MA 315 Galois Theory / January-April 2013

(Int. PhD, ME, MSc, PhD Programmes)

Download from : http://www.math.iisc.ernet.in/patil/courses/courses/Current Courses/...

Tel : +91-(0)80-2293 2239/(Maths Dept. 3212) **E-mails :** dppatil@csa.iisc.ernet.in / patil@math.iisc.ernet.in

Lectures : Monday and Wednesday ; 11:00–12:30 **Venue:** MA Lecture Hall I

2. Algebraic Extensions

Monday, March 17, 2014

2.1 Let $K|k$ be a field extension.

(a) Show that the following statements are equivalent:

(i) $K|k$ is algebraic.

(ii) For every intermediary subfield $L \in \mathfrak{F}(K|k)$, every k-algebra homomorphism $\sigma : L \to L$ is an automorphism.

(b) Let $x, y \in K$ be such that y is algebraic over $k(x)$ and y is transcendental over k. Show that x is algebraic over $k(y)$.

(c) Let $x, y \in K$ be algebraic over k. Prove that $\mu_{x,k}$ is irreducible over $k(y)$ if and only if $\mu_{y,k}$ is irreducible over $k(x)$. (**Remark :** For generazation see Exercise T2.6.)

2.2 Let k be a field of characteristic $\neq 2$.

(a) Let $K|k$ be a field extension of degree $[K : k] = 2$. Show that $K = k(x)$ with $x^2 = a \in k$. Moreover, show that $K|k$ is Galois extension with Galois group $\mathrm{Gal}(K|k) \approx \mathbb{Z}^\times$.

(b) Let $K|k$ be a field extension and let $x, y \in K$ with $x^2 = b \in k$ and $y^2 = b \in k$. Determine necessary and sufficient condition so that there exists a k-algebra isomorphism $k(x) \xrightarrow{\sim} k(y)$. (**Remark :** In any case there exists a k-vector space isomorphism $k(x) \xrightarrow{\sim} k(y)$. See also Exercise T2.3.)

(c) Let $z, w \in \mathbb{C}$ be algebraic numbers with $\mu_{z,\mathbb{Q}} = X^2 - 2$ and $\mu_{w,\mathbb{Q}} = X^2 - 4X + 2$. Show that there exist an isomorphism $\mathbb{Q}(z) \xrightarrow{\sim} \mathbb{Q}(w)$ of fields.

2.3 (Simple field extensions) A field extension $K|k$ is called simple with primitive element $x \in K$ if $K = k(x)$.

(a) Let $K|k$ be a simple algebraic field extension with primitive element $x \in K$. Let L be an intermediary subfield of $K|k$ and let $\mu_{x,L} = b_0 + b_1 X + \cdots + b_{m-1}X^{m-1} + X^m \in L[X]$ be the minimal polynomial of x over L. Show that $L = k(b_0, \ldots, b_{m-1})$. (**Hint :** Put $L' := k(b_0, \ldots, b_{m-1})$. Then $L' \subseteq L$, $L'(x) = L(x) = K$ and $\mu_{x,L} = \mu_{x,L'}$.)

(b) (Steinitz) Let $K|k$ be an algebraic field extension. Show that $K|k$ is simple if there are only finitely many intermediary subfields. (**Hint :** Let $\mathfrak{F}(K|k)$ denote the set of intermediary subfields of $K|k$. ($\Rightarrow$): Assume $K = k(x)$ is simple and let $\mathfrak{D}(x) := \{g \in K[X] \mid g \text{ is monic divisor of } \mu_{x,k} \text{ in } K[X]\}$. Use part (a) to show that the map $\mathfrak{D}(x) \to \mathfrak{F}(K|k)$, $g = b_0 + b_1 X + \cdots + b_{m-1}X^{m-1} + X^m \mapsto k(b_0, \ldots, b_{m-1})$ is surjective. ($\Leftarrow$): Assume that $\mathfrak{F}(K|k)$ is finite. We may also assume that k is infinite. Since $\{k(x) \mid x \in K\} \subseteq \mathfrak{F}(K|k)$ is finite, we can choose $x \in K$ with $[k(x) : k]$ maximal. We claim that $K = k(x)$. For, if $y \in K \setminus k(x)$, then consider the finite set $\{k(x + ay) \mid a \in k\} \subseteq \mathfrak{F}(K|k)$. Therefore, since k is infinite, there exist distinct $a, b \in k$ such that $k(x + ay) = k(x + by)$, but then $y = (a - b)^{-1}((x + ay) - (x + by)) \in k(x + ay)$ and hence $k(x + ay) = k(x, y) \supsetneq k(x)$ which contradicts the maximality of $[k(x) : k]$.)

