Proof of L4.12 Define $\delta : D \to D$, $\delta(x) = [a, x] = ax - xa$.

δ is a derivation ($\delta(xy) = \delta(x)y + x\delta(y)$, $\delta(x+y) = \delta(x) + \delta(y)$)

and $K := \mathbb{F}_p[a]$ linear ($\delta(\lambda x) = \lambda \delta(x)$ for $\lambda \in K$).

$m \geq 1$ minimal w. $a^{p^m} = a \Rightarrow K \cong \mathbb{F}_{p^m}$.

Claim: (1) $\delta^{p^n} = [a^{p^n}, x]$ $\forall n \geq 1$ (2) $\delta^{p^m} = \delta$

Proof: (1) $\delta^i(x) = \sum_{j=0}^{i} (-1)^{i-j} \binom{i}{j} a^j x a^{i-j}$ (combinatorial argument or induction)

Now $p \mid \binom{p^n}{j}$ unless $j \in \{0, p^n\} \Rightarrow \delta^{p^n}(x) = a^{p^n} x - x a^{p^n}$

(2) $a^{p^m} = a \Rightarrow \delta^{p^m}(x) = \delta(x)$ $\square$(Claim)

So $f(\delta) = 0$ with $f = t^{p^m} - t \in \mathbb{F}_p[t]$ (taken in $\mathrm{End}_K(D)$)

$f = \prod_{b \in K} (t - b)$. Let $g = t(t-b_1)\cdots(t-b_e)$ with e minimal s.t.

$g(\delta) = 0 \Rightarrow e \geq 1$ since $\delta \neq 0 \Rightarrow \delta(\delta - b_1)\cdots(\delta - b_{e-1}) \neq 0$

($b_1, \dots, b_e \in K \setminus \{0\}$ pw. distinct.)

Let $v \in D$ be s.t. $x := \delta(\delta - b_1) \cdots (\delta - b_{e-1}) v \neq 0$

$\Rightarrow (\delta - b_e) x = 0$, so x is an eigenvector of δ w. eigenvalue $b := b_e \in K$

$\Rightarrow ax - xa = bx \Rightarrow xa = (a-b)x \Rightarrow xax^{-1} = a - b$

Now a, $a-b$ are elements of the finite field K of same multiplicative order. Since $K^\times$ is cyclic, they generate the same subgroup

$\Rightarrow a - b = a^i$ for some $i \geq 1$, $a \neq a^i$ since $b \neq 0$. $\square$

For $n \geq 1$, let $\mu_n(\overline{\mathbb{Q}}) := \{\zeta \in \overline{\mathbb{Q}} : \zeta^n = 1\}$ the n-th roots of unity, and $\mu_n^*(\overline{\mathbb{Q}}) := \{\zeta \in \mu_n(\overline{\mathbb{Q}}) : \zeta^m \neq 1 \text{ for } m \mid n, m \neq n\}$ the n-th primitive roots of unity. Then $|\mu_n(\overline{\mathbb{Q}})| = n$, $|\mu_n^*(\overline{\mathbb{Q}})| = \varphi(n)$ Euler-φ-function

Define $\Phi_n(x) := \prod_{\zeta \in \mu_n^*(\overline{\mathbb{Q}})} (x - \zeta)$ the n-th cyclotomic polynomial.

Lemma 4.14: (1) If $m \mid n$, then $x^m - 1 \mid x^n - 1$ in $\mathbb{Z}[x]$

(2) $\Phi_n(x) \in \mathbb{Z}[x]$ and $\Phi_n(x) \mid x^n - 1$ in $\mathbb{Z}[x]$

Proof: (1) $x^n - 1 = (x^m)^{n/m} - 1^{n/m} = (x^m - 1) \sum_{j=0}^{n/m - 1} x^{mj}$

(2) If $m \mid n$, then $x^m - 1 \mid x^n - 1$. Since $\mathbb{Z}[x]$ is a UFD, also $F := \operatorname{lcm}(\{x^m - 1 : m \mid n, m < n\})$ divides $x^n - 1$.

$$\frac{x^n - 1}{F} = \prod_{\substack{\zeta \in \mu_n(\overline{\mathbb{Q}}) \\ \zeta \notin \mu_m(\overline{\mathbb{Q}}) \\ m \mid n,\ m \neq n}} (x - \zeta) = \prod_{\zeta \in \mu_n^*(\overline{\mathbb{Q}})} (x - \zeta) = \Phi_n(x).$$

$\frac{x^n - 1}{F} \in \mathbb{Z}[x]$

□

Remark: Φ_n is irreducible

Lemma 4.15: If D is a division ring and $K \subseteq L \subseteq D$ are subfields, then $[D : K] = [D : L][L : K]$ ($[D : K] = \dim_K D$)

Proof: If $\{e_i\}_{i \in I}$ is an L-basis of D and $\{f_j\}_{j \in J}$ is a K-basis of L, then $\{e_i f_j : i \in I, j \in J\}$ is a K-basis of D.

