2. Galois theory

Notation. If otherwise not specified k, K , L and so on will be arbitrary fields.

Theorem. $k[T]$ is a principal ideal domain.

Proof. Euclid's algorithm ■

Definition 2.1. If the inclusion $k \hookrightarrow K$ is fixed then K is called an extension of k (notation K/k). Under this condition k could be identified with its image in K. Suppose K_1/k and K_2/k are extensions of k and $\sigma : K_1 \to K_2$ is a field homomorhism. If $\sigma|_k = \mathrm{Id}$ then σ is called a homomorphism of extensions $K_1/k \to K_2/k$.

Key Lemma 2.2. Suppose K_1/k and K_2/k are extensions of k, $\sigma : K_1/k \to K_2/k$ a homomorphism of extensions. Suppose $P(T) \in k[T]$, $\alpha \in K_1$. Then $P(\alpha) = 0 \Rightarrow P(\sigma(\alpha)) = 0$.
Proof. Clear ■

Definition 2.3. Suppose K/k is an extension, $\alpha \in K$. α is called algebraic over k iff $\exists P \in k[T]$ such that $P(\alpha) = 0$. K/k is called algebraic iff all elements of K are algebraic over k.

Definition 2.4. K/k is called finite iff K is a finitely dimensional vector space over k. Its degree (notation $[K : k]$) $\stackrel{\text{def}}{=} \dim_k K$.

Theorem 2.5. K/k is finite $\Rightarrow$ K/k is algebraic.

Proof. In the finitely dimensional vector space the powers $1, \alpha, \alpha^2, \alpha^3, \ldots$ are linearly dependent ■

Remark. The opposite is clearly not true.

Basic examples:
k_P - construction. Suppose $P \in k[T]$ is irreducible of degree ≥ 1. Then (P) is a maximal ideal in $k[T]$ hence $k_P \stackrel{\text{def}}{=} k[T]/(P)$ is a field. $[k_P : k] = \deg P$ (hometask).
$k(\alpha)$. Suppose K/k is an extension, $\alpha \in K$. Then $k(\alpha) \stackrel{\text{def}}{=} \{$ the mimimal subfield of K containing both k and $\alpha\}$.

Remark. Let $\{\alpha_{i,\,i\in I}\}$ be any set of elements of K. The subfield $k(\{\alpha_i\}) \subset K$ could be defined by the same property. Any element $\alpha \in k(\{\alpha_i\})$ is representable (not necessary in a unique way) with the formula $\alpha = \frac{P(\{\alpha_i\})}{Q(\{\alpha_i\})}$ where P and Q are polynomials in variables $\{T_i,\ i \in I\}$ and $Q(\{\alpha_i\}) \neq 0$.

Theorem 2.6. Suppose K/k is an extension, $\alpha \in K$ algebraic over k. Let $P_{\alpha,\,K/k} \in k[T]$ (shortly just $P_{\alpha,\,k}$ or even P_α) be a monic irreducible polynomial such that $P_\alpha(\alpha) = 0$. Then
1) P_α exists and is unique.
2) $k_{P_\alpha} \simeq k(\alpha) \simeq k[\alpha]$ (where $k[\alpha]$ is the minimal subring of K containig both k and α).

Proof. 1) Since α is algebraic some $P \in k[T]$ such that $P(\alpha) = 0$ does exist. One may suppose P is irreducible (otherwise decompose) and monic (otherwise divide by the leading coefficient). If P and Q are both irreducible and monic then either $P = Q$ or $\exists G, H \in k[T]$ such that $PG + QH = 1$ (Euclid algorithm). If $P(\alpha) = Q(\alpha) = 0$ the latter case is excluded, so P=Q ■
2) Consider the ring homomorphism $\phi : k[T] \to K$, $\phi|_k = \mathrm{Id}$, $T \overset{\phi}{\mapsto} \alpha$. By construction $\mathrm{im}\,(\phi) = k[\alpha]$. Since ϕ does not act on k and P_α has coefficients in k, $\phi(P_\alpha(T)) = P_\alpha(\phi(T)) = P_\alpha(\alpha) = 0$, hence $P_\alpha \in \ker(\phi)$. Therefore ϕ defines a surjective homomorphism $\overline{\phi} : k[T]/(P_\alpha) \to k[\alpha]$. Since P_α is irreducibe $k[T]/(P_\alpha)$ is a field, so $\overline{\phi}$ is also injective, hence an isomorphism. This means $k[\alpha]$ is a field, so $k[\alpha] = k(\alpha)$ ■

Theorem 2.7. Suppose K/k and L/K are finite extensions. Then L/k is finite and $[L : K][K : k] = [L : k]$.

Proof. Let $\{x_i\} \in K$ be a basis of the vector space K over k, $\{y_j\} \in L$ same for L over K. Then $\{x_i y_j\}$ is a basis of the vector space L over k (hometask) ■

Theorem 2.8. Suppose K/k is algebraic and finitely generated. Then K/k is finite.

Proof. If $K = k(\alpha)$ (i.e generated by one algebraic element) then K/k is finite by the Theorem 2.6.2). Suppose now $K = k(\alpha, \beta)$. Then $k(\alpha, \beta)/k(\alpha)$ and $k(\alpha)/k$ are both finite hence $k(\alpha, \beta)/k$ is finite by the previous theorem. The proof ends by induction ■

Theorem 2.9. Suppose K is generated over k by any number of algebraic elements. Then K/k is algebraic.

Proof. By 2.6.2) and by the Remark before Theorem 2.6 it suffices to prove that $\alpha \pm \beta$, $\alpha\beta$ are algebraic over k for any α, $\beta \in k$. As in the proof of the previous theorem one may conclude that $k(\alpha, \beta)/k$ is finite. Therefore it is algebraic ■

Theorem 2.10. Suppose L/K and K/k are both algebraic (not necessary finite). Then L/k is algebraic.

Proof. Suppose $\alpha \in L$. By assumption α is algebraic over K hence α is a root of the polynomial $P_{\alpha,K} \in K[T]$. Let k_1 be the subfield of K generated over k by all coefficients of the polynomial $P_{\alpha,K}$. Then $k \subset k_1 \subset k_1(\alpha)$, $k_1(\alpha)/k_1$ finite by the Theorem 2.6.2), k_1/k finite by the Theorem 2.8. So $k_1(\alpha)/k$ is finite by the Theorem 2.7, hence algebraic. In particular α is algebraic over k ■

Definition 2.11. A field K is called algebraicaly closed iff K has no algebraic extensions. Equivalently, any nonconstant irreducible polynomial $P \in K[T]$ is of degree 1.

Theorem 2.12. $\forall k \, \exists \, \overline{k}/k$ such that $\overline{k}$ is algebraic over k and $\overline{k}$ is algebraically closed.

Remark. The notation $\overline{k}$ is justified later when we prove that $\overline{k}/k$ is unique up to a (non-canonical) isomorphism.

Proof. Step 1. First we construct an algebraic extension K_1/k such that any nonconstant polynomial with coefficients in k has a root in K_1. This is just a refinement of the k_P - construction above. Consider the ring $k[\{T_P\}]$, T_P being independent variables numbered by all monic nonconstant polynomials in $k[T]$. Let $I \subset k[\{T_P\}]$ be the ideal generated by the elements $P(T_P)$. Then I is nontrivial. Indeed, suppose the opposite is true. Then there exist some polynomials $P_i \in k[T]$ and some elements $g_i \in k[\{T_P\}]$ such that $\sum_{i=1}^{n} g_i P_i(T_{P_i}) = 1$. Consider a field $K_0 \supset k$ such that each P_i from this finite set has a root in K_0. Certainly one may get K_0 by successive use of the k_P-construction. For $1 \leq i \leq n$ suppose $\alpha_i \in K_0$ and $P_i(\alpha_i) = 0$. Consider the ring homomorphism $\phi : k[\{T_P\}] \to K_0$ defined as follows: $\phi|_k = \mathrm{Id}$; $\phi(T_{P_i}) = \alpha_i$ if $1 \leq i \leq n$; $\phi(T_{P_i}) = 0$ otherwise. Acting with ϕ on the equation above one gets 0=1 in K_0.
Since I is nontrivial there exists a maximal ideal M, $I \subset M \subset k[\{T_P\}]$. Let K_1 be the quotient field $k[\{T_P\}]/M$. K_1 is algebraic over k because it is generated by the images of the independent variables T_P which are all algebraic by construction of M (the latter contains all $P(T_P)$) ■

Step 2. Now construct $k \subset K_1 \subset K_2 \subset K_3 \ldots$ as in step 1 (for all i any nonconstant polynomial with coefficients in K_i has a root in K_{i+1}). Let $\overline{k} \overset{\text{def}}{=} \bigcup K_i$. Clearly the set $\overline{k}$ carries the natural structure of the field. By the Theorem 2.10 all the K_i are algebraic over k hence same is $\overline{k}$ as any element of $\overline{k}$ lies in some K_i. Suppose $P \in \overline{k}[T]$. P has a finite number of coefficients therefore all of them are contained in some K_i. Then P has a root in K_{i+1} hence in $\overline{k}$ ∎

Now we switch to the main object of study in Galois theory : homomorphism s of extensions.