(c) The assumption that $K|k$ is algebraic is necessary in part (b). More precisely, show that the simple field extension $k(X)|k$ has infinitely many intermediary subfields. (**Hint :** Note that $k(X^n) \in \mathfrak{F}(k(X)|k)$ for every $n \in \mathbb{N}^*$ and by part (a) $k(X^n) = k(X^m)$ for $n, n \in \mathbb{N}^*$, $n \neq m$.)

2.4 **(a)** Let $K = k(x)$ be a finite simple extension of a field k of degree n. Show that the number of

intermediate fields L with $k \subseteq L \subseteq K$ is at most 2^{n-1}, i. e. $\#\mathfrak{F}(K|k) \leq 2^{[K:k]-1}$. Give an example to show that this inequality can be very strict.

(b) Let $K|k$ be a field extension and let $x, y \in K^\times$. If $x^m \in k$ and $y^n \in k$ for some relatively prime natural numbers $m, n \in \mathbb{N}^*$. Show that $x \cdot y$ is a primitive element of the field extension $k(x,y)|k$. (**Hint :** There exists $s, t \in \mathbb{Z}$ such that $1 = zm + tn$.)

(c) Let X, Y be two indeterminates over $\mathbb{Z}_p$ and let $k := \mathbb{Z}_p(X^p, Y^p) \subseteq \mathbb{Z}_p(X,Y) =: K$. Show that the field extension $K|k$ has degree p^2 and is not simple. Exhibit an infinite number of many intermediary subfields of $K|k$. (**Hint :** Note that $[k(X+fY) : k] = p$ for every $f \in k$.)

2.5 Let p, q be prime numbers with $q < p$ and let k be a field of characteristic $\neq p$. Let $K(x,y)|k$ be a field extension with $[k(x) : k] = p$ and $[k(y) : k] = q$. Show that $K|k$ is a simple extension with primitive element $x + y$. (**Hint :** If the assertion is not true, then $\mu_{x+y,k}(X+y) = \mu_{x,k}$ and $\mu_{x+y,k}(x+X) = \mu_{y,k}$ which is not possible by assumptions.)

2.6 (Galois group of the function field) Let k be a field and let $K = k(X)$ be the rational function field in one indeterminate X over k.

(a) Let $\varphi \in k(X)$ be a non-constant rational function (i. e. $\varphi \notin k$). Show that the field extension $K|k(\varphi)$ is finite. Moreover, show that $[K : k(\varphi)] = \deg \varphi$, where for a rational function $\varphi = f/g$ with $f, g \in k[X]$, $\gcd(f,g) = 1$, put $\deg \varphi := \max\{\deg f, \deg g\}$. (**Hint :** Since X is a zero of the polynomial $f(Y) - \varphi \cdot g(Y) \in k(\varphi)[Y]$, X is algebraic over $k(\varphi)$. Use $gcd(f,g) = 1$ to show that $\mu_{X,k(\varphi)} = f(Y) - \varphi \cdot g(Y)$.)

(b) If $L \in \mathfrak{F}(k(X)|k)$ is an intermediary subfield with $k \neq L$, then show that the field extension $k(X)|L$ is finite. (**Hint :** Choose $\varphi \in L \setminus k$ and use the part (a).)

(c) Let $\varphi = f/g \in k(X) \setminus k$ with $\gcd(f,g) = 1$. Show that the map $k(X) \to k(X)$, $F/G \mapsto F(\varphi)/G(\varphi)$ is a k-algebra homomorphism. Moreover, it is a k-algebra automorphism if and only if $\deg \varphi = \max\{\deg f, \deg g\} = 1$.

