed numbers. The points of intersection (which are either $0, 1$ or 2) are obtained by solving them simultaneously. Thus, the solutions are in a quadratic extension of a field generated by already constructed numbers. Thus, inductively, it follows that α is in a finite tower of quadratic extensions starting from $\mathbf{Q}$, elements of which are constructed numbers.

We need to prove the converse, viz., that for any finite tower of quadratic extensions contained in the real field, any element is constructible. Once again, by induction, it suffices to establish that if $F \subset \mathbf{R}$ is a field consisting of constructible numbers, then the elements of any real quadratic extension $F(\sqrt{d})$ are constructible too. It is clear that it amounts to showing that $\sqrt{d}$ is constructible whenever d is. Draw a circle with diameter $1 + d$ and at a distance d draw a perpendicular to the diameter. The length of this perpendicular segment within the circle is then $\sqrt{d}$. Thus, the result is proved.

Let us now point out how the result at once solves all the four problems above. The answer to the first three problems is 'No' in general. For example, the angle of 60 degrees cannot be trisected as $Cos 20^\circ$ is an algebraic number of degree 3; its minimal polynomial over $\mathbf{Q}$ is $X^3 - \frac{3}{4}X - \frac{1}{8}$. Duplication of a cube is impossible as it is equivalent to the constructibility of $2^{1/3}$. Finally, squaring the circle is equivalent to constructing π which is impossible since π is not even algebraic. The last problem is equivalent to finding all n for which $Cos 2\pi/n$ can be constructed or, equivalently, the points on the unit circle which correspond to the primitive n-th roots of unity can be constructed. If $\zeta = e^{2i\pi/n}$, then the degree $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \phi(n)$ and the degree $[\mathbf{Q}(Cos 2\pi/n) : \mathbf{Q}] = \phi(n)/2$. But, $\phi(n)$ is a power of 2 if, and only if, n is a power of 2 times a product of distinct Fermat primes. Thus, the easier part follows viz., if an n-gon is constructible, then n is as asserted. For the converse, one needs Galois theory. The extension $\mathbf{Q}(\zeta)$ is a Galois extension of $\mathbf{Q}$ and has an abelian Galois group viz., the group $(\mathbf{Z}/n)^\times$. If n is a power of 2 times a product of distinct Fermat primes, this extension is of degree a power of 2 i.e., $(\mathbf{Z}_n)^\times$ is a 2-group. By the theory of abelian groups, this group has a filtration by successive subgroups of index 2 and this produces a corresponding filtration of fields. So, the regular n-gon will be constructible.

- *Solvability of radicals*

This is probably the first and biggest success story of modern algebra. Polynomial equations (in one variable) of degrees at the most 4 can be solved for all their roots by explicitly finding a 'closed expression' in terms of the coefficients. It is to be understood that the expression is independent of the polynomial. This 'formula' involves taking square roots, cube roots and fourth roots. It was an open question for a long time as to whether there is such a formula valid for all fifth degree equations. It was proved by Ruffini and Abel that such a formula cannot exist for all polynomials of a given degree ≥ 5. The introduction by Galois of his theory completes demystifies the problem. Using Galois theory, as we shall see, one can say which polynomials can be solved by radicals i.e., by taking various higher roots and which ones cannot be so solved.
Our definitions are slightly different from those of Morandi.

Definitions.
(i) A finite extension L/K is called a *radical extension of* K if $L = K(u)$ where either $u^n \in K$ for some n with char K not dividing n or $u^p - u \in K$ with char $K = p > 0$.
(ii) A *tower of radical extensions over* K is a finite tower of extensions

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$$

with each K_i/K_{i-1} a radical extension.
(iii) A finite extension L/K is said to be *solvable by radicals over* K if $L \subseteq K_r$ for some tower

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$$

of radical extensions.
(iv) A polynomial $f \in K[X]$ is said to be *solvable by radicals over* K if its splitting field over K is solvable by radicals over K (that is, contained in K_r for a tower of radical extension of K as above).

Warning: We will see later that there exist polynomials which are solvable by radicals but its splitting field may NOT be a part of a radical tower over K.

Galois's theorem on solvability by radicals.
A finite extension M/K is solvable by radicals over K if, and only if, M is contained in a finite, Galois extension N of K such that $Gal(N/K)$ is solvable.
In particular, a finite Galois extension M/K is solvable by radicals over K if, and only if, its Galois group is solvable.

Corollary. A polynomial $f \in \mathbb{Q}[X]$ is solvable by radicals over $\mathbb{Q}$ if, and only if, the splitting field N of f over $\mathbb{Q}$ has Galois group $Gal(N/\mathbb{Q})$ to be solvable. Since S_n is not solvable for $n \geq 5$, the general polynomial of degree $n \geq 5$ over $\mathbb{Q}$ (which has Galois group S_n) is not solvable by radicals over $\mathbb{Q}$.