Theorem 2.13. Suppose K/k is algebraic, $\sigma : K/k \to K/k$ is a homomorphism of extensions. Then σ is an automorphism.

Proof. Any field homomorphism is injective so it suffices to prove σ is surjective. Suppose $\alpha \in K$. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be the full list of the roots of P_α in K. $k(\alpha_1, \ldots, \alpha_n)/k$ is finite by the Theorem 2.8. $\sigma(k(\alpha_1, \ldots, \alpha_n)) \subset k(\alpha_1, \ldots, \alpha_n)$ (see the key Lemma 2.2). Since $\ker \sigma = 0$ σ is a nondegenerate linear transformation of the k - vector space of finite dimension, therefore σ is surjective. In particular $\alpha \in \operatorname{im} \sigma$ ∎

Definition 2.14. Supppose K/k and L/k are two extensions of the same ground field. Then $\Sigma_{K/k}^{L/k}$ is the set of all homomorphism s $\sigma : K/k \to L/k$.

Example. Suppose $K = k_P$. A homomorphism $\sigma : K/k \to L/k$ uniquely extends to the ring homomorphism $\widetilde{\sigma}: k[T] \to L$ such that $\widetilde{\sigma}\,|_k = \mathrm{Id}$ and $P(\widetilde{\sigma}\,(T)) = 0$. Therefore in this case the set $\Sigma_{K/k}^{L/k}$ coincides with the set of different roots of $P(T)$ in L.

Theorem 2.15. Suppose $k \subset M \subset K$, $K = M(\alpha)$, α algebraic over M, L/k algebraically closed. Then any element $\sigma \in \Sigma_{M/k}^{L/k}$ could be extended to an element of $\Sigma_{K/k}^{L/k}$.

Proof. Define the extension L/M by including $M \hookrightarrow L$ via σ. Then the set $\Sigma_{M(\alpha)/M}^{L/M}$ is nonempty by the Theorem 2.6.2) and the Example above ∎

Theorem 2.16. Suppose K/k is algebraic (not necessary finite), L/k algebraically closed. Then $\Sigma_{K/k}^{L/k}$ is nonempty. If both K/k and L/k are algebraic and algebraically closed then any $\sigma \in \Sigma_{K/k}^{L/k}$ is an isomorphism.

Proof. We will use the transfinite induction. Consider the set of pairs (M, σ) where $k \subset M \subset K$ and $\sigma : M/k \to L/k$ is a homomorphism . Define an ordering on this set as follows: $(M_1, \sigma_1) \leq (M_2, \sigma_2)$ iff $M_1 \subset M_2$ and $\sigma_2|_{M_1} = \sigma_1$. Clearly any linearly ordered subset $(M_1, \sigma_1), (M_2, \sigma_2), (M_3, \sigma_3), \ldots$ has an upper bound $(M_\infty = \bigcup M_i, \sigma_\infty = (\sigma_i \text{on} M_i))$. By the Zorn Lemma there exists a pair (M, σ) which is a maximal element in the set. Suppose that $M \neq K$. Then $\exists \alpha \in K$ such that $\alpha \notin M$. By the previous theorem there exists a homomorphism $M(\alpha) \to L$ extending σ. This contradicts the assumption that the pair (M, σ) is maximal.
Therefore $M = K$, so $\Sigma_{K/k}^{L/k}$ is nonempty. If K is algebraically closed same is $\sigma(K)$. If L is algebraic over k it is also algebraic over $\sigma(K)$, so L and $\sigma(K)$ must coincide ■

Definition 2.17. The number $[K : k]_s \stackrel{\text{def}}{=} \#(\Sigma_{K/k}^{\overline{k}/k})$ is called the separable degree of the algebraic extension K/k.

Remark. At the moment it is not yet clear that $[K : k]_s$ is finite for the finite extension K/k.

Theorem 2.18. 1) $[L : K]_s [K : k]_s = [L : k]_s$ if all three are finite.
2) If K/k is a finite extension then $[K : k]_s \leq [K : k]$.

Proof. 1) Let $k \subset K \subset L \subset \overline{k}$. Consider the natural map $\phi : \Sigma_{L/k}^{\overline{k}/k} \to \Sigma_{K/k}^{\overline{k}/k}$ (the restriction to K). For any $\sigma_0 \in \Sigma_{K/k}^{\overline{k}/k}$ the "fiber" $F_{\sigma_0} \stackrel{\text{def}}{=} \{\sigma \in \Sigma_{L/k}^{\overline{k}/k}$ such that $\sigma|_K = \sigma_0\}$ is in one-to-one correspondence with the set $\Sigma_{L/K}^{\overline{k}/K}$. Indeed, if $\sigma_0 = \text{Id}$ then it follows from the definition of Σ. Now suppose σ_0 is arbitrary. Let $\{\sigma_i \in \Sigma_{L/k}^{\overline{k}/k}\}$ be the full set of different elements of F_{σ_0}. Then $\forall i \;\; k \subset \sigma_0(K) \subset \sigma_i(L) \subset \overline{k}$. The map $\sigma_i \mapsto \sigma_i \circ \sigma_1^{-1}$ provides a one-to-one correspondence $F_{\sigma_0} \stackrel{\sim}{\to} \Sigma_{\sigma_1(L)/\sigma_0(K)}^{\overline{k}/\sigma_0(K)}$, the latter set clearly being isomorphic to $\Sigma_{L/K}^{\overline{k}/K}$. The number of elements in the "total space" of the "fibration" ϕ is equal to $[L : k]_s$, the cardinality of the "base" is $[K : k]_s$ while each "fiber" consists of $[L : K]_s$ elements as has just been proved, whence the statement ■
2) If K is generated over k by one algebraic element α then $K = k_{P_\alpha}$. $[K : k] = \deg P_\alpha$ while $[K : k]_s = \#(\Sigma_{K/k}^{\overline{k}/k}) = \{$the number of different roots of P_α in $\overline{k}\}$. Clearly the second number is less or equal than the first one. For the general case consider the finite extension K/k as a tower of the extensions generated by one algebraic element and then use 1) ■

Definition 2.19. A finite extension K/k is called finite separable iff $[K:k]_s = [K:k]$.

Definition 2.20. Suppose $k \subset K$, $\alpha \in K$ algebraic over k. The element α is called separable over k iff the extension $k(\alpha)/k$ is finite separable. The algebraic (not necessary finite) extension K/k is called separable iff all $\alpha \in K$ are separable over k.

Theorem 2.21. Suppose $k \in K$, $\alpha \in K$ algebraic. Then α is separable over $k \Leftrightarrow P_\alpha(T)$ has no multiple roots in $\overline{k}$.

Proof. Clear ■

Remark. This justifies the name "separable": α is separable iff the roots of its minimal polynomial are "separated" from each other.

Theorem 2.22. For the finite extension K/k Definitions 2.19 and 2.20 lead to the same concept.

Proof. If K/k fits the Definition 2.19 then $\forall \alpha \in K \quad k \subset k(\alpha) \subset K$ hence $k(\alpha)/k$ also fits 2.19 by the Theorem 2.18. Conversely, suppose all $\alpha \in K$ are separable over k. Consider K as a finite tower $k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset K$. Since each α_i is separable over k it is by the Theorem 2.21 also separable over $k(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$ because $P_{\alpha_i, k(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})}$ is a factor of $P_{\alpha_i, k}$. To finish the proof one may use the Theorem 2.18 ■

Theorem 2.23. If $\mathrm{char}(k) = 0$ then any algebraic extension K/k is separable. If $\mathrm{char}(k) = p$ and K/k is finite then $[K:k] = p^\nu [K:k]_s$ for some nonnegative integer ν.