□

Proof of T4.13: $Z(D) := F$ is a finite field

$\Rightarrow |F| = q$ with q a prime power $\Rightarrow |D| = q^n$ with $n = \dim D_F$

Class equation for $D^\times$:

For $a \in D^\times$ $C(a) := \{b \in D : ba = ab\}$ (centralizer) is a division ring, $|\{bab^{-1} : b \in D\}| = |D^\times| / |C(a)^\times|$.

$$\Rightarrow q^n - 1 = |D^\times| = \underbrace{q-1}_{\text{center}} + \sum_{i=1}^{\ell} \frac{|D^\times|}{|C(a_i)^\times|} = q - 1 + \sum_{i=1}^{\ell} \frac{q^n - 1}{q^{m_i} - 1} \quad (*)$$

where $a_1, \dots, a_\ell$ represent the non-trivial conjugacy classes in $D^\times$.

Here $|C(a_i)^\times| = q^{m_i} - 1$ for $1 \leq m_i < n$ since $C(a_i)$ is a division ring with some $m_i = \dim C(a_i)_F$.

Note $\frac{x^n - 1}{x^{m_i} - 1} = \Phi_n(x) H_i(x)$ with $H_i \in \mathbb{Z}[x]$.

$\Phi_n(x) \in \mathbb{Z}[x] \to \Phi_n(q) \in \mathbb{Z}$ and $\Phi_n(q) \mid \frac{q^n - 1}{q^{m_i} - 1}$

$(*) \Rightarrow \Phi_n(q) \mid q - 1$

But $\Phi_n(q) = \prod_{\zeta \in \mu_n^*(\mathbb{C})} (q - \zeta)$ and $|q - \zeta| > q - 1$ if $\zeta \neq 1$

so this is only possible if $n = 1 \Rightarrow D = F$. $\square$

5. Tensor Products

Let $M_R \in \text{Mod-}R$, ${}_R N \in R\text{-Mod}$, $X \in Ab$ ($= \mathbb{Z}\text{-Mod}$)

A map $\varphi: M \times N \to X$ is **R-balanced** if $\forall m, m' \in M \; \forall n, n' \in N \; \forall r \in R$:

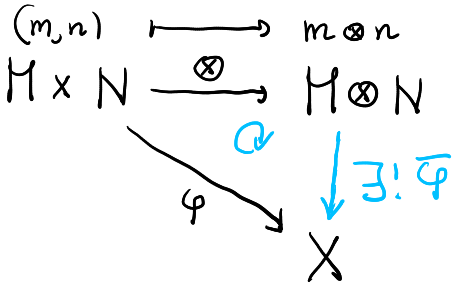
$$\varphi(m+m', n) = \varphi(m, n) + \varphi(m', n)$$

$$\varphi(m, n+n') = \varphi(m, n) + \varphi(m, n') \quad \text{and}$$

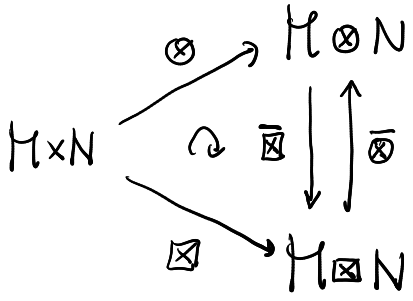
$$\varphi(mr, n) = \varphi(m, rn)$$

The **tensor product** of M and N is an abelian group $M \otimes_R N$ together with an R-balanced map $\otimes: M \times N \to M \otimes_R N$ satisfying the following

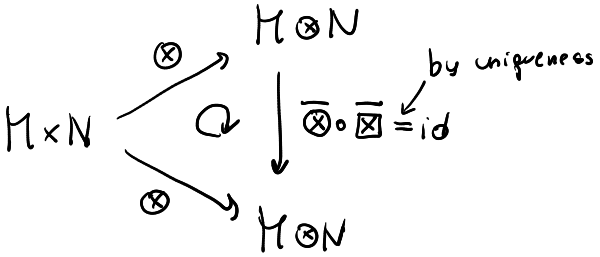
UP: If $\varphi: M \times N \to X$ ($X \in Ab$) is R-balanced, there exists a unique group hom. $\overline{\varphi}: M \otimes_R N \to X$ s.t. $\varphi = \overline{\varphi} \circ \otimes$.



