Dec. 29, 2006

The following theorem says that finitely generated purely transcendental extension are just rational function fields.

Theorem 3.14.4. *If $\{s_1, ..., s_n\} \subset F$ is algebraically independent over K. Then $K(s_1, ..., s_n) \cong K(x_1, ..., x_n)$.*

Proof. We consider the homomorphism $\theta : K[x_1, ..., x_n] \to K[s_1, ..., s_n]$. θ is surjective by definition. It's injective because $\{s_1, ..., s_n\} \subset F$ is algebraically independent. Then θ induces an isomorphism on quotient fields. □

One notices that the notion of being algebraic independent is an analogue of being linearly independent. Therefore, one can try to define the notion of "basis" and "dimension" in a similar way.

Definition 3.14.5. *$S \subset F$ is said to be a transcendental basis of F/K if S is a maximal algebraically independent set. In other words, for all $u \in F - S$, $S \cup \{u\}$ is algebraically dependent.*

We will then define the *transcendental degree* to be the cardinality of a transcendental basis (in a analogue of dimension). In order to show that this is well-defined. We need to work harder.

Proposition 3.14.6. *Let $S \subset F$ be an algebraically independent set over K and $u \in F - K(S)$. Then $S \cup \{u\}$ is algebraically independent if and only if u is transcendental over $K(S)$.*

Proof. The proof is straightforward. □

Corollary 3.14.7. *S is a transcendental basis of F/K if and only if $F/K(S)$ is algebraic.*

Proof. Suppose that S is a transcendental basis of F/K. If $u \in F - K(S)$, then $S \cup \{u\}$ is not algebraically independent. Thus, u is algebraic over $K(S)$ by the Proposition.

On the other hand, suppose that $F/K(S)$ is algebraic. Then for all $u \in F - S$, u is algebraic over $K(S)$. By the Proposition, $S \cup \{u\}$ is algebraically dependent if $u \in F - K(S)$. In fact, it's easy to see directly that $S \cup \{u\}$ is algebraically dependent if $u \in K(S)$. Thus S is a maximal algebraically independent set. □

Corollary 3.14.8. *Let $S \subset F$ be an subset over such that $F/K(S)$ is algebraic. Then S contains a transcendental basis.*

Proof. By Zorn's Lemma, there exists a maximal algebraically independent subset $S' \subset S$. Then $K(S)$ is algebraic over $K(S')$ and hence F is algebraic over $K(S')$. □

Theorem 3.14.9. *Let S, T be transcendental bases of F/K. If S is finite, then $|T| = |S|$.*

Proof. Let $S = \{s_1, ..., s_n\}$ and $S' := \{s_2, ..., s_n\}$. We first claim that there is an element $t \in T$, say $t = t_1$ such that $\{t_1, s_2, ..., s_n\}$ is a transcendental basis.

to see this, if every element of T is algebraic over $K(S')$, then F is algebraic over $K(T)$ hence over $K(S')$ which is a contradiction. Thus, there is an element $t \in T$, say $t = t_1$ such that t_1 is transcendental over $K(S')$. And hence $T' := \{t_1, s_2, ..., s_n\}$ is algebraically independent.

By the maximality of S, one sees that s_1 is algebraic over $K(T')$. It follows that F is algebraic over $K(t_1, s_1, ..., s_n)$ and hence algebraic over $K(T')$. Therefore, T' is a transcendental basis.

By induction, one sees that there is a transcendental basis $\{t_1, ..., t_n\} \subset T$. Thus $T = \{t_1, ..., t_n\}$. □

Theorem 3.14.10. *Let S,T be transcendental bases of F/K. If S is infinite, then $|T| = |S|$.*

Proof. By the previous theorem, we may assume that T is infinite as well.

For $s \in S$, we have $s \in F$ hence algebraic over $K(T)$. Let $T_s \subset T$ be the subset of T of elements that appearing in the minimal polynomial of s. It's clear that $T_s \neq \emptyset$ otherwise, s is algebraic K which is not the case. Also note that T_s is finite.

Let $T' := \cup_{s\in S} T_s$. We claim that $T' = T$. To this end, one sees that for $u \in F$, u is algebraic over $K(S)$ and hence algebraic over $K(T')$. Thus $F/K(T')$ is algebraic. T is a transcendental basis, hence $T = T'$.