(d) Show that the map

$$\mathrm{Gal}\,(k(X)|k) \to \mathrm{PGL}_2(k) := \mathrm{GL}_2(k)/k^\times \quad \sigma \mapsto \text{ the image of } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ in } \mathrm{PGL}_2(k)$$

is a canonical isomorphism of groups, where σ is defined by $\sigma(X) = \dfrac{aX+b}{cX+d}$, see the part (c). (**Remarks :** The group $\mathrm{PGL}_n(k)$ is the well-known group of projective collineations of the projective space $\mathrm{P}_k(k^n)$ over k. It is called the Projective linear group over k and often occurs in Projective Geometry, Complex Analysis and Riemann Surfaces.)

(e) If k is infinite then show that $\mathrm{Fix}_{\mathrm{Gal}\,(k(X)|k)}\, k(X) = k$. (**Hint :** The group $\mathrm{Gal}\,(k(X)|k)$ is generated by the elements $X \mapsto aX$, $X \mapsto X + b$, $X \mapsto 1/X$, with $a \in k^\times, b \in k$.)

(f) Show that the set of translations $\mathrm{T}(k(X)|k) := \{\tau_a \in \mathrm{Gal}\,(k(X)|k) \mid \tau_a(X) = X + a, a \in k\}$ is a subgroup of the Galois group $\mathrm{Gal}\,(k(X)|k)$. Moreover, the map $(k, +) \to \mathrm{T}(k(X)|k)$, $a \mapsto \tau_a$ is an isomorphism of groups. If k is infinite then show that $\mathrm{Fix}_{\mathrm{T}(k(X)|k)}\, k(X) = k$.

(g) Assume that the characteristic of k is 0. Let $a \in k^\times$ and let $\mathrm{H}(\tau_a) \subseteq \mathrm{Gal}\,(k(X)|k)$ be the subgroup of $\mathrm{Gal}\,(k(X)|k)$ generated by $\tau_a : k(X) \to k(X)$, $X \mapsto X + a$. Show that G is infinite cyclic. Determine the fixed field $\mathrm{Fix}_{\mathrm{H}(\tau_a)}\, k(X)$. What is $[k(X) : \mathrm{Fix}_{\mathrm{H}(\tau_a)}\, k(X)]$?

2.7 Let k be a field of characteristic 0 and let $k(X)$ be the field of rational functions in one indeterminate X over k. Let $L := k(X^2)$, $L' := k(X^2 + aX + b)$ be two intermediary subfields of $k(X)|k)$. Show that both field extensions $k(X)|L$ and $k(X)|L'$ are finite field extensions of degrees 2. Moreover, show that if $a \neq 0$, then $L \cap L' = k$ and hence the field extension $k(X)|(L \cap L')$ is not algebraic. (**Hint :** Use Exercise2.?-(a) and note that $\varphi \in L'$ if and only if $\varphi(-X - a) = \varphi(X)$. Show that any $\varphi \in k(X)$ with $\varphi(X + a) = \varphi(X)$ must be constant (here one needs to use $\mathrm{Char}\, k = 0$).)

2.8 Let k be a finite field with q elements, $K|k$ be a finite extension of k and let $0 \neq x \in K$. Let $d \in \mathbb{N}$ be the order of $x \in K^\times$ in the multiplicative group $K^\times$ of K. Show that $s := [k(x) : k]$ is equal to the order of the residue class of q in the unit group $(\mathbb{Z}/\mathbb{Z}d)^\times$ of the ring $\mathbb{Z}/\mathbb{Z}d$. Moreover, show that s is the smallest positive natural number with $x = x^{q^s}$ and $\mu_{x,k} = \prod_{i=0}^{s-1} (X - x^{q^i})$ is the minimal polynomial of x over k.

2.9 (Compositum of subfields) Let $K|k$ be a field extension. For two intermediary subfields L and L' of $K|k$, the compositum $L \cdot L'$ of L and L' is the smallest subfield of K which contain $L \cup L'$.

For two intermediary subfields L and L' of a field extension $K|k$, show that:

(a) $L \cdot L' = L(L') = L'(L)$.

(b) If $L|k$ is algebraic, then so is $L \cdot L'|L'$. Moreover, if $L|k$ is finite, then so is $L \cdot L'|L'$ and $[L \cdot L' : L'] \leq [L : k]$, but, in general, $[L \cdot L' : L]$ is not a divisor of $[L : k]$. (**Hint :** Consider $L = \mathbb{Q}(x)$ and $L = \mathbb{Q}(\zeta_3 x)$, where $x \in |R$ is the cube root of 2 and $\zeta_3 = e^{2\pi \mathrm{i}/3}$.)

