(optional) 52

— Exercise V Prove that γ_u is A-bilinear, and the last sentence of the proof.

— — — — — — — to here 22.11 —

29.11.17

Thm Let B, C, D be A-rings, and let $g: B \to D$ and $h: C \to D$ be A-ring hom's. Then there's a unique A-ring hom.

$$g \otimes h : B \otimes_A C \to D$$

s.t.

$$(g \otimes h)(b \otimes c) = g(b) \cdot h(c) \qquad (*)$$

for all $b \in B$ and $c \in C$.

(pf. on p. 52)

Prop. In the situation of Thm. [p. 50], the functions

$$\begin{cases} B \to B \otimes_A C \\ b \mapsto b \otimes 1_C \end{cases} \quad \text{and} \quad \begin{cases} C \to B \otimes_A C \\ c \mapsto 1_B \otimes c \end{cases}$$

are A-ring hom's.

The proof is easy (opt. exercise)

in a comm. diag.

$$\begin{tikzcd}
 & A \arrow[dl] \arrow[dr] \arrow[d] & \\
B \arrow[r] \arrow[ddr, "g"'] & B \otimes_A C \arrow[dd, "g \otimes h"] & C \arrow[l] \arrow[ddl, "h"] \\
 & & \\
 & D &
\end{tikzcd}$$

<u>pf of thm</u>. Let $p: B \times C \to D$ be

$p(b,c) := g(b) \cdot h(c)$.

This is A-bilinear, so $\exists!$ A-lin. hom

$g \otimes h : B \otimes_A C \to D$, sats $(\dagger)$.

A calculation shows that $g \otimes h$ is an A-ring hom.

$\square$

§4

Exercise. Prove that there's a can. ring isom $A[t] \cong A \otimes_{\mathbb{Z}} \mathbb{Z}[t]$.
Here A is a ring and t is a variable.

Exercise Prove that

$$A[s,t] \cong A[s] \otimes_A A[t].$$

A is a ring and s,t are variables.

§3

Tensors and Galois Theory (mostly self-study)

Two thms we won't prove.

<u>Def.</u> A ring A is <u>reduced</u> if the only nilpotent element in it is 0.

<u>Exa.</u> $\mathbb{K}[\varepsilon] := \mathbb{K}[t]/(t^2)$ is not reduced.

<u>Thm.</u> Let $k \subseteq L$ be a finite field extension. TFAE:

(i) L is separable ext. of k.

(ii) For ~~any~~ every finite field ext. $k \subseteq k'$ the ring $k' \otimes_k L$ is reduced.

For a proof see Matsumura "Comm. Alg." Ch. 27.

→ <u>Exercise</u> ** (= hard)

Consider the field $K := \mathbb{K}(t)$, the field of rational functions in the variable t, over a field $\mathbb{K}$ of characteristic $p > 0$.

Let $L := K[s]/(s^p - t)$, with $u \in L$ the class of s.

Since the polynomial $s^p - t \in K[s]$

(5b)

is irreducible, L is a field. In L we have
$$u = \sqrt[p]{t}.$$
The extension $k \subseteq L$ is not separable.
Find a nonzero nilpotent element
$$\varepsilon \in L \otimes_k L.$$
[Hint: in char p, $(a+b)^p = a^p + b^p$.]

Suppose $k \subseteq L$ is a finite Galois field extension, with group G.
Consider the ring
$$L \times \cdots \times L = F(G, L)$$
of functions $\varphi : G \to L$. It has an action by G (permuting the source). There's a ring hom
$$\alpha : L \to F(G,L) \quad \text{the "const. functions"}$$
$$\alpha(a)(g) = a \qquad \forall a \in L,\ g \in G$$
and also
$$\beta : L \to F(G,L), \quad \beta(a)(g) = g(a).$$
α & β are k-ring homs so get ring hom
$$\boxed{\alpha \otimes \beta : L \otimes_k L \to F(G, L)}$$

Thm. $\alpha \otimes \beta$ is an isomorphism.

(proof: ? discussion in Milne's "Étale Cohomology")

→ Exercise ** Consider the Galois ext. $\mathbb{R} \subseteq \mathbb{C}$.

The group is $G = \{id, \sigma\}$ σ = conjugation.

So $F(G, \mathbb{C}) = \mathbb{C} \times \mathbb{C} \cong \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ by the theorem

- there are idempotents $e_1 = (1,0)$ $e_2 = (0,1)$

$e_1^2 = e_1$, $e_2^2 = e_2$ $e_1 + e_2 = 1$, $e_1 \cdot e_2 = 0$, $e_2 = (id \otimes \sigma)(e_1)$

Find the tensors e_1 and e_2, as elements of $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$.

Flatness

A is a comm. ring, Given a module M and an A-mod. hom $\psi : N_1 \to N_2$, there's an induced A-mod. hom

$$\boxed{id_M \otimes \psi : M \otimes_A N_1 \to M \otimes_A N_2.}$$

<u>Def</u> An A-module M is called <u>flat</u> if for every <u>injective</u> A-mod. hom.

$$\psi : N_1 \to N_2,$$

the hom.

$$id_M \otimes \psi : M \otimes_A N_1 \to M \otimes_A N_2$$

is also <u>injective</u>.

In terms of exact seq.: M is flat if for every ex. seq.

$$0 \to N_1 \xrightarrow{\psi} N_2$$

the seq.

$$0 \to M \otimes_A N_1 \xrightarrow{id \otimes \psi} M \otimes_A N_2$$

is also exact.