Lastly, one sees that

$$|T| = |T'| = | \cup_{s\in S} T_s| \leq |S| \cdot \aleph_0 = |S|.$$

Replace S by T, one has $|S| \leq |T|$. We are done. □

With these two theorem, we can define the transcendental degree of an extension. And the definition is independent of choices of basis.

Definition 3.14.11. *Let F/K be an extension and S be a transcendental basis. We define the transcendental degree of F/K, denoted* $\mathrm{tr.d.}F/K$*, to be $|S|$.*

Theorem 3.14.12. *Let F/E and E/K be extensions. Then*

$$\mathrm{tr.d.}F/K = \mathrm{tr.d.}F/E + \mathrm{tr.d.}E/K.$$

Proof. Let T be a transcendental basis of F/E and S be a transcendental basis of E/K. We would like to show that $S \cup T$ is a transcendental basis of F/K. Note that $T \cap E = \emptyset$, hence $S \cap T = \emptyset$. Thus $|S \cup T| = |S| + |T|$, and we are done.

To see the claim, it's easy to check that $E(T) = EK(S \cup T)$. Hence $E(T)/K(S \cup T)$ is algebraic if $E/K(S)$ is algebraic. Also, $F/E(T)$ is algebraic, therefore, $F/K(S \cup T)$ is algebraic.

It suffices to show that $S \cup T$ is algebraically independent. Suppose that there is $f(x_1, ..., x_n, y_1, ..., y_m)$ such that $f(s_1, ..., s_n, t_1, ..., t_m) = 0$. We can write

$$f(x_1, ..., x_n, y_1, ..., y_m) = \sum_I h_I(x_1, ..., x_n) y^I,$$

and we have $\sum_I h_I(s_1, ..., s_n) t^I$. Since T is algebraically independent over $E \ni h_I(s_1, ..., s_n)$. It follows that $h_I(s_1, ..., s_n) = 0$ for all I. Since S is algebraically independent over K, if follows that $h_I(x_1, ..., x_n) = 0 \in K[x_1, ..., x_n]$ for all I. Therefore $f(x_1, ..., x_n, y_1, ..., y_m) = 0$. Hence $S \cup T$ is algebraically independent. $\square$

Example 3.14.13.

Let $V := \{(a, b) | a^3 = b^2, a, b \in K\}$. Then "polynomial function on V can be described as $R := K[x, y]/(y^2 - x^3)$. And rational functions on V is nothing but the field of quotient of R, denoted F. Then $\text{tr.d.}_K F = 1$, which is the same as the "dimension of V". $\square$

Some related problems:
1. Lüroth's theorem and rationality problem.
The Lüroth's theorem states that a non-trivial subfield of $k(x)$ is of the form $k(t)$, where $t \in K(x)$. More generally, one can ask a subfield $E \subset K(x, y)$ of $\text{tr.d}_\text{K} = 2$ is purely transcendental or not. One can prove that this is true when $K = \mathbb{C}$ by geometric method. However, this is not true in general when transcendental degree is higher.

Nevertheless, suppose that there is a finite group G acts on $k(x_1, ..., x_n)$. One can ask whether the subfield of invariant purely transcendental or not. Or under what condition, the field of invariant is purely transcendental. A variety (as V above) is called **rational** if its rational function field is purely transcendental. So this is called **rationality problem**.
2. Automorphism of function fields.
Consider $F = K(x)$. It's well-known that $\text{Aut}_K(F) = PGL(2, K)$. How about K-automorphism $F = K(x_1, ..., x_n)$?
3. Characterize birational invariants.
Varieties as said to be birational if their function fields are isomorphic. Therefore, those birational invariant, which reflect the birational geometry of varieties, are invariant of fields. Can you read it from the fields?

4. Homological Algebra

Some useful references:
Serge Lang,*Algebra*, GTM 211, Springer
S. Gelfand, Y. Manin, *Methods of homological algebra*, Springer
David Eisenbud, *Commutative algebra*, GTM 150, Springer

4.1. categories and functors.

In this section, we are going to define some basic notions.