Proof. Suppose $\alpha \in K$. $P_\alpha(T)$ has multiple roots in $\overline{k} \Leftrightarrow \gcd(P_\alpha, P'_\alpha) \neq 1$. Since P_α is irreducible this leads to $P'_\alpha = 0$. If $\mathrm{char}(k) = 0$ this is not possible as P_α is nonconstant. If $\mathrm{char}(k) = p$ then $P'_\alpha = 0$ means that $P_\alpha(T) = Q(T^{p^\mu})$ where $Q \in k[T]$ is some polynomial such that $Q' \neq 0$ and μ is a positive integer. Clearly $\deg P_\alpha = p^\mu \deg Q$. If $\alpha_1, \alpha_2, \ldots, \alpha_{\deg Q}$ are the roots of P_α in $\overline{k}$ then $\alpha_1^{p^\mu}, \alpha_2^{p^\mu}, \ldots, \alpha_{\deg Q}^{p^\mu}$ are the roots of Q in $\overline{k}$. This means that the Theorem is true for the extension generated by one element. In general, K/k is a tower of extensions of that kind whence the Theorem ■

Theorem 2.24 (primitive element). Suppose K/k is a finite separable extension. Then $\exists \alpha \in K$ such that $K = k(\alpha)$.

Proof. One may suppose k is infinite (otherwise K is a finite field, so K is generated over k by any group generator of its multiplicative group K^*). By the induction it suffices to prove the following statement: if K is separable over k and is generated over k by two elements then it is generated over k by one element. Suppose $K = k(\alpha, \beta)$. Let $\{\sigma_i\}$ be the full set of elements of $\Sigma_{K/k}^{\overline{k}/k}$. Define $P(T)$ by the formula $P(T) = \prod_{i \neq j} (\sigma_i(\alpha) + \sigma_i(\beta)T - \sigma_j(\alpha) - \sigma_j(\beta)T)$. SInce k is infinite $\exists t_0 \in k$ such that $P(t_0) \neq 0$. This means that for any two $i \neq j \quad \sigma_i(\alpha + \beta t_0) \neq \sigma_j(\alpha + \beta t_0)$. Therefore $[k(\alpha + \beta t_0) : k]_s \geq \{\text{number of different } \sigma_i\} = [k(\alpha, \beta) : k]_s$. Since both $k(\alpha + \beta t_0)/k$ and $k(\alpha, \beta)/k$ are separable this means that $[k(\alpha + \beta t_0) : k] \geq [k(\alpha, \beta) : k]$ which finishes the proof ■

Example. If k and K are finite fields than the extension K/k is always separable. Indeed, if $K = \mathbf{F}_q$ then $\forall \alpha \in K \;\; P_{\alpha, K/k} \,|\, T^q - T$, the latter polynomial having no double roots.

We now will study the conditions under which $\mathrm{Aut}(K/k)$ could be identified with $\Sigma_{K/k}^{\overline{k}/k}$.

Definition-Theorem 2.25. Suppose $P \in k[T]$ is of degree $d \geq 1$. The extension K/k (and the field K itself if no mix up is possible) is called its splitting field (notation $k_{P,\,\mathrm{split}}$) iff two conditions hold:
1) $P = \prod_{i=1}^{d} (T - \alpha_i)$ in K and
2) $K = k(\alpha_1, \ldots, \alpha_d)$
Let K_1/k, K_2/k be two splitting fields for the same polynomial P. Then there exists an isomorphism $\sigma : K_1/k \xrightarrow{\sim} K_2/k$. If $k \subset K_2 \subset \overline{k}$ then any $\sigma' : K_1/k \to \overline{k}/k$ maps K_1 to K_2.

Proof. The field $\overline{K_2}$ could be considered as $\overline{k}$, so one may suppose $k \subset K_2 \subset \overline{k}$. By the Theorem 2.15 $\exists\, \sigma : K_1/k \to \overline{k}/k$. The images of the roots of P in K_1 under σ are the roots of P in $\overline{k}$ by the key Lemma hence $\sigma(K_1) \subset K_2$. Since K_1/k is a splitting field for P one may conclude by using the definition that $\sigma(K_1)/k$ is also a splitting field for P. But $\sigma(K_1) \subset K_2$, therefore $\sigma(K_1) = K_2$ ■

Remark 1. In the Definition above P needs not to be irreducible.

Remark 2. As opposite to k_P no simple construction of $k_{P,\,\mathrm{split}}$ is available. In particular it is not clear how to calculate the degree $[k_{P,\,\mathrm{split}} : k]$.

Examples.

deg $P = 1 \quad k_{P,\,\text{split}} = k$

deg $P = 2$ If P is irreducible then $k_{P,\,\text{split}} \overset{\sim}{=} k_P$ else $k_{P,\,\text{split}} = k$.

Indeed, suppose $P(T) = a_0 + a_1T + a_2T^2$ is irreducible. Then $P(S) = (S - \phi(T))(a_2S + a_2\phi(T) + a_1)$ in the ring $k_P[S]$ where $\phi : k[T] \to k_P$ is a standard homomorphism . So P splits completely in $k_P[T]$ hence $k \subset k_{P,\,\text{split}} \subset k_P$. But $k_{P,\,\text{split}} \neq k$ while $[k_P : k] = 2$, therefore $k_{P,\,\text{split}} = k_P$.

Definition-Theorem 2.26. The algebraic extension K/k is called normal iff, equivalently,
1) All $\sigma \in \Sigma_{K/k}^{\overline{k}/k}$ have the same image or
2) For any irreducible $P \in k[T]$ P has a root in $K \Rightarrow P$ totally splits in K.

Proof. 1) $\Rightarrow$ 2). One may suppose $k \subset K \subset \overline{k}$. Let $\alpha \in K$, $P(\alpha) = 0$. Then $k \subset k(\alpha) \subset K$, $k(\alpha) \overset{\sim}{=} k_P$. Let $P(T) = \prod_{i=1}^{d}(T - \beta_i)$ in $\overline{k}$. Then $\forall\, \beta_i \,\exists\, \tilde{\sigma}_i$: $k_P/k \to \overline{k}/k$ such that $\tilde{\sigma}_i\,(\alpha) = \beta_i$. As in the proof of the Theorem 2.15 each $\tilde{\sigma}_i$ could be extended to some $\sigma_i \in \Sigma_{K/k}^{\overline{k}/k}$ (i.e. $\sigma_i|_{k(\alpha)} = \tilde{\sigma}_i$). Hence $\beta_i \in \operatorname{im}\sigma_i (= \operatorname{im}\sigma_1$ by the assumption 1)). Since $\sigma_1 : K \to \operatorname{im}\sigma_1$ is an isomorphism $P(T) = \prod_{i=1}^{d}(T - \sigma_1^{-1}(\beta_i))$ in K ■

2) $\Rightarrow$ 1). Suppose $\sigma_1 \in \Sigma_{K/k}^{\overline{k}/k}$, $\beta \in \operatorname{im}\sigma_1$. The polynomial $P_\beta \in k[T]$ has a root $\sigma_1^{-1}(\beta)$ in K hence (by the assumption 2)) $K_1 \overset{\text{def}}{=} k_{P_\beta,\,\text{split}} \subset K$. Consider an arbitrary $\sigma_i \in \Sigma_{K/k}^{\overline{k}/k}$. By the Definition-Theorem 2.25 $\sigma_i(K_1)$ coincides with the unique subfield of $\overline{k}$ isomorphic to $k_{P_\beta,\,\text{split}}$. In particular $\beta \in \sigma_i(K_1) \subset \sigma_i(K) = \operatorname{im}\sigma_i$ ■

Theorem 2.27. For any nonconstant $P \in k[T]$ $k_{P,\,\text{split}}$ is a normal extension.

Proof. Hometask ■

Examples. Suppose $k \subset K \subset L$ is a tower of algebraic extensions.

1. If L/k is normal then L/K is normal. In fact, one may identify $\overline{K}$ with $\overline{k}$. Then $\Sigma_{L/K}^{\overline{K}/K} \subset \Sigma_{L/k}^{\overline{k}/k}$ so if the criterion 2.25.1) holds for L/k it also holds for L/K.

2. L/k normal, K/k not normal. Let $k = \mathbf{Q}$, $K = \mathbf{Q}(\sqrt[3]{2})$, $L = \overline{\mathbf{Q}} \subset \mathbf{C}$. Certainly $\overline{k}/k$ is normal for any k. But K/k is not normal as the complex roots of the polynomial $T^3 - 2$ are not in K.