$(M \otimes_R N, \otimes)$ is unique up to unique iso: If $(M \boxtimes N, \boxtimes)$ satisfies the same UP:



but also:



and $\overline{\boxtimes} \circ \overline{\otimes} = id$

Existence: Let F be the free $\mathbb{Z}$-module with basis

$$\{e_{(m,n)} : (m,n) \in M \times N\}$$

Let $K \leq F_{\mathbb{Z}}$ be generated by $(\forall m, m' \in M \; \forall n, n' \in N \; \forall r \in R)$:

$$e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)}, \quad e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')},$$

$$e_{(mr,n)} - e_{(m,rn)}.$$

Define $M \otimes_R N := F/K$, $\otimes : M \times N \to M \otimes_R N$, $(m,n) \mapsto m \otimes n := e_{(m,n)} + K$

Check: $\otimes$ R-balanced, $M \otimes_R N$ satisfies the UP (using homomorphism thm)

Elements of form $m \otimes n$ are pure (= elementary), general elements: $\sum_{i=1}^{k} m_i \otimes n_i$, $m_i \in M$, $n_i \in N$.

If $f : M_R \to M'_R$, $g : {}_R N \to {}_R N'$ are module hom's then

$(f,g) : M \times N \longrightarrow M' \otimes_R N'$, $(m,n) \mapsto f(m) \otimes g(n)$ is R-balanced

$[\; f(mr) \otimes g(n) = f(m)r \otimes g(n) = f(m) \otimes rg(n) = f(m) \otimes g(rn) \;]$,

and induces a unique $f \otimes g : M \otimes N \to M' \otimes N'$.

$\Longrightarrow$ $\otimes : \underline{\text{Mod}}\text{-}R \times R\text{-}\underline{\text{Mod}} \longrightarrow \underline{\text{Ab}}$ is a functor.

⚠ $f \otimes g$ also makes sense as element of $\text{Hom}(M,M') \otimes_{\mathbb{Z}} \text{Hom}(N,N')$, but this is something different in general.

Bimodules: If ${}_S M_R$, ${}_R N_T$ are (S,R), resp. (R,T)-bimodules, then ${}_S M_R \otimes_R N_T = {}_S(M \otimes_R N)_T$ is an (S,T)-bimodule via

$s(mn)t := (sm)\otimes(nt)$.

Remarks: (1) If ${}_{R,R}M$ or ${}_{R,R}N$ are just modules, they are ${}_{\mathbb{Z}}M_R$, ${}_R N_{\mathbb{Z}}$ bimodules, so the previous case is a special case!

(2) If R is commutative, every module is an (R,R)-bimodule, so for $M,N \in \text{Mod-}R$, $M\otimes_R N$ is again an R-module.

$\Rightarrow \otimes$ is a functor $(S,R)\text{-Mod} \times (R,T)\text{-Mod} \to (S,T)\text{-Mod}$.

R commutative: $M,N,X \in R\text{-Mod}$

$f: M\times N \to X$ is R-bilinear if f is R-balanced & $f(rm,n) = rf(m,n) = f(m,rn)$ $\forall m\in M\ \forall n\in N\ \forall r\in R$

Then $M\otimes_R N$ satisfies analogous UP wrt. R-bilinear maps:

$f: M\times N \to X$ R-bilinear

$\Rightarrow \exists!\ \bar{f}\in \mathrm{Hom}_R(M\otimes_R N, X_R)$: $\bar{f}\circ\otimes = f$.

$\otimes$-Hom Adjunction:

Motivation/Comparison: In Set,

$\otimes$ $\mathrm{Hom}(A\times B, C) \cong \mathrm{Hom}(A, \mathrm{Hom}(B,C))$ (functorial in A,B,C)

$f: A\times B \to C \mapsto (a \mapsto f_a: B\to C)$, $f_a(b) = f(a,b)$

$(a,b) \mapsto (\underbrace{f(a)}_{B\to C})(b) \leftarrow\!\shortmid f$

Two (bi) functors: $- \times -$: $\mathrm{Set}\times\mathrm{Set}\to\mathrm{Set}$

$\mathrm{Hom}(-,-)$: $\mathrm{Set}^{op}\times\mathrm{Set}\to\mathrm{Set}$

$- \times B : \underline{Set} \to \underline{Set}$, $\quad \mathrm{Hom}(B, -) : \underline{Set} \to \underline{Set}$

$\otimes$: $- \times B$ is left adjoint to $\mathrm{Hom}(B, -)$

($\Rightarrow$ $- \times B$ commutes with colimits ; $\mathrm{Hom}(B, -)$ with limits)

For (bi)modules: first note: if M_R, N_R are modules

$\mathrm{Hom}(M_R, N_R)$ is i.g. only an abelian group! [$(fr)(m) \neq f(mr)$ does not work.]. But:

-) If ${}_S M_R$ is a bimodule, $\mathrm{Hom}({}_S M_R, N_R)_S$ is a right S-module, (contravariant)

via $(fs)(m) := f(sm)$.