Definition 4.1.1. *A* **category** *is a class* $\mathcal{C}$ *of objects, denoted* $A, B, C, ...,$ *etc., together with*

(1) *a class of disjoint set, denoted* $\mathrm{Hom}_{\mathcal{C}}(A, B)$*, called* **morphism** *and*
(2) *for each triple* (A, B, C) *of objects a function* $Hom(B, C) \times \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C)$*, called the* **composition** *subjects to*
   (a) $h \circ (g \circ f) = (h \circ g) \circ f$.
   (b) *for each object* $A \in \mathcal{C}$*, there exists* $\mathbf{1}_A \in \mathrm{Hom}(A, A)$ *such that* $\mathbf{1}_A \circ f = f, f \circ \mathbf{1}_A = f$.

Example 4.1.2.

(1) The category of Sets, denoted *Set*.
(2) The category of groups, denoted *Gp*, is a subcategory of *Set*.
(3) The category of abelian groups, denoted *Ab*, is a subcategory of *Gp*.

Definition 4.1.3. *Let* $\mathcal{C}, \mathcal{D}$ *be categories. A covariant functor (resp. contravariant functor)* F *of* $\mathcal{C}$ *to* $\mathcal{D}$ *is a rule which to each object* $A \in \mathcal{C}$ *associate an object* $F(A) \in \mathcal{D}$*, and to each morphism* $f : A \to B$ *associate a morphism* $F(f) : F(A) \to F(B)$ *(resp.* $F(f) : F(B) \to F(A)$*) such that:*

(1) $F(\mathbf{1}_A) = \mathbf{1}_{F(A)}$.
(2) $F(g \circ f) = F(g) \circ F(f)$ *(resp.* $F(g \circ f) = F(f) \circ F(g)$*).*

There are many cases we met the *universal property*. This can be seen via the universal object in a suitable category.

Definition 4.1.4. *In a category* $\mathcal{C}$*, an object* P *is said to be universally attracting (resp. repelling) if* $\mathrm{Hom}(A, P)$ *(resp.* $\mathrm{Hom}(P, A)$*) has only one element for all* $A \in \mathcal{C}$.

Example 4.1.5.

The group of one element is the universally repelling and attracting object in *Gp*.

Example 4.1.6.

Fixed a set S. Let $\mathcal{C}$ be the category of maps form S to abelian groups. The free abelian group is the universally repelling object.

Similarly, if we consider the category of maps from S to groups. Then we get free group by considering the universal repelling object. □

Example 4.1.7.

In a category $\mathcal{C}$, the product of A, B can be defined as (P, f, g) consisting of an object P and $f : P \to A$, $g : P \to B$ such that for any (C, s, t), there exist a unique $h : C \to P$, which makes the diagram commute.

In other words, let $\mathcal{D}$ be the category of the triple (C, s, t), then P is nothing but the universal attracting object. □

We now formulate the axioms of **additive category** and **abelian category**.

A1. $\mathrm{Hom}(A, B)$ is an abelian group. And composition is bilinear.

A2. There exist a zero object 0, i.e. such that $\mathrm{Hom}(0, A), \mathrm{Hom}(A, 0)$ has precisely one element.

A3. Finite direct sum and finite direct product exist. In other words, for $A_1, A_2 \in \mathcal{C}$, there exist an object $C \in \mathcal{C}$ and $p_i : C \to A_i$, $\imath_i : A_i \to C$ such that $p_i \imath_i = \mathbf{1}_{A_i}$, $p_i \imath_j = 0$ if $i \neq j$, $\imath_1 p_1 + \imath_2 p_2 = \mathbf{1}_C$.

A4. For any morphism $f : A \to B$, there exist a sequence, called a *canonical decomposition*

$$K \xrightarrow{k} A \xrightarrow{\imath} I \xrightarrow{\jmath} B \xrightarrow{c} K'$$

such that

(1) $\jmath \circ \imath = f$
(2) K is the kernel of f and K' is the cokernel of f.
(3) I is cokernel of k and kernel of c.

In the above canonical decomposition, K can be viewed as kernel, I as the image and K' as the cokernel.