3. K/k normal, L/K normal, L/k not normal. Let $k = \mathbf{Q}$, $K = \mathbf{Q}(\sqrt{2})$, $L = \mathbf{Q}(\sqrt[4]{2})$. K/k and L/K are both of degree 2 hence normal (see Example 2 of the splitting field). But L/k is not normal as the imaginary roots of $T^4 - 2$ are not in L.

Definition 2.28. An algebraic extension K/k is called Galois iff it is separable and normal. If this is the case then the group $\mathrm{Aut}\,(K/k)$ is called its Galois group (notation $\mathrm{Gal}\,(K/k)$). If $k \subset K \subset \overline{k}$ then $\mathrm{Gal}\,(K/k)$ could be identified with the set $\Sigma_{K/k}^{\overline{k}/k}$.

In what follows all the fields are supposed to be the subfields of the fixed $\overline{k}$.

Theorem 2.29. Suppose K/k is a finite Galois extension. Then $\#\mathrm{Gal}\,(K/k) = [K : k]$.

Proof. Since K/k is finite separable $[K : k] = \#\Sigma_{K/k}^{\overline{k}/k}$, the latter set being identical to $\mathrm{Gal}\,(K/k)$ ■

Definition 2.30. Suppose $H \subset \mathrm{Gal}\,(K/k)$ is a subgroup. The fixed field $K^H \overset{\mathrm{def}}{=} \{x \in K$ such that $\forall h \in H \;\; h(x) = x\}$.

Theorem 2.31 (the fundamental theorem of Galois theory). Suppose K/k is a finite Galois extension, $G = \mathrm{Gal}\,(K/k)$ its Galois group. Then
1) There exists a one-to-one correspondence $\{$subgroups $H \subset G\} \leftrightarrow \{$ subfields $k \subset M \subset K\}$ defined by the maps $H \mapsto K^H$, $\mathrm{Gal}\,(K/M) \leftarrow\!\shortmid M$.
2) M/k is normal $\Leftrightarrow$ $H \triangleleft G$ (i.e. H is a normal subgroup).

Proof. $\forall M \;\; K/M$ is separable (easy hometask) and normal (see Example 1 above) therefore Galois.
1) - *Step 1.* First we prove that $K^G = k$. Indeed, suppose $\alpha \in K^G$. Any $\widetilde{\sigma}$: $k(\alpha)/k \to \overline{k}/k$ could be extended to some $\sigma : K/k \to \overline{k}/k$ which is an element of the Galois group

$\mathrm{Gal}\,(K/k)$. By assumption $\sigma(\alpha) = \alpha$ hence $\#\Sigma^{\bar{k}/k}_{k(\alpha)/k} = 1$. Since α is separable over k this means that $[k(\alpha) : k] = 1$ hence $\alpha \in k$. By the same token $\forall M \;\; M = K^{\mathrm{Gal}\,(K/M)}$. Therefore the composition map $M \mapsto \mathrm{Gal}\,(K/M) \mapsto K^{\mathrm{Gal}\,(K/M)}$ leads back to M ■

1) - *Step 2.* To finish the proof of the first statement of the Theorem it remains to prove that $\mathrm{Gal}\,(K/K^H) = H$. If $h \in H$ then by definition h does not act on K^H hence $H \subset \mathrm{Gal}\,(K/K^H)$. We still need to prove that $\mathrm{Gal}\,(K/K^H)$ does not contain "extra" elements. Since $\#\mathrm{Gal}\,(K/K^H) = [K : K^H]$ it suffices to prove that $[K : K^H] \leq \#H$.
Suppose $\alpha \in K$. Choose the elements $\mathrm{Id} = \sigma_1, \sigma_2, \ldots, \sigma_r \in H$ such that all $\sigma_i(\alpha)$ are different and the set $\{\sigma_1, \ldots, \sigma_r\}$ is maximal with this property (i.e $\forall \sigma \in H \;\; \sigma(\alpha)$ coincides with some $\sigma_i(\alpha)$). Let $P(T) \overset{\mathrm{def}}{=} \prod_{i=1}^{r}(T - \sigma_i(\alpha))$. Then $\forall h \in H \;\; {}^hP(T) = P(T)$. Indeed, ${}^hP(T) = \prod_{i=1}^{r}(T - h \circ \sigma_i(\alpha))$ where the action of h just permutes the roots $\sigma_i(\alpha)$ (otherwise for some $i \;\; h \circ \sigma_i(\alpha)$ were different from all $\sigma_j(\alpha)$ in contradiction with the choice of the set $\{\sigma_i\}$). This means that $P(T) \in K^H[T]$ hence α is of degree $\leq r$ over K^H.
This holds for arbitrary α. Since K is separable over K^H (see the start of the proof) by the Theorem about a primitive element $\exists \alpha \in K$ such that $K = K^H(\alpha)$. This α is also of degree $\leq r$ over K^H hence $[K : K^H] \leq r$, the latter being $\leq \#H$ by construction ■

2) If M/k is normal then the restriction of any $\sigma \in \mathrm{Gal}\,(K/k)$ to M maps M to itself therefore belongs to $\mathrm{Gal}\,(M/k)$. Clearly $\mathrm{Gal}\,(K/M) = \ker(\mathrm{Gal}\,(K/k) \overset{\sigma \mapsto \sigma|_M}{\longrightarrow} \mathrm{Gal}\,(M/k))$ hence $\mathrm{Gal}\,(K/M) \lhd \mathrm{Gal}\,(K/k)$. Conversely, if M/k is not normal then $\exists \sigma \in \Sigma^{\bar{k}/k}_{M/k}$ such that $\sigma(M) \neq M$ so $\mathrm{Gal}\,(K/\sigma(M)) \neq \mathrm{Gal}\,(K/M)$ by the first statement of the Theorem. This σ could be extended to $\widetilde{\sigma} \in \Sigma^{\bar{k}/k}_{K/k} = \mathrm{Gal}\,(K/k)$. The subgroups $\mathrm{Gal}\,(K/M)$ and $\mathrm{Gal}\,(K/\sigma(M))$ are conjugate in $\mathrm{Gal}\,(K/k)$ (namely $\mathrm{Gal}\,(K/\sigma(M)) = \widetilde{\sigma} \circ \mathrm{Gal}\,(K/M) \circ \widetilde{\sigma}^{-1}$, for the proof see hometask) and different hence neither of them is normal ■

Remark. The finiteness of the extension K/k is essential only for the step 2 of the proof of the first statement. If K/k is infinite the "extra" elements in $\mathrm{Gal}\,(K/M)$ may exist. The correct formulation of the fundamental theorem in the general case looks as follows: intermediate fields are in one-to-one correspondence with subgroups of $\mathrm{Gal}\,(K/k)$ which are closed in the certain topology on $\mathrm{Gal}\,(K/k)$ named the Krull topology. The latter is nothing but the topology on $\mathrm{Gal}\,(K/k)$ considered as the projective limit of its finite quotient groups $\mathrm{Gal}\,(M/k)$, $M/$k running over the set of all normal finite sub-extensions of K/k.

Examples.

Example 1. Suppose $P \in k[T]$ is a nonconstant monic separable polynomial (not necessary irreducible). Let $K = k_{P,\,\text{split}}$, $P(T) = \prod\limits_{i-1}^{n}(T - \alpha_i)$, $\alpha_i \in K$. The data above define a natural inclusion $\text{Gal}\,(K/k) \hookrightarrow \mathbf{S}_n$.
The group $\mathbf{S}_n$ is nothing but the group of permutations of the roots α_i. Since α_i generate K the homomorphism above is an inclusion.

Definition-Theorem 2.32. Suppose $P \in k[T]$ is a monic separable polynomial, $P(T) = \prod\limits_{i-1}^{n}(T - \alpha_i)$, $\alpha_i \in \overline{k}$. The discriminant $\Delta_P \stackrel{\text{def}}{=} \prod\limits_{i<j}(\alpha_i - \alpha_j)^2$. Then $\Delta_P \in k$. Let $\delta_P \stackrel{\text{def}}{=} \sqrt{\Delta_P}$. $\delta_P \in k_{P,\,\text{split}}$, it is defined up to a sign. $\delta_P \in k \Leftrightarrow$ {the image of $\text{Gal}\,(k_{P,\,\text{split}}/k)$ in $\mathbf{S}_n$ is contained in the subgroup of even permutations $\mathbf{A}_n$}.