59

<u>Lem.</u> Suppose M is a free A-mod with basis $\underline{m} = \{m_i\}_{i\in I}$. For any A-mod N there's a unique A-mod. isomorphism

$$\Psi : M \otimes_A N \xrightarrow{\cong} F_{fin}(I, N)$$

s.t.

$$\Psi(m_i \otimes n)(j) = \begin{cases} n & \text{if } j = i \\ 0 & \text{o/w.} \end{cases}$$

using a bilinear function

Pf. Very similar to the pf. of Thm [p. 43], The inverse hom. Φ is

$$\Phi(v) := \sum_{i\in I} m_i \otimes v(i), \quad v \in F_{fin}(I, N).$$

The full details are an opt. exercise.

□

Thm. If M is a free A-module, then it is flat.

Pf. Let $\underline{m} = \{m_i\}_{i \in I}$ be a basis of M.
Given an injective A-mod. hom. $\varphi : N_1 \to N_2$ we look at this diagram

$$\begin{array}{ccc} M \otimes_A N_1 & \xrightarrow{id_M \otimes \varphi} & M \otimes_A N_2 \\ \Psi \downarrow \cong & & \cong \downarrow \Psi \\ F_{fin}(I, N_1) & \xrightarrow{\tilde{\varphi}} & F_{fin}(I, N_2) \end{array} \qquad (†)$$

lemma [p. 59]

where $\tilde{\varphi}(v) := \varphi \circ v$

The diag. (†) is commutative, since

$$\begin{array}{ccc} m_i \otimes n & \longmapsto & m_i \otimes \varphi(n) \\ \downarrow & & \downarrow \\ \boxed{\begin{cases} i \mapsto n \\ j \mapsto 0, & j \neq i \end{cases}} & \overset{\tilde{\varphi}}{\longmapsto} & \boxed{\begin{cases} i \mapsto \varphi(n) \\ j \mapsto 0 & j \neq i \end{cases}} \end{array}$$

It suffices to prove that $\tilde{\varphi}$ is injective. This is easy: if $v \neq 0$ then $v(i) \neq 0$ for some $i \in I$. Then, since φ is inj. we have

$$\underset{\tilde{\varphi}(v)(i)}{\underset{\parallel}{\varphi(v(i))}} \neq 0. \qquad \text{So} \quad \tilde{\varphi}(v) \neq 0.$$

$\square$

<u>Thm</u> Let M be a fin. gen. abelian group. TFAE:

(i) M is free

(ii) M is a flat $\mathbb{Z}$-module.

<u>pf.</u> We already know that (i) $\Rightarrow$ (ii).
For the other direction, if M is not free then there is some $m \in M$, $m \neq 0$, but $a \cdot m = 0$ for some nonzero integer a.

Consider $\varphi : \mathbb{Z} \to \mathbb{Z}$, $\varphi(b) := a \cdot b$.
This is injective. Like in the pf. of last thm, we have a comm. diagram (using Lem [p. 59])

$$\begin{tikzcd} M \otimes_{\mathbb{Z}} \mathbb{Z} \arrow[r, "id_M \otimes \varphi"] \arrow[d, "\cong"'] & M \otimes_{\mathbb{Z}} \mathbb{Z} \arrow[d, "\cong"] \\ M \arrow[r, "\tilde{\varphi}"] & M \end{tikzcd}$$

$\tilde{\varphi}(n) = a \cdot n$.
But $m \neq 0$, $m \in \ker(\tilde{\varphi})$. So M not flat.

Δ

(62)

Categories and Functors

Def A <u>category</u> $\underline{C}$ consists of:

- A set $Ob(\underline{C})$, whose elements are the <u>objects</u> of $\underline{C}$.

- For every pair of object $C, D \in Ob(\underline{C})$ there is a set $Hom_{\underline{C}}(C, D)$, whose elements are called <u>morphisms</u>. They are denoted by $f: C \to D$.

- For every triple $C, D, E \in Ob(\underline{C})$ there is a function

$$\circ : Hom_{\underline{C}}(D,E) \times Hom_{\underline{C}}(C,D) \to Hom_{\underline{C}}(C,E)$$

called <u>composition</u>. $(g,f) \mapsto g \circ f$

- For every object C there is a morphism $id_C \in Hom_{\underline{C}}(C,C)$, called the <u>identity</u> morphism.

The <u>axioms</u> are:

- <u>Associativity</u>: $h \circ (g \circ f) = (h \circ g) \circ f$ for composable morphisms f, g, h.

- <u>Units</u>: $id_D \circ f = f = f \circ id_C$ for all $f: C \to D$.

Remark on set theory: we fix a universe $\underline{\mathcal{U}}$, a set large enough to contain as elements all mathematical objects (groups rings etc) that we are interested in, their cartesian products, etc.

A set $S \in \underline{\mathcal{U}}$ is called small.

We always assume that

$$Ob(\underline{C}) \subseteq \underline{\mathcal{U}} \quad \text{and} \quad Hom_{\underline{C}}(C, D) \in \underline{\mathcal{U}}.$$

[For deeper discussion see Mac Lane, "Cats for the Working Mathematician", I.6]

- to here 29.11 -

Example 1. The category Set. Its objects are the small sets. $Ob(\underline{Set}) = \underline{\mathcal{U}}$.
The morphisms $f: S \to T$ are the functions.

Example 2. Fix a (small) ring A. The cat. Mod A has as objects the (small) A-mods.
The morphisms $\varphi: M \to N$ are the A-mod. homs.