Lecture 16

Noncentral Case

(for those familiar with Field Theory).

Proposition. (1) Let K/F be a Galois extension, $|K:F|=n$. Then

$$K\otimes_F K \cong \underbrace{K\oplus\cdots\oplus K}_{n}$$

(2) If char $F=p>0$, K/F is a purely unseparable extension then

$$K\otimes_F K/\mathrm{Rad}(K\otimes_F K)\cong K.$$

In particular, if K/F is an extension that is not separable, then $K\otimes_F K$ contains nonzero nilpotent elements.

Proof. Let $G=\{\sigma_1=\mathrm{Id},\sigma_2,\dots,\sigma_n\}$ be the Galois group $Gal(K/F)$. For each automorphism σ_i the mapping $K \times K \to K$, $a \times b \to a^{\sigma_i} b$ is F-bilinear (and therefore F-balanced). Hence there exists a homomorphism of F-algebras

$$\chi_i : K \otimes_F K \to K, \quad a \otimes b \to a^{\sigma_i} b.$$

Consider the homomorphism

$$\chi : K \otimes_F K \to \underbrace{K \oplus \cdots \oplus K}_{n}, \quad \chi(a \otimes b) = \chi_1(a \otimes b) \oplus \cdots$$

$$\cdots \chi_n(a \otimes b) = (a^{\sigma_1} b, a^{\sigma_2} b, \ldots, a^{\sigma_n} b).$$

Let us show that $\ker \chi = (0)$.

Let $\sum_{i=1}^{n} a_i \otimes b_i \in \ker \chi$, the elements $a_1, \ldots, a_n$ are linearly independent over F.

Then $\sum_{i=1}^{n} a_i^{\sigma} b_i = 0$ for all automorphisms $\sigma \in G$.

Viewing these n equalities as a system of linear equations with variables $b_1, \dots, b_n$ we get

$$\det \left| a_i^{\sigma_j} \right|_{1 \le i,j \le n} = 0$$

It means that the columns in this matrix are linearly dependent, i.e. there exist $k_1, \dots, k_n \in K$, not all equal to 0, such that

$$k_1 a_i^{\sigma_1} + k_2 a_i^{\sigma_2} + \dots + k_n a_i^{\sigma_n} = 0$$

for every $i = 1, 2, \dots, n$.

Since $a_1, \dots, a_n$ is a basis of K over F it follows that for an arbitrary element $a \in K$

$$k_1 a^{\sigma_1} + \cdots + k_n a^{\sigma_n} = 0,$$

in other words $k_1 \sigma_1 + \cdots + k_n \sigma_n = 0$.

This contradicts <u>Artin's Theorem</u> on linear independence of automorphisms in Galois groups.

We proved that χ is an embedding of algebras. Computing dimensions of $K \otimes_F K$ and $\underbrace{K \oplus \cdots \oplus K}_{n}$ we see that χ is an isomorphism. This completes the proof of the part (1).

Suppose now that the extension K/F is purely inseparable. It means that char $F = p > 0$ and for an arbitrary element $a \in K$ there exists a p-power p^k such that $a^{p^k} = \alpha \in F$. Now,

$$(a \otimes 1 - 1 \otimes a)^{p^k} = a^{p^k} \otimes 1 - 1 \otimes a^{p^k} = \alpha \otimes 1 - 1 \otimes \alpha = 0.$$

Hence all elements $a \otimes 1 - 1 \otimes a$ lie in the radical $\mathrm{Rad}(K \otimes_F K)$ and therefore

$$K \otimes_F K = K \otimes 1 + \mathrm{Rad}(K \otimes_F K),$$

$$K \otimes_F K / \mathrm{Rad}(K \otimes_F K) \cong K.$$

This argument also shows that if the extension K/F is not separable then $K \otimes_F K$ contains a nonzero nilpotent element $a \otimes 1 - 1 \otimes a$, $a \in K$.

Fractions.

How do we get rational numbers from integers?