(c) $L \cdot L'$ is finite over k if and only if both $L|k$ and $L'|k$ are finite. Moreover, in this case $[L \cdot L : k] \leq [L : k] \cdot [L' : k]$. Further, if $\gcd([L : k], [L' : k]) = 1$, then the equality holds. Give an example of intermediary subfields L, L' of $K|k$ such that $[L \cdot L' : k] < [L : k] \cdot [L' : k]$.

(d) If $L \cdot L'$ is finite over k and the equality $[L \cdot L : k] = [L : k] \cdot [L' : k]$ hold, then show that $L \cap L' = k$. Further, show that the converse holds if either $[L : k] = 2$ or $[L' : k] = 2$. Use Example in the Hint of part (b) to check that $L \cap L' = k$, $[L : k] = 3 = [L' : k] = 2$, but $[L \cdot L' : k] < 9$.

(e) $L \cdot L'$ is algebraic over k if and only if both $L|k$ and $L'|k$ are algebraic.

Below one can see some supplements to the results proved in the class.

Supplements

To understand and appreciate the Supplements which are marked with the symbol † one may possibly require more mathematical maturity than one has! These are steps towards applications to various other branches of mathematics, especially to Analysis, Number Theory and Algebraic Geometry.

T2.1 Let $K|k$ be a field extension and let $x \in K$.

(a) Let $\underline{x} \subseteq K$ be an arbitrary subset. Show that $y \in K$ is algebraic over $k(\underline{x})$ if and only if y is algebraic over $k(x_1,\ldots,x_n)$ for some $n \in \mathbb{N}^*$ and $x_1,\ldots,x_n \in \underline{x}$.

(b) Show that $K|k$ is algebraic if and only if every subring R of K with $k \subseteq R \subseteq K$ is a field.

(c) Let p be a prime number and let $x \in \mathbb{R}$ be the cube root $\sqrt[3]{p}$ of p (in $\mathbb{R}$), i. e. $x^3 = p$. If the subset $\{a+bx \mid a,b \in \mathbb{Q}\} \subseteq \mathbb{R}$ of R a subfield?

(d) Let $z \in \mathbb{C}$ be a square root of $2\mathrm{i}$. What is the degree of the field extension $\mathbb{Q}(z)|\mathbb{Q}$?

(e) If $[K:k] = p$ is a prime number, then show that there is no intermediate field between k and K.

(f) If $[K;k]$ is finite, then show that $\deg \mu_{x,k}$ divides $[K:k]$.

(g) If $x \in K$ is algebraic over k with $\deg \mu_{x,k}$ is odd, then show that $\deg \mu_{x^2,k}$ is also odd and $k(x) = k(x^2)$.

(h) If $x,y \in K$ are algebraic over k, then $[k(x,y):k] \leq \deg \mu_{x,k} \cdot \deg \mu_{y,k}$. Moreover, if $\mu_{x,k}$ and $\mu_{y,k}$ are relatively prime i. e., $\gcd(\mu_{x,k},\mu_{y,k}) = 1$, then the equality holds.

(i) Suppose that $K|k$ is finite of degree m and $f \in k[X]$ is an irreducible polynomial over k of degree n. If $\gcd(m,n) = 1$, then show that f is also irreducible over K.

T2.2 Show that every non-constant rational function $\varphi \in k(X_1,\ldots,X_n)$ is transcendental over k. (**Remark :** It follows that k is algebraically closed in every rational function field over k.)

T2.3 Show that the $\mathbb{Q}$-vector spaces $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are isomorphic, but they are not isomorphic as fields. See also Exercise 2.2-(b), (c).

T2.4 Let $Q(X)$ be the rational functions field in one indeterminate X over $\mathbb{Q}$ and let $L := \mathbb{Q}(X^2), L' := \mathbb{Q}(X^3)$ be two intermediary subfields of $\mathbb{Q}(X)|\mathbb{Q}$. Determine the Galois groups $\mathrm{Gal}\,(\mathbb{Q}(X)|L)$ and $\mathrm{Gal}\,(\mathbb{Q}(X)|L')$.