Proof of Galois's theorem.
First, suppose that M is contained in K_r where

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$$

where each K_i is a radical extension of K_{i-1}.
We write $K_r = K(u_1, \cdots, u_r)$; here, either char K does not divide n_i and $u_i^{n_i} \in K(u_1, \cdots, u_{i-1})$, or char $K = p > 0$ and $u_i^p - u_i \in K(u_1, \cdots, u_{i-1})$.
We will show that the above tower can be refined to end in a normal extension N over K.
Let n be the product of all the n_i's that occur.
If ζ is a primitive n-th root of unity in some algebraic closure of K_r, then $K_r(\zeta)$ is an abelian extension of K_r. We look at the tower of radical extensions

$$K_0(\zeta) \subseteq K_1(\zeta) = K_0(u_1, \zeta) \subseteq \cdots \subseteq K_r(\zeta) = K_0(u_1, \cdots, u_r, \zeta).$$

Rename this tower as

$$L_0 = K_0(\zeta) \subseteq L_1 = L_0(u_1) \subseteq \cdots \subseteq L_r = L_{r-1}(u_r) = L(u_1, \cdots, u_r)$$

where $L_0 = K_0(\zeta)$.
Due to L_0 containing the primitive n-th roots of unity, and the fact that each n_i divides n, the advantage of the above tower is that each successive extension is cyclic here!
If $\sigma_0 = Id, \sigma_1, \cdots, \sigma_{n-1}$ are the K=embeddings of $K_r = K(u_1, \cdots, u_r)$ in an algebraic closure, we know that the conjugates of $u_1, \cdots, u_r$ are the $\sigma_j(u_i)$'s.
We continue the last tower

$$L_0 \subseteq L_1 = L_0(u_1) \subseteq \cdots \subseteq L_r = L_0(u_1, \cdots, u_r)$$

by adding to the right the tower

$$L_{r+1} := L_r(\sigma_1(u_1)) \subseteq L_{r+2} = L_{r+1}(\sigma_1(u_2)) \cdots \subseteq L_{2r} = L_{2r-1}(\sigma_1(u_r)).$$

Note that the augmented tower is again a tower of radical extensions because $L_{r+1} = K_r(\sigma_1(u_1), \zeta)$ is radical over $L_r = K_r(\zeta)$.
To see this last assertion, consider two cases; first let $u_1^n \in K$ when char K does not divide n. Then, $\sigma_1(u_1)^n = \sigma_1(u_1^n) = u_1^n \in K \subseteq L_r$ which shows L_{r+1} is radical over L_r. If char $K = p > 0$ and $u_1^p - u_1 \in K$, then the conjugate $\sigma(u_1)$ must be of the form $u_1 + i$ for some $i < p$ and once again it follows that L_{r+1} is radical over L_r.
In this manner, for each of the K-embeddings $\sigma_0, \sigma_1, \sigma_{n-1}$ of K_r, we have a radical tower of length r which, when out together, form a tower of length nr ending in the extension $L_{nr} = K(\zeta, \sigma_j(u_i))$ where $0 \leq j < n$ and $1 \leq i \leq r$.
The tower makes it also clear that L_{nr} is separable over K as each successive extension is so. Thus, L_{nr} is a Galois extension, and the tower

$$L_0 \subseteq L_1 \cdots \subseteq L_{nr}$$

gives the chain of groups

$$\{1\} = Gal(L_{nr}/L_{nr}) \leq Gal(L_{nr}/L_{nr-1}) \leq \cdots$$

$$\leq Gal(L_{nr}/L_0) = Gal(L_{nr}/K(\zeta)) \leq Gal(L_{nr}/K)$$

where each successive inclusion is as a normal subgroup, and each successive quotient is abelian - they are actually cyclic excepting the last one $Gal(K(\zeta)/K)$. Therefore, $Gal(L_{nr}/K)$ is solvable.
Finally, note that $M \subseteq K_r \subseteq L_{nr}$.
Therefore, when M is itself Galois, the Galois group $Gal(M/K)$ is a quotient of the solvable group $Gal(L_{nr}/K)$ and is, itself thus solvable.

Conversely, if M is contained in a Galois extension N over K with $Gal(M/K)$ solvable, we have that the Galois closure M_0 of M over K is also contained in N. Hence, to show M is contained in the top term of a radical tower over K, it suffices to M_0 is contained in the top term of a radical tower. Therefore, we may assume without loss of generality that M itself is Galois over K and that $M \subseteq N$ with N, a Galois extension of K with $Gal(N/K)$ solvable.
Note that $Gal(M/K)$ is solvable, being a quotient of the solvable group $Gal(N/K)$.

Let $n = [M : K]$. If char $K = p > 0$ and $N = p^k n_0$ with p not dividing n_0, adjoin a primitive n_0-th root of unity ζ to K; call $L = K(\zeta)$. If char $K = 0$, then we take $L = K(\zeta)$ where ζ is a primitive n-th root of unity.
Now, ML is Galois over L with

$$Gal(ML/L) \cong Gal(M/(M \cap L)) \leq Gal(M/K)$$

which shows that $[ML : L]$ divides $[M : K] = n$.
Also, then $Gal(ML/L)$ is solvable, and has a composition series

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_k = Gal(ML/L);$$

that is, each G_i is normal in G_{i+1} and the quotient is a cyclic group of prime order.
The corresponding fixed fields of G_i's in ML gives a tower of field extensions

$$L = L_k \subseteq L_{k-1} \subseteq \cdots \subseteq L_0 = ML$$

where each successive extension is Galois with Galois group cyclic of prime order (this is the reason we took ζ in L).
By our description of cyclic extensions using Hilbert 90, we have that the tower above is a radical tower. Thus, $ML = MK(\zeta)$ is solvable by radicals over $L = K(\zeta)$. From this, it is clear that M is solvable by radicals over K.

Example.
The polynomial $f = X^3 - 3X + 1$ is solvable by radicals over $\mathbb{Q}$ (as its discriminant is the square 81, its Galois group is A_3). However, its splitting field is not a radical extension (that is, it is not purely cubic).