Proof. Neither permutation of the roots acts nontrivially on Δ_P hence $\text{Gal}\,(k_{P,\,\text{split}}/k)$ does not act on it by the previous example, therefore $\Delta_P \in k$ by the Galois theory. It is clear from the definition of δ_P that any permutation τ of the roots of P multiplies δ_P with $\text{sign}(\tau)$ whence the Theorem.

Example 2. Suppose $P \in k[T]$ is separable of degree 2. It is irreducible iff $\delta_P \notin k$. In this case $k_{P,\,\text{split}} \simeq k_P$ and $\text{Gal}\,(k_{P,\,\text{split}}/k) = \mathbf{Z}/(2)$.

Example 3. Suppose $P \in k[T]$ is separable irreducible of degree 3. By the Example 1 $\#\text{Gal}\,(k_{P,\,\text{split}}/k)|\,\#\mathbf{S}_3 = 6$ hence $[k_{P,\,\text{split}} : k]|\,6$. On the other hand, $\forall i\ k(\alpha_i) \subset k_{P,\,\text{split}}$, thus $[k_{P,\,\text{split}} : k] = 3$ or 6.
Consider the tower of extensions $k \subset k(\delta_P) \subset k_{P,\,\text{split}}$. One may conclude that
$\delta_P \in k \Leftrightarrow \text{Gal}\,(k_{P,\,\text{split}}/k) \subset \mathbf{A}_3 \Leftrightarrow \text{Gal}\,(k_{P,\,\text{split}}/k) = \mathbf{A}_3 \Leftrightarrow k_{P,\,\text{split}} \simeq k_P$, and
$\delta_P \notin k \Leftrightarrow \text{Gal}\,(k_{P,\,\text{split}}/k) = \mathbf{S}_3$.

Example 4. Suppose k_0 ia a field, $K = k_0(t_1, t_2, \ldots, t_n)$ is generated over k_0 by n independent variables. Let $k = k_0(s_1, s_2, \ldots, s_n)$ where s_i are elementary symmetric functions of t_i. Let $P(T) = \prod\limits_{i=1}^{n}(T - t_i) = \sum\limits_{j=0}^{n-1}(-1)^{n-j}s_{n-j}T^j + T^n$.

Theorem 2.33. $K = k_{P,\,\text{split}}$. $\text{Gal}\,(K/k) \simeq \mathbf{S}_n$.

Proof. The first statement is clear. By the definition of K any permutation of t_i's defines an automorphism of K. Since k is generated by the symmetric functions such automorphism acts trivially on k therefore is an element of $\mathrm{Gal}\,(K/k)$, hence the inclusion from Example 1 is surjective in this case ■

Example 5. Finite fields. Suppose $\mathbf{F}_q \subset K \subset \overline{\mathbf{F}_q}$, $K/\mathbf{F}_q$ is finite. Let $m \stackrel{\mathrm{def}}{=} [K : \mathbf{F}_q]$.

Theorem 2.34. $K/\mathbf{F}_q$ is Galois, $\mathrm{Gal}\,(K/\mathbf{F}_q) \simeq \mathbf{Z}/(m)$. It is generated by the relative Frobenius homomorphism Fr_q which sends any element of $\overline{\mathbf{F}_q}$ to its q-th power.

Proof. $\#K = q^m \Rightarrow K = \mathbf{F}_{q^m} = \mathbf{F}_{q\ T^{q^m}-T,\,\mathrm{split}}$. Hence $K/\mathbf{F}_q$ is normal and separable. Therefore the restriction of Fr_q to K is an element of $\mathrm{Gal}\,(K/\mathbf{F}_q)$ (note that $Fr_q = \mathrm{Id}$ on $\mathbf{F}_q$) which is of order m. Clearly $Fr_q^m = \mathrm{Id}$ on K but neither smaller power of Fr_q acts as Id on K (for the proof see hometasks ■

Example 6. "The Fundamental Theorem of Algebra".

Theorem 2.35. $\overline{\mathbf{R}} = \mathbf{R}_{T^2+1}$.

Proof. Suppose $\mathbf{R} \subset K_0 \subset \overline{\mathbf{R}}$ and $K_0/\mathbf{R}$ is finite. If $K_0/\mathbf{R}$ is not Galois choose K, $R \subset K_0 \subset K \subset \overline{\mathbf{R}}$ such that $K/\mathbf{R}$ is Galois. This is always possible because $K_0/\mathbf{R}$ is separable hence $K_0 = \mathbf{R}(\alpha)$ by the Theorem 2.24. Now let $K = K_{0\ P_\alpha,\,\mathrm{split}}$. We are going to prove that $[K : \mathbf{R}] = 2$. The Theorem then follows as any quadratic extension of $\mathbf{R}$ clearly is contained in $\mathbf{R}(\sqrt{-1})$.
To finish the proof we need four Lemmas.

Lemma 1. $\mathbf{R}$ has no nontrivial finite extensions of odd degree.

Lemma 2. Suppose G is a finite group. If G is not a 2-group (i.e. $\#G$ is not a power of 2) then $\exists H \subset G$ such that $(G : H)$ is odd and greater than 1.

Lemma 3. If G is a finite 2-group then $\exists H \subset G$ such that $(G : H) = 2$.

Lemma 4. $\mathbf{R}_{T^2+1}$ has no quadratic extensions.

Let us derive the Theorem from the Lemmas above. Let $G = \mathrm{Gal}\,(K/\mathbf{R})$. If G is not a 2-group then $\exists H \subset G$ from the Lemma 2, hence by the Galois theory $\mathbf{R} \subset K^H \subset K$, and $[K^H : \mathbf{R}]$ is odd which is impossible by the Lemma 1. So one may suppose G is a 2-group. Then by Lemma 3 there exist $H \subset G$ and the tower $\mathbf{R} \subset K^H \subset K$ such that $[K^H : \mathbf{R}] = 2$. Clearly $K^H = \mathbf{R}(\sqrt{-1})$. If H is a trivial subgroup of G then $K = K^H$ and the proof ends. If not, consider $G_1 = \mathrm{Gal}\,(K/K^H)$. By the same Lemma $\exists H_1 \subset G_1$ such that $K^H \subset K^{H_1} \subset K$ and $[K^{H_1} : K^H] = 2$ which is not possible by the Lemma 4 ■

It remains to prove the Lemmas.

Proof of Lemma 1 & Lemma 4. Hometasks ■

Proof of Lemma 2 & Lemma 3. We will prove both by induction on the $\#G$ using the wellknown class formula: for any finite group G

$$\#G = \#Z_G + \sum_{C:\,\#C>1} \#C,$$

where C in the sum runs over the set of nontrivial conjugate classes of G. Let me recall that the conjugate class is, by definition, an orbit of the action of G on itself by conjugations. The conjugate class is called trivial iff it consists of one element; such elements constitute the center Z_G of the group G. For any conjugate class C $\#C = (G : G_x)$, G_x being the subgroup of G which consists of all elements which commute with $x \in C$. Of course, G_x depends on x, but if x and y are in the same C then G_x and G_y are conjugate.

Now we prove Lemma 2. If $\#G$ is odd one may take $H = \{1\}$. Suppose $\#G$ is even but not a power of 2. If $G : H$ is even for any subgroup H then all nontrivial conjugate classes in G have an even order, hence by the class formula $\#Z_G$ is also even. Z_G is commutative therefore $\exists Z_0 \subset Z_G$ such that $\#Z_0 = 2$. Consider the quotient group $G_1 = G/Z_0$, let $\phi : G \to G_1$ be the projection. Since G is not a 2-group same is G_1. By the induction, $\exists H_1 \subset G_1$ such that $(G_1 : H_1)$ is odd, but $(G : \phi^{-1}(H_1)) = (G_1 : H_1)$ which contradicts the assumption that the Lemma 2 does not hold for G ■

The proof of Lemma 3 is the same (any 2-group has a nontrivial center thanks to the class formula) ■

Example 7. Cyclotomic fields. Suppose n is a positive integer, k a field such that $\gcd(\mathrm{char}\,(k), n) = 1$. Our goal is to study the extension $k_{T^n-1,\ \mathrm{split}}/k$. Certainly its structure depends on the nature of the field k. The polynomial $T^n - 1$ is never irreducible, sometimes splitting totally (say $k = \mathbf{F}_q$ and $n = q - 1$).