T2.5 (Regular representation of a finite field extension) Let $K|k$ be a finite field extension. and let $x \in K$. Let $\lambda_x : K \to K$, $y \mapsto x \cdot y$ be the left-multiplication by x. Then λ_x is a k-endomorphism of the k-vector space K. Further,

(a) The map $\lambda : K \to \mathrm{End}_k K$ defined by $x \mapsto \lambda_x$ is an injective ring homomorphism. This ring homomorphism λ is called the regular representation of $K|k$, i. e. $\mu_{\lambda_x,k} = \mu_{x,k}$.

(b) The minimal polynomial μ_{λ_x} of $\lambda_x \in \mathrm{End}_k K$ is the minimal polynomial of the (algebraic) element $x \in K$ over k.

(c) Let $\chi_x \in k[X]$ denote the characteristic polynomial of λ_x. Show that $\chi_x(x) = 0$, in particular, $\chi_x \in \mathrm{Ker}\,\Phi_x$, where $\Phi_x : k[X] \to K$ is the substitution homomorphism. Therefore, this polynomial is also known as the characteristic polynomial of x over k.

(d) Let $x_1,\ldots,x_n \in K$ be a basis of K over k and let $x \cdot x_j = \sum_{i=1}^n a_{ij}x_i$, $j = 1,\ldots,n$; $a_{ij} \in k$. Then $\chi_x = \mathrm{Det}\,(X\,\mathfrak{E}_n - \mathfrak{A})$, where $\mathfrak{E}_n$ denote the identity matrix in $\mathrm{M}_n(k)$ and $\mathfrak{A} := \left(a_{ij}\right)_{1\leq i,j\leq n} \in \mathrm{M}_n(k)$ is the matrix of λ_x with respect to the basis $x_1,\ldots,x_n$.

(e) If $K = k(x)$, then $\chi_x = \mu_{x,k}$. More generally, if $[K:k(x)] = m$, then $\chi_{x,k} = \mu_{x,k}^m$.

(f) (Trace and Norm) Let $\mathrm{Tr}_{K|k}(x) := \mathrm{Tr}(\lambda_x)$ and $\mathrm{N}_{K|k}(x) := \mathrm{Det}\,\lambda_x$. The maps $\mathrm{Tr} : K \to k$ $\mathrm{N}_{K|k} : K \to k$ are called the trace and norm of the finite field extension $K|k$. In the situation of the part (c), we have

$$\mathrm{Tr}_{K|k}(x) = \sum_{i=1}^n a_{ii} \quad \text{and} \quad \mathrm{N}_{K|k}(x) = \mathrm{Det}\left(a_{ij}\right)_{1\leq i,j\leq n}.$$

(g) $\mathrm{Tr} : K \to k$ is k-linear and $\mathrm{N}_{K|k} : K \to k$ is multiplicative, i. e. $\mathrm{N}_{K|k}(x \cdot y) = \mathrm{N}_{K|k}(x) \cdot \mathrm{N}_{K|k}(y)$ for all $x, y \in K$. Further, $\mathrm{Tr}_{K|k}(a) = [K : k] \cdot a$ and $\mathrm{Nr}_{K|k}(a) = a^{[K:k]}$ for every $a \in k$.

(h) If $\chi_x = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0, n := [K : k]$, then $\mathrm{Tr}_{K|k}(x) = -a_{n-1}$ and $\mathrm{N}_{K|k}(x) = (1)^n a_0$.

(i) If $\mu_{x,k} = X^r + b_{r-1}X^{r-1} + \cdots + b_1 X + b_0, r := [k(x) : k]$ and if $[K : k(x)] = m$, then $\mathrm{Tr}_{K|k}(x) = -m \cdot b_{r-1}$ and $\mathrm{N}_{K|k}(x) = (1)^n b_0^m$.

(j) For the field extension $K := \mathbb{Q}(\sqrt{d})|\mathbb{Q}$ with $q \in \mathbb{Q}$ and the element $x := a + b\sqrt{d} \in K$, $a, b \in \mathbb{Q}$, compute $\chi_{x,\mathbb{Q}}$, $\mu_{x,\mathbb{Q}}$, $\mathrm{Tr}_{K|\mathbb{Q}}(x)$ and $\mathrm{N}_{K|\mathbb{Q}}$ as functions of a and b.