-) If ${}_T N_R$ is a bimodule, ${}_T\mathrm{Hom}(M_R, {}_T N_R)$ is a left T-module, (covariant)

via $(tf)(m) := tf(m)$

$\otimes$-Hom Adjunction: ${}_R M_S$ bimodule,

$- \otimes_R M : \underline{\mathrm{Mod}\text{-}R} \to \underline{\mathrm{Mod}\text{-}S}$, $\quad \mathrm{Hom}_S(M_S, -) : \underline{\mathrm{Mod}\text{-}S} \to \underline{\mathrm{Mod}\text{-}R}$

are adjoint via ($X_R \in \mathrm{Mod}\text{-}R$, $Y_S \in \mathrm{Mod}\text{-}S$):

$$\mathrm{Hom}_S(X_R \otimes_R M_S, Y_S) \cong \mathrm{Hom}_R(X_R, \mathrm{Hom}(M_S, Y_S)_R)$$

$$f \longmapsto (x \mapsto f_x), \quad f_x(m) = f(x \otimes m)$$

$$x \otimes m \mapsto g(x)(m) \longleftarrow g$$

[Proof: using UP!]

Remark: If X is a (T, R)-bimodule, Y a (T', S) bimodule, then the iso is as (T', T)-bimodules.

So: $\otimes$ commutes with colimits (direct sum, cokernel)

If $A_R \to B_R \to C_R \to 0$ is exact, then so is

$A_R \otimes M \to B \otimes_R M \to C \otimes_R M \to 0$, i.e. $- \otimes_R M$ is right exact

(i.e., $f: A_R \to B_R$ injective $\not\Rightarrow$ $f \otimes M: A \otimes_R M \to B \otimes_R M$ injective)

Proof Sketch: First verify:

(i) $0 \to N_R \xrightarrow{f} M_R \xrightarrow{g} K_R$ exact

$\Leftrightarrow \forall X \in \text{Mod-}R$: $0 \to \text{Hom}(X_R, N_R) \xrightarrow{f_*} \text{Hom}(X_R, M_R) \xrightarrow{g_*} \text{Hom}(X_R, K_R)$ exact

$f_*(\varphi) = f \circ \varphi \qquad g_*(\psi) = g \circ \psi$

(ii) $N_R \xrightarrow{f} M_R \xrightarrow{g} K_R \to 0$ exact

$\Leftrightarrow \forall X \in \text{Mod-}R$: $0 \to \text{Hom}(K_R, X_R) \xrightarrow{g^*} \text{Hom}(M_R, X_R) \xrightarrow{f^*} \text{Hom}(N_R, X_R)$ exact

$g^*(\varphi) = \varphi \circ g \qquad f^*(\psi) = \psi \circ f$

($\to$: $\text{Hom}(X_R, -)$, $\text{Hom}(-, X_R)$ are left exact)

Now: $A_R \xrightarrow{f} B_R \xrightarrow{g} C_R \to 0$ exact, ${}_R X \in R\text{-Mod}$

Consider $A \otimes_R X \xrightarrow{f \otimes \mathrm{id}_X} B \otimes_R X \xrightarrow{g \otimes \mathrm{id}_X} C \otimes_R X \to 0$ (*)

Apply $\text{Hom}_{\mathbb{Z}}(-, Y)$, $Y \in Ab$:

$$\begin{array}{ccccccc} 0 \to & \text{Hom}_{\mathbb{Z}}(C \otimes_R X, Y) & \longrightarrow & \text{Hom}_{\mathbb{Z}}(B \otimes_R X, Y) & \longrightarrow & \text{Hom}_{\mathbb{Z}}(A \otimes_R X, Y) & \\ & \downarrow \wr \ (\otimes\text{-Hom adj.}) & \circlearrowright & \downarrow \wr & \circlearrowright & \downarrow \wr & \\ 0 \to & \text{Hom}_R(X, \text{Hom}_{\mathbb{Z}}(C, Y)) & \longrightarrow & \text{Hom}_R(X, \text{Hom}(B, Y)) & \to & \text{Hom}_R(X, \text{Hom}(A, Y)) & \end{array}$$

$\xRightarrow{(i),(ii)}$ lower row is exact $\to$ upper row is exact

$\xRightarrow{(ii)}$ (*) is exact.