We consider formal pairs $\frac{a}{b}$; $a, b \in \mathbb{Z}$, $b \neq 0$

Then we introduce equivalence

$$\frac{a}{b} \sim \frac{c}{d} \text{ if } ad = bc.$$

classes of equivalence $= \mathbb{Q}$.

Our aim: extend this result to noncommutative rings.

An ~~elet~~ element $0 \neq a \in R$ is called regular if it is not a zero divisor,

$ab = 0 \iff b = 0$, $ba = 0 \iff b = 0$.

Let $S \subset R$ be a multiplicative subsemigroup of R (so $a, b \in S \Rightarrow ab \in S$) that consists of regular elements.

<u>Def.</u> An overring $R \subseteq \tilde{R}$ is called a (left) <u>ring of fractions with respect to S</u> if

(1) all elements from S are invertible in $\tilde{R}$,

(2) an arbitrary element $x \in \tilde{R}$ can be represented as $x = s^{-1}a$, $s \in S$, $a \in R$.

<u>Ore Condition:</u> for arbitrary elements $s \in S, a \in R$ there exist elements $s_1 \in S, a_1 \in R$

such that $s_1 a = a_1 s$.

<u>Theorem</u>. A ring of fractions of R with respect to S exists if and only if the Ore Condition is satisfied.

<u>P.S.</u> If a ring of fractions exists then it is unique.

<u>Proof</u>. Suppose that a ring of fractions $\tilde{R}$ exists. An arbitrary element from S is invertible in $\tilde{R}$ and an arbitrary element of $\tilde{R}$ can be represented as $s^{-1}a$.

Choose $s \in S$ and $a \in R$. Then there exist elements $s_1 \in S$, $a_1 \in R$ such that

$as^{-1} = s_1^{-1}a_1$. Multiplying this equality on the left by s_1 and on the right by s, we get $s_1 a = a_1 s$.

Now suppose that the Ore Condition holds. Let us show that it is sufficient to embed the ring R in a ring $\tilde{R}$, where all elements from S are invertible. Let $\tilde{R}$ be such a ring. Consider the subring generated by $S^{-1} = \{s^{-1} \mid s \in S\}$ and R. In order to represent an arbitrary element of this subring as $s^{-1}a$, $a \in R$, it suffices to represent an arbitrary element as^{-1} in this form. Let

$s_1 a = a_1 s$; $s_1 \in S$, $a_1 \in R$. Then

$a s^{-1} = s_1^{-1} a_1$.

Now our aim is to embed R in a ring $\tilde{R}$ where all elements from S are invertible.

We could try to immitate the construction of $\mathbb{Q}$: consider formal pairs (s, a) (having in mind $s^{-1}a$). The next step (equivalence!) would hit a bump because of noncommutativity.

Still we could do it (since the Ore condition looks like a "common denominator" condition), but it will be technical. We will go a different way.

Let $L \triangleleft_e R$ be a left ideal. For an element $a \in R$ we define

$$La^{-1} = \{x \in R \mid xa \in L\}.$$

This is again a left ideal. An element a does not need to be invertible, for example

$$L0^{-1} = R.$$

<u>Def.</u> A left ideal $L \triangleleft_e R$ is called <u>dense</u> if $\forall a \in R$ the right annihilator of La^{-1} is (0), i.e.

$$x \in R,\ (La^{-1})x = (0) \Rightarrow x = 0.$$

This condition means that $\forall a \in R$ $\forall\, 0 \neq x \in R$ there exists an element $b \in R$ such that $ba \in L$, $bx \neq 0$.

In other words we can move one element to L without "killing" another (nonzero) element.

Notation: $L \triangleleft_e^{\text{dense}} R$.

<u>Lemma</u>: If $L_1 \triangleleft_e^{\text{dense}} R$, $L_2 \triangleleft_e^{\text{dense}} R$, then $L_1 \cap L_2 \triangleleft_e^{\text{dense}} R$.