†**T2.6** (D e d e k i n d[1]) In this we give generalization of the Exercise 2.1-(c): Let $f, g \in k[X]$ be polynomials both without multiple zeroes (in an algebraic closure of k) and let $L = k(x)$ and $M = k(y)$ with $f(x) = 0$ and $g(y) = 0$. Show that if $f = f_1 \cdot \cdots \cdot f_r$ and $g = g_1 \cdot \cdots \cdot g_r$ are prime factorizations of f over $k(y)$ and of g over $k(x)$, then $r = s$ and there are (after reordering) isomorphisms $k(y)[X]/(f_i) \xrightarrow{\sim} k(x)[X]/(g_i)$, in particular, $[k(y) : k] \cdot \deg f_i = [k(x) : k] \cdot \deg g_i$ for all $i = 1, \ldots, r$. (**Hint :**)

†**T2.7** Let L be an intermediary subfield of the field extension $k(X)|k$ with $k \neq L$. Then we have seen in Exercise 2.6-(b) that $k(X)|L$ is finite. Further,

(a) Let

$$\mu_{X,L} := Y^n + t_{n-1}(X)Y^{n-1} + \cdots + t_1(X)Y + t_0(X) \in L[Y]$$

be the minimal polynomial of X over L. Multiplying $\mu_{X,L}$ by a polynomial in $k[X]$, we get a polynomial

$$F(X,Y) = c_n(X)Y^n + c_{n-1}(X)Y^{n-1} + \cdots + c_1(X)Y + c_0(X) \in k[X][Y]$$

which is primitive over $k[X]$, i. e. $\mathrm{GCD}\,(c_n(X), \ldots, c_0(X)) = 1$.

(b) Let $\varphi \in L \setminus k$, $\varphi = f/g$ with relatively prime $f, g \in k[X]$. Show that the polynomial $F(X,Y)$ in the part (a) divides $g(X)f(Y) - f(X)g(Y)$ in $k[X][Y]$ and hence using Exercise 2.6-(a) deduce that

$$\deg_X F(X,Y) \leq [k(X) : k(\varphi)].$$

Moreover, if $\deg f, \deg g \leq \deg_X F(X,Y)$, then deduce that

$$g(X)f(Y) - f(X)g(Y) = aF(X,Y) \quad \text{for some} \quad a \in k^\times \quad \text{and hence} \quad L = k(\varphi).$$

(c) (L ü r o t h) Using the part (b) above show that $L|k$ is purely transcendental, i. e. L it self is a field of rational functions in one indeterminate over k. (**Hint :** At least one of $t_i := t_i(X) \notin k$ and for each of such we have $L = k(t_i)$. – **Remarks:** Lüroth proved this Theorem in 1876. It led to the following rationality problem: If L is an intermediate subfield of $k(X_1, \ldots, X_n)|k$ with transcendence degree n, is $L|k$ is rational, i. e. is L a purely transcendental extension of k?. In 1893 Castelnuovo proved that this is true for $n = 2$ if k is algebraically closed. It was not until early 1970s, an example of an intermediate subfield of $\mathbb{C}(X,Y,Z)|\mathbb{C}$ that is not rational over $\mathbb{C}$ was found.

A natural question is to ask what geometric information about a variety can be determined from the field theoretic information about its function field.

A fundamental problem is Algebraic geometry is to determine when an algebraic variety V over a field k is *rational*, i. e. the function field $k(V)$ of V is purely transcendental over k. We know from elementary calculus that a curve in the real plane $\mathbb{R}^2$ can be parameterized in the form $x = f(t)$ and $y = g(t)$ where f and g are real valued functions; i. e. the curve consists of the points $\{(f(t), g(t)) \in \mathbb{R}^2 \mid t \in \mathbb{R}\}$. For example, the unit circle is parameterized by $x = \cos t$ and $y = \sin t$. In the case of algebraic varieties, we are interested in parameterizations involving polynomial or rational functions.

[1] Incidently, it was Dedekind who baptized what we know as fields – with German word *Körper* which literally mean "body".

The problem of rationality has a more geometric formulation. To relate the concept of parametrization to that of rationality, first make the concept of parametrization precise, we restrict ro the case of algebraic curves; an algebraic variety of dimension 1 is said to be a c u r v e. An algebraic curve $\mathscr{C} \subseteq \mathbb{A}^n_{\bar{k}}$ defined over a field k, where $\mathbb{A}^n_{\bar{k}}$ denote the affine n-space over the algebraic closure $\bar{k}$ of k, is said to be p a r a m e t e r i z e d if there are rational functions $f_1, \ldots, f_n \in k(t)$ such that $\{(f_1(t), \ldots, f_n(t)) \in \mathbb{A}^n_k \mid t \in \bar{k}\}$ is a dense subset of $\mathscr{C}$ in the k-Zariski topology of $\mathscr{C}$.