Definition 4.1.8. *A category satisfying* $A1, A2, A3$ *is called an additive category. An additive category satisfying* $A4$ *is called an abelian category.*

Remark 4.1.9. *The kernel and cokernel should be defined abstractly. For example, given* $A \in \mathcal{C}$*, one can define a functor* $h_A : \mathcal{C}^\circ \to Set$ *such that* $h_A(C) = \mathrm{Hom}(C, A)$*. A functor* F *is* **representable** *by* B *is* $F \cong h_B$*.*

In an additive categoty $\mathcal{C}$*, for a morphism* $f : A \to B$*, one can define a kernel functor* $Ker(f) : \mathcal{C}^\circ \to Ab$ *such that* $Ker(f)(C) = Ker(h_A(C) \to h_B(C))$*.*

We say that kernel of f *exists if the functor* $Ker(f)$ *is representable.*

Cokernel can be defined similarly but a little bit subtle. It's $ker(f^\circ)^\circ$*.*

Example 4.1.10.

The followings are abelian categories:

(1) *Ab*.
(2) category of R-modules, where R is a ring.
(3) category of finite dimensional vector space over k.
(4) category of sheaves of abelian groups over a topological space.

□

4.2. **complexes, examples of homology and cohomology groups.** There are various situation where we need to consider a sequence of abelian group. This is basically why homological algebra arise.

Definition 4.2.1. *Let $\mathcal{A}$ be an abelian category. A comlpex $K^\bullet = (K^i, d_i)_{i\in\mathbb{Z}}$ consists of $K^i \in \mathcal{A}$, $d^i : K^i \to K^{i+1}$ such that $d^{i+1}d^i = 0$ for all i.*

A complex is said to be exact if $\ker(d^{i+1}) = \mathrm{im}(d^i)$.

Example 4.2.2 (Homology of simplicial complex)**.**

Given a simplicial complex X, we can view it as $\cup X_n$, where X_n denotes the n-skeleton. To each n, we attach a free abelian C_n on n-simlpex. Note that there is a natural *boundary map* ∂_n from a n-complex to $(n-1)-$ complex. Note that one need to handle signs by considering the orientation. It follows that $\partial \circ \partial = 0$. Hence we have a complex of free abelian groups (C_n, ∂).

The homology can be considered as the obstruction of this complex being exactness. That is, $H_i(X, \mathbb{Z}) := \ker(\partial_n)/\mathrm{im}(\partial_{n-1})$.

For example, the homology of S^2 can be realized by

$$0 \to \mathbb{Z}[f] \to \mathbb{Z}[e_1] \oplus \mathbb{Z}[e_2] \to \mathbb{Z}[x_1] \oplus \mathbb{Z}[x_2] \oplus \mathbb{Z}[x_3] \to 0.$$

And $\partial[f] = [e_1] + [e_2] - [e_2] - [e_1], \partial[e_1] = [x_2] - [x_1], \partial[e_2] = [x_3] - [x_2], \partial[x_i] = 0$. Therefore, $H_2(S^2) \cong \mathbb{Z}$, $H_1 \cong 0$, $H_0 \cong \mathbb{Z}$. □

Exercise 4.2.3. *compute the homology of $S^n, \mathbb{RP}^2, T^2$ and Klein bottle.*

Example 4.2.4.

[differential forms, De Rham complex and cohomology] Let X be a differentiable manifold, e.g $\mathbb{R}^n$. Let C^i be the vector space of $\mathcal{C}^\infty$ i-forms on X. There is the natural differential $d : C^i \to C^{i+1}$. Then we have a complex (C^i, d), called the de Rham complex. Similarly, we have de Rham cohomology $H^i := \ker(d^i)/\mathrm{im}(d^{i-1})$. □

Example 4.2.5 (Koszul complex, free resolution)**.**

Given a ring $R = k[x, y, z, w]/(xz - y^2, xw - yz, yw - z^2)$. How can we realize it via describing generators and relations?

Let $S = k[x, y, x]$, then there is an exact sequence

$$0 \to \oplus S^2 \to \oplus^3 S \overset{(xz-y^2, xw-yz, yw-z^2)}{\longrightarrow} S \to R \to 0.$$

So the ring R can be realized as the complex of free modules. This is an example of so-called *free-resolution*. $\square$

What we would like to do is more or less the algebraic structure needed for this kind of situation.