Definition 2.36. The set of all roots of $T^n - 1$ in $\overline{k}$ is called the set of "roots of 1 of degree n". They form a group under multiplication which is cyclic (being a finite subgroup of $\overline{k}^*$). Any generator of this group is called a primitive root.

Theorem 2.37. Suppose ζ is a primitive root. Then $k(\zeta)/k$ is Galois. There exists an inclusion $\mathrm{Gal}\,(k(\zeta)/k) \hookrightarrow (\mathbf{Z}/(n))^*$.

Proof. Suppose $\sigma \in \Sigma^{\overline{k}/k}_{k(\zeta)/k}$. $\sigma(\zeta)$ is a power of ζ hence $k(\zeta)/k$ is normal. Since $\gcd(\mathrm{char}(k), n) = 1$ $T^n - 1$ is separable, so $k(\zeta)/k$ is Galois. Let $\sigma(\zeta) = \zeta^{l(\sigma)}$, then $l(\sigma) \mod n$ is correctly defined by σ. Clearly $l(\sigma) \in \mathbf{Z}/(n)$ is invertible (otherwise $\sigma(\zeta)$ were not primitive) and defines the homomorphism we need ■

In particular, $[k(\zeta) : k] \mid \phi(n)$.

Definition 2.38. $T^n - 1 = \prod_{d|n} f_d(T)$, where $f_d(T) = \prod_{(\text{order of}\,\omega)=d} (T - \omega)$ is called the cyclotomic polynomial of degree d.

Examples. $f_1 = T - 1$; $f_2 = T + 1$; $f_4 = T^2 + 1$; $f_p = 1 + T + T^2 + \cdots + T^{p-1}$ if p is a prime integer.

Theorem 2.39. $f_d \in \mathbf{Z}[T]$; $\deg f_d = \phi(d)$.

Remark. Of course $\mathrm{char}(k)$ may be finite, in this case the Theorem means that the coefficients of f_d are the elements of the prime field $\mathbf{F}_p$.

Proof. Let $k_0 \subset k$ be any subfield. Then $k_0(\zeta)$ contains all the roots of unity of degree n since ζ is primitive. Any automorphism of $k_0(\zeta)$ sends the elements of the group of roots of 1 to the elments of that group preserving the order of the element. Hence $f_d(T) \in k_0[T]$, whichever is k_0. This means that if $\mathrm{char}(k) = 0$ then $f_d(T) \in \mathbf{Q}[T]$ (hence $f_d(T) \in \mathbf{Z}[T]$ by the Gauss Lemma) while if $\mathrm{char}(k) = p$ then $f_d(T) \in \mathbf{F}_p[T]$. If $d|n$ then the number of elements of order exactly d in the cyclic group of order n equals $\phi(d)$ which finishes the proof ■

Theorem 2.40. f_d is irreducible over $\mathbf{Q}$.

Proof. Choose $\zeta \in \overline{\mathbf{Q}}$ a primitive d - root of 1. Then $P_\zeta | f_d$. Let p be any prime integer not dividing d. Clearly ζ^p is also a primitive d - root. We are going to prove that ζ^p

is a root of P_ζ. Indeed, suppose the opposite is true. Then $f_d = P_\zeta g$ and ζ^p is a root of g. Define $h(T) \stackrel{\text{def}}{=} g(T^p)$, then ζ is a root of h. Therefore $P_\zeta \,|\, h$. P_ζ, g and h are all in $\mathbf{Z}[T]$ so one may consider residues $\mod p$. Then $h(T) = g(T^p) \equiv (g(T))^p \mod p$. Since $P_\zeta \mid h$ P_ζ and g have common roots in $\overline{\mathbf{F}_p}$ which is impossible as both are factors of $T^d - 1$. Since any primitive d - root could be obtained from ζ by successive taking prime powers, all of them are the roots of P_ζ, therefore $f_d = P_\zeta$ ■

Remark. Any quadratic extension of $\mathbf{Q}$ is a subfield of some field generated by the roots of 1. Indeed, let ζ be a p - root of 1. Consider the Gaussian sum $\tau_p \stackrel{\text{def}}{=} \sum\limits_{a \mod p} \left(\frac{a}{p}\right) \zeta^a$. Then $\tau_p^2 = (-1)^{\frac{p-1}{2}} p$ (an easy calculation). Thus, $\mathbf{Q}(\sqrt{p}) \subset \mathbf{Q}(\zeta, \sqrt{-1})$. This is a small part of the deep Kronecker-Weber theorem which states that any Galois extension $K/\mathbf{Q}$ such that $\mathrm{Gal}\,(K/\mathbf{Q})$ is commutative is contained in the field generated over $\mathbf{Q}$ by the roots of 1.

Definition 2.41. Suppose K/k is a finite extension, $\alpha \in K$. Then the multiplication with α defines a linear transformation of the k-vector space K. Its characteristic polynomial is called the characteristic polynomial of α (notation $\chi_{\alpha,\,K/k}(T)$), its determinant is called the norm of α (notation $N_{K/k}(\alpha)$) and its trace is called the trace of α (notation $Tr_{K/k}(\alpha)$).

Remark 1. Clearly $N : K^* \to k^*$ and $Tr : K^+ \to k^+$ are the group homomorphisms.

Remark 2. If $[K : k] = n$ and $\chi_{\alpha,\,K/k}(T) = \sum_{i=0}^{n-1} a_i T^i + T^n$ then $Tr_{K/k}(\alpha)) = -a_{n-1}$ and $N_{K/k}(\alpha) = (-1)^n a_0$ (this is a standard statement from linear algebra which is true for the determinant and trace of an arbitrary linear transformation).

Remark 3. If $[K : k] = n$ and $\alpha \in k$ then $\chi_{\alpha,\,K/k}(T) = (T - \alpha)^n$, $N_{K/k}(\alpha) = \alpha^n$, $Tr_{K/k}(\alpha) = n\alpha$.

Theorem 2.42. Suppose $[K : k] = n$, $\alpha \in K$, $\deg P_{\alpha,\,K/k} = d$. Then $\chi_{\alpha,\,K/k} = P_{\alpha,\,K/k}^{\frac{n}{d}}$.

Proof. Consider the tower $k \subset k(\alpha) \subset K$. Let $m = \frac{n}{d}$. The set $\{\alpha^i,\ 0 \le i \le d-1\}$ is a vector space basis for $k(\alpha)$ over k. Let $\{y_j,\ 1 \le j \le m\}$ be any basis of the vector space K over $k(\alpha)$. As we have earlier proved $\{\alpha^i y_j\}$ is a basis for K over k. The matrix of the multiplication with α in that basis is a block matrix consisting of m equal blocks of the form

$$\begin{pmatrix} 0 & 0 & \dots. & & -a_0 \\ 1 & 0 & \dots. & & -a_1 \\ \dots & \dots & \dots & \dots & \dots \\ \dots. & 1 & 0 & & -a_{d-2} \\ 0 & \dots. & & 1 & -a_{d-1} \end{pmatrix}$$

where a_j are the coefficients of the polynomial $P_\alpha(T) = \sum_{i=0}^{d-1} a_i T^i + T^d$. The characteristic polynomial of each block equals P_α (please check and calculate) which finishes the proof of the Theorem ■

Theorem 2.43. Suppose K/k is separable. Then $\forall \alpha \in K$ $N_{K/k}(\alpha) = \prod_{\sigma \in \Sigma_{K/k}^{\bar{k}/k}} \sigma(\alpha)$,

$Tr_{K/k}(\alpha) = \sum_{\sigma \in \Sigma_{K/k}^{\bar{k}/k}} \sigma(\alpha)$.

Proof. Let us prove the statement for the norm (the proof for the trace is close). Consider the tower $k \subset k(\alpha) \subset K$. Let again $d = \deg P_\alpha$, $n = [K : k]$, $m = \frac{n}{d}$. Then $N_{K/k}(\alpha) = \det(\cdot\alpha) = (-1)^n\cdot$ (the free term of $\chi_{\alpha,\, K/k}$). By the Theorem 2.42 this equals $((-1)^d(\text{free term of } P_{\alpha,\, K/k}))^m$. Clearly the free term of $P_{\alpha,\, K/k}$ equals $(-1)^d \prod\limits_{\overline{\sigma}\in\Sigma^{\overline{k}/k}_{k(\alpha)/k}} \overline{\sigma}(\alpha)$.