For example, the unit circle $\mathrm{S}^1 = \{(x,y) \in \mathbb{R}^2 \mid x^2+y^2 = 1\}$ is parameterized by $x = (1-t^2)/(1+t^2)$ and $y = 2t/(1+t^2)$; an easy calculation show that $\{\big((1-t^2)/(1+t^2), 2t/(1+t^2)\big) \mid t \in \mathbb{C}, t^2 \neq -1\} = \mathrm{S}^1 \setminus \{(-1,0)\}$. Intuitively, $t = \infty$ is needed to get $x = -1$ and $y = 0$.

Lüroth's Theorem proves that : *An irreducible algebraic curve $\mathscr{C}$ defined over a field k can be parameterized if and only if the function field $k(\mathscr{C})$ is rational over k.*

Some examples:

(a) The algebraic curve $\mathscr{C} : x^2+y^2+1 = 0 \ := \{(x,y) \in \mathbb{C}^2 \mid x^2+y^2+1 = 0\}$ is defined over $\mathbb{R}$ as well as over $\mathbb{C}$. The function field $\mathbb{K}(\mathscr{C})$ of $\mathscr{C}|$, over $\mathbb{K}$ is isomorphic to $\mathbb{K}(t)(\sqrt{1-t^2})$, where $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$. Therefore $\mathbb{R}(\mathscr{C})$ is not rational over $\mathbb{R}$, but $\mathbb{C}(\mathscr{C})$ is rational over $\mathbb{C}$. Find a parametrization of $\mathscr{C}$ over $\mathbb{C}$. Further, $\mathscr{C}$ has no parametrization over $\mathbb{R}$; this can also be directly proved by showing that $\mathscr{C}$ has no $\mathbb{R}$-rational points, i. e. points $(a,b) \in \mathbb{R}^2$ with $(a,b) \in \mathscr{C}$.

(b) Let k be a field of characteristic $\neq 2$ and let $a, b \in k^\times$. Let $\mathscr{C}' : ax^2+by^2-1 = 0 \ := \{(x,y) \in \bar{k}^2 \mid ax^2+by^2-1 = 0\}$. Show that $k(\mathscr{C}')$ is rational over k if and only if $\mathscr{C}'$ has a k-rational point. Note that the example in (a) is a special case of this.

(c) Let $\mathscr{C} \subseteq \mathbb{C}^2$ be an irreducible non-singular algebraic curve over $\mathbb{C}$. If $\mathscr{C}$ is rational over $\mathbb{C}$, then the coordinate ring $\mathbb{C}[\mathscr{C}]$ is not a factorial domain. We shall use this result to show that the elliptic curve $\mathscr{E} : y^2 - x^3 + x = 0$. is not rational over $\mathbb{C}$ by verifying the following steps: Let $K := \mathbb{C}(\mathscr{E})$.

(i) The field extension $K|\mathbb{C}(X)$ has degree 2. If $\sigma \in \mathrm{Gal}\,(K|\mathbb{C}(X))$ is a non-identity, then $\sigma(y) = -y$ and hence $\sigma(\mathbb{C}[\mathscr{E}]) \subseteq \mathbb{C}[\mathscr{E}]$.

(ii) $\mathrm{N}_{K|\mathbb{C}(X)}(f) \in \mathbb{C}[X]$ for every $f \in \mathbb{C}[\mathscr{E}]$, where $\mathrm{N}_{K|\mathbb{C}(X)} : K \to \mathbb{C}(X)$ is the norm map.

(iii) $\mathbb{C}[\mathscr{E}]^\times = \mathbb{C}^\times$. (**Hint :** Use the above part (ii).) Show that $x, y \in \mathbb{C}[\mathscr{E}]$ are irreducible elements in $\mathbb{C}[\mathscr{E}]$ and $y^2 = x(1-x)$ are two different irreducible factorizations in $\mathbb{C}[\mathscr{E}]$.)