<u>Proof</u>. Let $a \in R$, $x \neq 0$. There exists an element b_1 that moves a to L_1 and does not kill x: $b_1 a \in L_1$, $b_1 x \neq 0$.

Then there exists an element $b_2 \in R$: $b_2 b_1 a \in L_2$, $b_2 b_1 x \neq 0$. We have $(b_2 b_1) a \in L_1 \cap L_2$, $(b_2 b_1) x \neq 0$. This completes the proof of the lemma.

Every left ideal L can be viewed as a left R-module. Consider the set
$\widetilde{\widetilde{R}} = \{ R$-module homomorphisms ${}_R L \to {}_R R$, where $L \triangleleft_e^{dense} R \}$.

<u>Equivalence</u>. Let $\varphi : L_1 \to R$, $\psi : L_2 \to R$ be R-module homomorphisms; L_1 and L_2 are dense left ideals. We say that $\varphi \sim \psi$ if there exists a dense left ideal $L_3 \triangleleft_e^{dense}$, $L_3 \subseteq L_1 \cap L_2$, such that

$\varphi|_{L_3} = \psi|_{L_3}$.

<u>Exercise</u>. By Lemma this relation is transitive, hence an equivalence.

Let $\varphi : L_1 \to R$, $\psi : L_2 \to R$ lie in $\tilde{\tilde{R}}$.

<u>Addition</u>. Let

$$\varphi/\sim + \psi/\sim = (\varphi|_{L_1 \cap L_2} + \psi|_{L_1 \cap L_2})/\sim$$

It is easy to see that if $\varphi_1 \sim \varphi$, $\psi_1 \sim \psi$, then $\varphi_1 + \psi_1 \sim \varphi + \psi$, so the operation is well defined.

<u>Multiplication</u>. What is $\varphi\psi$?

The left ideal

$$L_3 = \{ a \in L_2 \mid \psi(a) \in L_1 \} = \psi^{-1}(L_1)$$

is dense. Indeed, choose $b \in R$, $0 \neq x \in R$. We need to find an element $c \in R$ such that $cb \in L_2$ and $\psi(cb) \in L_1$ and $cx \neq 0$.

First we find $c_1 : c_1 b \in L_2$, $c_1 x \neq 0$. Then we find $c_2 : c_2 \psi(c_1 b) \in L_1$, $c_2 (c_1 x) \neq 0$.

Then $c = c_2 c_1$ is the element that we have been looking for.

Then $\varphi\psi$ is defined on L_3 and we define

$$\varphi/_\sim \cdot \psi/_\sim = \varphi\psi\Big|_{L_3} /_\sim$$

It is straightforward that

$$\tilde{R} = \tilde{\tilde{R}} /_\sim$$

is a ring.

The ring R is embedded in $\tilde{R}^{op}$. Indeed, for an element $a \in R$ $R_a : R \to R,\ x \to xa,$ is a module homomorphism, $a \to R_a/\sim$ is an embedding into $R_{\tilde{R}} \cong \tilde{R}^{op}$.

Let us show that for an element $s \in S$ the right multiplication R_s is invertible. We notice that Rs is a dense left ideal. Indeed, for elements $a \in R$, $0 \neq x \in R$ there exist elements $a_1 \in R$, $s_1 \in S$ such that

$s_1 a = x_1 s \in Rs$. But $s_1 x \neq 0$ since the element s_1 is regular.

Consider the R-module homomorphism

$$R_{s^{-1}} : Rs \to R \quad , \quad xs \to x .$$

Then $R_{s^{-1}}/\sim$ is the inverse of $R_s/\sim$.

We showed that all elements from S are invertible in $\tilde{R}^{op}$. This completes the proof of the theorem.

Remark. Those who had a rigorous course of Analysis should compare this proof to Distributions, Sobolev Spaces etc. Like in Analysis instead of functions (rings) we considered functionals on functions (homomorphisms $\varphi: L \to R$).