For any $\sigma \in \Sigma^{\overline{k}/k}_{K/k}$ $\sigma(\alpha)$ depends only on the restriction $\overline{\sigma}$ of σ to $k(\alpha)$, each fiber of this surjective restriction map containing m elements by the proof of the Theorem 2.18. This ends the proof ■

Example 8. Cyclic extensions.

Theorem 2.44. (linear independence of characters). Suppose C is an arbitrary group, K any field. Suppose $\chi_1, \dots, \chi_n : C \to K^*$ are different homomorphisms. Then the maps χ_i are linearly independent over K.

Proof. Suppose the opposite is true. Choose a shortest linear relation $\sum a_i\chi_i = 0$. This means that $\forall c \in C$ $\sum a_i\chi_i(c) = 0$. One may change c to c_0c in this equation to conclude that $\forall c \in C$ $\sum a_i\chi_i(c_0c) = \sum a_i\chi_i(c_0)\chi_i(c) = 0$ thus the linear relation $\sum \chi_i(c_0)a_i\chi_i = 0$ is also valid. Now choose c_0 for which $\chi_1(c_0) \neq \chi_2(c_0)$, multiply the first linear relation with $\chi_1(c_0)$ and substract from the second one obtaining the shorter linear relation which contradicts the assumption ■

Theorem 2.45. (Theorem 90 Hilbert's) Suppose K/k is a cyclic extension (i.e. finite Galois extension with a cyclic Galois group). Suppose σ is a generator of $\mathrm{Gal}\,(K/k)$, $\alpha \in K$. Then $N_{K/k}(\alpha) = 1 \Leftrightarrow \exists\beta \in K$ such that $\alpha = \frac{\sigma(\beta)}{\beta}$.

Proof. $\Leftarrow$ By the Theorem 2.43 $N_{K/k}(\sigma(\beta)) = N_{K/k}(\beta)$ ■
$\Rightarrow$ Let $n = [K : k]$. Consider the map $\psi : K^* \to K$, $\psi(x) = x + \alpha\sigma(x) + \alpha\sigma(\alpha)\sigma^2(x) + \cdots + \alpha\sigma(\alpha)\sigma^2(\alpha)\dots\sigma^{n-2}(\alpha)\sigma^{n-1}(x)$. The map ψ is a linear combinations of characters for the group $C = K^*$ which fits the conditions of Theorem 2.44. Therefore $\exists z \in K^*$ such that $\psi(z) \neq 0$. Since $N_{K/k}(\alpha) = 1$ $\alpha\sigma(\psi(z)) = \psi(z)$ hence $\alpha = \frac{\sigma(\psi(z)^{-1})}{(\psi(z)^{-1})}$ ■

Theorem 2.46. Suppose $\gcd(\mathrm{char}(k), n) = 1$. Let $\zeta \in \overline{k}$ be a primitive n - root of 1. Suppose $\zeta \in k$. Then
1) K/k is cyclic of degree n $\Rightarrow$ $\exists b \in k$ such that $K \simeq k_{T^n-b}$.
2) $\forall b \in k$ $k_{T^n-b,\,\mathrm{split}}$ is cyclic of some degree d, $d|n$.

Proof. 1) Let σ be a generator of $\mathrm{Gal}\,(K/k)$. Since $\zeta \in k$ $N_{K/k}(\zeta) = \zeta^n = 1$ hence by the previous theorem $\exists \beta \in K$ such that $\sigma(\beta) = \zeta\beta$. Then $\forall i$ $\sigma^i(\beta) = \zeta^i\beta$, therefore $[k(\beta) : k]_s \geq n$ hence $[k(\beta) : k] \geq n$ thus $K = k(\beta)$. But $\sigma(\beta^n) = (\sigma(\beta))^n = \zeta^n\beta^n = \beta^n$. Since σ generates $\mathrm{Gal}\,(K/k)$ the latter acts trivially on β^n hence $\beta^n \in k$ ■
2) Let $\beta \in \overline{k}$ be a root of the polynomial $T^n - b$. Any other root of $T^n - b$ is of the form $\zeta^i\beta$ for some i hence $k(\beta)$ is normal over k. Since $\gcd(\mathrm{char}(k), n) = 1$ it is also separable. Let $G = \mathrm{Gal}\,(k(\beta)/k)$. $\forall g \in G$ $g(\beta) = \omega\beta$, $\omega^n = 1$ (ω is not necessary primitive). This gives an injective homomorphism $G \hookrightarrow$ {group of roots of 1 of degree n in k}.The latter is cyclic of order n hence G is cyclic of some order dividing n ■

Theorem 2.47. Suppose char(k)=p. Then
1) K/k is cyclic of degree p $\Rightarrow$ $\exists b \in k$ such that $K \simeq k_{T^p-T-b}$.
2) $\forall b \in k$ $T^p - T - b$ is either irreducible or splits totally in $k[T]$. In the former case k_{T^p-T-b} is cyclic of degree p.

Lemma (Hilbert's 90, additive form). Suppose K/k is cyclic of degree n , σ is a generator of $\mathrm{Gal}\,(K/k)$,
$\alpha \in K$. Then $Tr_{K/k}(\alpha) = 0 \Leftrightarrow \exists \beta \in K$ such that $\alpha = \sigma(\beta) - \beta$.

Proof of the Lemma. $Tr : K \to k$ is a k-linear map which is nonzero by 2.43 and 2.44, hence $\dim_k \ker(Tr) = n-1$. By Galois Theory, $\ker(\sigma - \mathrm{Id}\,) = k$ hence $\dim_k \mathrm{im}\,(\sigma - \mathrm{Id}\,) = n - 1$. Obviously $\mathrm{im}\,(\sigma - \mathrm{Id}\,) \subset \ker(Tr)$ ■

Proof of the Theorem. 1) Consider $\alpha = 1$. $Tr_{K/k}(\alpha) = p\alpha = 0 \Rightarrow 1 = \sigma(\beta) - \beta$ for some $\beta \in K$. $\sigma(\beta) \neq \beta$ hence $\beta \notin k$. Since the degree $[K : k]$ is prime there are no subfields between k and K thus $k(\beta) = K$. Let $b = \beta^p - \beta$. Then $\sigma(b) = \sigma(\beta^p) - \sigma(\beta) = (\sigma(\beta))^p - \sigma(\beta) = (1+\beta)^p - (1+\beta) = 1 + \beta^p - 1 - \beta = b$, therefore $b \in k$ ■
2) The polynomial $P(T) = T^p - T - b$ is separable. Suppose $\beta \in \overline{k}$ is its root. Then the full set of the roots of P coincides with $\beta, \beta+1, \beta+2, \ldots, \beta+(p-1)$. It is easy to see that the map $\mathrm{Gal}\,(k_{P,\,\mathrm{split}}/k) \to \mathbf{Z}/(p)$ which sends $g \mapsto g(\beta) - \beta$ is an injective homomorphism . Hence it is either isomorphic or trivial ■

Remark. To describe cyclic extensions of degree p^k, $k > 1$ over the field k of characteristic p one needs more complicated method (Witt vectors).

Example 9. Solving equations in radicals.

We restrict ourselves to the classical problem of solving equations over $\mathbf{Q}$. First prove an important general theorem about Galois extensions.

Theorem 2.48. Suppose K/k is a finite Galois extension, M/k any extension (not necessary algebraic). Suppose both K and M are subfields of some field $\widetilde{k}$. Let $KM \subset \widetilde{k}$ be the composite field (i.e the minimal subfield of $\widetilde{k}$ containing both K and M).
Then KM/M is finite Galois, $\mathrm{Gal}\,(KM/M) = \mathrm{Gal}\,(K/K \bigcap M)$.

Proof. K/k is separable therefore $\exists P \in k[T]$ irreducible and separable such that $K \simeq k_P$. Since K/k is normal $K = k_{P,\,\mathrm{split}}$. By definition $KM = M_{P,\,\mathrm{split}}$ hence KM/M is finite Galois. Consider the restriction homomorphism $\mathrm{Gal}\,(KM/M) \to \mathrm{Gal}\,(K/k)$, $\sigma \mapsto \sigma|_K$. It is injective (if $\sigma|_K = \mathrm{Id}$ then σ acts trivially on the roots of P hence on $KM = M_{P,\,\mathrm{split}}$) and its image is contained in $\mathrm{Gal}\,(K/K \bigcap M)$. Let H be this image. Suppose $\alpha \in K$. If H acts trivially on α then $\alpha \in M$ by the Galois theory for KM/M. This means $\alpha \in K \bigcap M$. Therefore by the Galois theory for $K/K \bigcap M$ H must coincide with the entire group $\mathrm{Gal}\,(K/K \bigcap M)$ ■

Definition 2.49. Suppose $K/\mathbf{Q}$ is a finite extension. Let $L/\mathbf{Q}$ be the minimal Galois extension such that $K \subset L$. The extension $K/\mathbf{Q}$ is called solvable iff $\mathrm{Gal}\,(L/\mathbf{Q})$ is a solvable group (recall this means that G admits a composition series of subgroups $\{1\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_r = G$ such that $\forall i,\ 1 \le i \le r,\ G_i/G_{i-1}$ is cyclic).

