3. 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 3.1. 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 3.2. 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 3.3. 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 3.4. 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 3.5. 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. $[k_P : k] = \deg P$ (see Problem 19).
$k(\alpha)$. 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 3.6. 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 3.7. 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 (see Problem 20) ■

Theorem 3.8. 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 3.6.2). 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 3.9. Suppose K is generated over k by any number of algebraic elements. Then K/k is algebraic.

Proof. By 3.6.2) and by the Remark before Theorem 3.6 it suffices to prove that $\alpha \pm \beta,\ \alpha\beta$ are algebraic over k for any $\alpha,\ \beta \in k$. As in the proof of the previous theorem one may conclude that $k(\alpha, \beta)/k$ is finite. Therefore it is algebraic ■

Theorem 3.10. 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 3.6.2), k_1/k finite by the Theorem 3.8. So $k_1(\alpha)/k$ is finite by the Theorem 3.7, hence algebraic. In particular α is algebraic over k ■

Definition 3.11. 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 3.12. $\forall k\, \exists\, \overline{k}/k$ 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 $k \subset K_1 \subset K_2 \subset K_3 \dots$ as in step 1 (for all i any nonconstant polynomial with coefficients in K_i has a root in K_{i+1}). Let $\overline{k} \stackrel{\text{def}}{=} \bigcup K_i$. Clearly the set $\overline{k}$ carries the natural structure of the field. By the Theorem 3.10 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 3.13. 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 $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ be the full list of the roots of P_α in K. $k(\alpha_1, \dots, \alpha_n)/k$ is finite by the Theorem 3.8. $\sigma(k(\alpha_1, \dots, \alpha_n)) \subset k(\alpha_1, \dots, \alpha_n)$ (see the key Lemma 3.2). 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 3.14. 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 $\widetilde{\sigma} \mid_k = \mathrm{Id}$ 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 3.15. 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 3.6.2) and the Example above ■

Theorem 3.16. 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 3.17. 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 3.18. 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 3.19. A finite extension K/k is called finite separable iff $[K:k]_s = [K:k]$.

Definition 3.20. 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 3.21. 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 3.22. For the finite extension K/k Definitions 3.19 and 3.20 lead to the same concept.

Proof. If K/k fits the Definition 3.19 then $\forall \alpha \in K \quad k \subset k(\alpha) \subset K$ hence $k(\alpha)/k$ also fits 3.19 by the Theorem 3.18. 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 3.21 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 3.18 ■

Theorem 3.23. 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 3.24 (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 $i \neq j$ $\sigma_i(\alpha + \beta t_0) \neq \sigma_j(\alpha + \beta t_0)$. 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.

Problems. (the deadline for 19-23 is October, 11th).

19. Prove that $[k_P : k] = \deg P$.
20. Prove that $\{x_i y_j\}$ is a basis of the vector space L over k provided that $\{x_i\} \in K$ is a basis of the vector space K over k, $\{y_j\} \in L$ same for L over K.
21. Suppose K/k is finite separable, $\Sigma_{K/k}^{\overline{k}/k} = \{\sigma_1, \ldots, \sigma_n\}$. Prove that $\alpha \in K$ generates K over $k \Leftrightarrow \sigma_i(\alpha)$ are all different.
22. Construct an example of finite extension K/k such that K is not generated by one element over k.
23. Prove that $\mathbf{F}_{p^m} \subset \mathbf{F}_{p^n} \Leftrightarrow m \,|\, n$.