Definition 2.50. Suppose $P(T) \in \mathbf{Q}[T]$ is irreducible. The equation $P(X) = 0$ could be solved in radicals iff there exist a field $L \supset \mathbf{Q}_{P,\,\mathrm{split}}$ and a sequence of subfields $\mathbf{Q} = L_0 \subset L_1 \subset \cdots \subset L_s = L$ such that $\forall i,\ 1 \le i \le s,\ \exists \alpha \in L_i$ such that $L_i = L_{i-1}(\alpha)$ and α is a root of the polynomial $T^m - a = 0$ for some $a \in L_{i-1}$ and some positive integer m.

Theorem 2.51. The equation $P(X) = 0$ could be solved in radicals $\Leftrightarrow$ $\mathbf{Q}_P/\mathbf{Q}$ is solvable.

Proof. $\Rightarrow$ Let $K = \mathbf{Q}_{P,\,\mathrm{split}}$. Choose an algebraic closure $\overline{\mathbf{Q}}$ so that $\mathbf{Q} \subset K \subset L \subset \overline{\mathbf{Q}}$, L being a field from the Definition 2.50. If $L/\mathbf{Q}$ is not normal then let $\widetilde{L}$ (resp. $\widetilde{L_i}$) be the minimal subfield of $\overline{\mathbf{Q}}$ which contains all the fields $\sigma(L)$(resp. $\sigma(L_i)$), $\sigma \in \Sigma^{\overline{\mathbf{Q}}/\mathbf{Q}}_{L/\mathbf{Q}}$. Then $\widetilde{L}$ enjoys the same property as L. Indeed, $\widetilde{L_i}$ could be generated over $\widetilde{L_{i-1}}$ by adding the roots of certain polynomial $T^m - a$ one by one (if $L_i = L_{i-1}(\alpha)$ then $\sigma(L_i) = \sigma(L_{i-1})(\sigma(\alpha))$). Thus, one may suppose $L/\mathbf{Q}$ is normal. Let $n = [L : \mathbf{Q}]$ and let $\zeta \in \overline{\mathbf{Q}}$ be a primitive root of 1 of degree n. Consider the sequence of fields $L_0(\zeta) \subset L_1(\zeta) \subset \cdots \subset L_s(\zeta)$. $L(\zeta)/\mathbf{Q}(\zeta)$ is Galois by the Theorem 2.48 and $\forall i,\ 1 \leq i \leq s,\ L_i(\zeta)/L_{i-1}(\zeta)$ is Galois cyclic by the assumption and by the Theorem 2.46. By definition, this means that $\mathrm{Gal}\,(L(\zeta)/\mathbf{Q}(\zeta))$ is solvable. $\mathrm{Gal}\,(\mathbf{Q}(\zeta)/\mathbf{Q})$ is commutative hence also solvable. The rest is simple group theory ■

$\Leftarrow$ Choose an algebraic closure $\overline{\mathbf{Q}}$ so that $\mathbf{Q} \subset \mathbf{Q}_{P,\,\mathrm{split}}(\overset{\mathrm{def}}{=} K) \subset \overline{\mathbf{Q}}$. Let $n = [K :\ \mathbf{Q}\ ]$, $\zeta \in \overline{\mathbf{Q}}$ a primitive root of 1 of degree n. By the Theorem 2.48 $K(\zeta)/\mathbf{Q}(\zeta)$ is Galois, $\mathrm{Gal}\,(K(\zeta)/\mathbf{Q}(\zeta))$ being isomorphic to a subgroup of $\mathrm{Gal}\,(K/\mathbf{Q})$. The latter group is solvable by the assumption hence the former group is solvable (again simple group theory). This means (by the Theorem 2.46) that the equation $P(X) = 0$ could be solved in radicals over $\mathbf{Q}(\zeta)$ hence also over $\mathbf{Q}$ ■

To finish our survey of Galois Theory it remains to discuss two results related to linear algebra.

Theorem 2.52. Suppose K/k is a finite separable extension, M/k any extension. Then there exists a M - algebra isomorphism $K \otimes_k M \simeq \oplus M_i$ where M_i are finite extensions of M of the type $M_{P_i},\ P_i \in M[T],\ \sum \deg P_i = [K : k]$. The set $\{M_i\}$ is unique up to a permutation.

Proof. Choose $P \in k[T]$ irreducible such that $K \simeq k_p$. Then there exist isomorphisms of M - algebras $K \otimes_k M \simeq (k[T]/(P)) \otimes_k M \simeq M[T]/(P)$. Let $P = \prod P_i$ be the decomposition of P in irreducible factors in the ring $M[T]$. Since P is separable same are all the P_i and they are pairwise coprime. The Chinese remainder theorem for the ring $M[T]$ leads to a further isomorphism $M[T]/\prod P_i \simeq \oplus M[T]/(P_i)$. Suppose now that there exists an M - algebra isomorphism $\phi : \oplus M_i \overset{\sim}{\to} \oplus M'_j$. Let $\pi_i : \oplus M_i \to M_i,\quad \pi'_j : \oplus M'_j \to M'_j$ be the natural projections, $I_i \overset{\mathrm{def}}{=} \ker(\pi_i)$. Then $\prod I_i = (0)$ hence $\forall j\ \ \prod(\pi'_j \circ \phi(I_i)) = \pi_j \circ \phi(\prod I_i) = (0)$. Therefore $\forall j\ \ \exists i$ such that $\pi'_j \circ \phi(I_i) = (0)$ (recall that M'_j is a field). Since the ideal $I_{i_1} + I_{i_2}$ contains 1 (i_1 and i_2 being different) such i is unique for j given, otherwise $\pi'_j \circ \phi$ were zero while it is surjective by the assumption. So i is uniquely defined after the choice of j. Since $\pi'_j \circ \phi(I_i) = (0)$ there exists a homomorphism $\phi_{ij} : M_i \to M'_j$ such that $\pi'_j \circ \phi = \phi_{ij} \circ \pi_i$. ϕ_{ij} is surjective by the assumption and injective because M_i is a field. This ends the proof ■

Remark. Besides the polynomials P_i are pairwise coprime some of the fields M_i may still be isomorphic.

Theorem 2.53. If K/k is separable then $Tr(ab) : K \times K \to k$ is a nondegenerate symmetric bilinear form. Otherwise the trace map is zero.

Proof. Suppose first that K/k is not separable, so $\mathrm{char}(k) = p$. Let $\alpha \in K$. By the Remark 2 after the Definition 2.41 $Tr_{K/k}(\alpha)$ is the negative of the second leading coefficient of its characteristic polynomial. By the Theorem 2.42 $\chi_{\alpha,\, K/k} = P^{\frac{n}{d}}_{\alpha,\, K/k}$ where $[K : k] = n$ and $\deg P_{\alpha,\, K/k} = d$. If $K/k(\alpha)$ is not separable then $p|\frac{n}{d}$ hence the degrees of all nonzero terms of $\chi_{\alpha,\, K/k}$ are divisible by p. If $K/k(\alpha)$ is separable then α is not (otherwise K/k were separable), hence the statement about the degrees is true for the $P_{\alpha,\, K/k}$. In both cases $Tr_{K/k}(\alpha)$ is zero.
Now let K/k be separable. Suppose there exists $a \in K$ such that $\forall b \in K\ Tr(ab) = 0$. Since$K/k$ is separable one may use Theorem 2.43, thereby concluding that $\forall b \in K$ $\sum\limits_{\sigma \in \Sigma^{\overline{k}/k}_{K/k}} \sigma(a)\sigma(b) = 0$. This contradicts to the Theorem 2.44 according to which the group homomorphisms $\sigma_i : K^* \to \overline{k^*}$ must be linearly independent ■