# November 29, hours 32-33: Uniqueness

November-24-11
12:08 PM

$\frac{1}{2}$T2C2W: [$M$ f.g. / $R$ PID $\Rightarrow$ $M \cong \overbrace{R^k \oplus \bigoplus R/\langle p_i^{s_i}\rangle}^{\text{unique}}$]

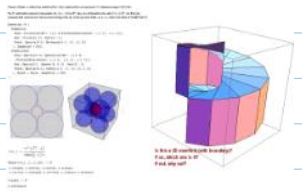
$\Rightarrow$ structure of f.g. Abelian groups, J.C.F.

**Goal:** Uniqueness.

HW 4 due, HW5 & last week's schedule on web.

Riddle solutions. $\infty$, Möbius.

Nov 24 Riddles.png:



**Tensor Products.** Given $M, N$

$$M \otimes_R N := \left\{ \sum_{i=1}^{\infty} a_i (m_i \otimes n_i) : n \in \mathbb{N}, a_i \in R \right\} \Big/ \begin{array}{l} (am)\otimes n = a(m\otimes n) = m\otimes(an) \\ (m_1+m_2)\otimes n = \ldots \\ m\otimes(n_1+n_2) = \ldots \end{array}$$

Example. If $q \in \gcd(a,b)$, $q = sa+tb$, $\frac{R}{\langle a\rangle} \otimes \frac{R}{\langle b\rangle} \cong \frac{R}{\langle q\rangle}$

Proof. $[r_1]_a \otimes [r_2]_b \longrightarrow [r_1 \cdot r_2]_q$ well-def: $[q]\otimes[1] = [sa+tb]\otimes[1] = 0$

$[r]_a \otimes [1]_b \longleftarrow [r]_q$ Inverseness: $[r_1 r_2]\otimes[1] = [r_1][r_2]$

**Theorem.** $(R\text{-mod}, \oplus, \otimes, 0, R)$ is a "ring".

**Theorem.** The universal property.

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes N \\ & \searrow^{\text{bilinear}} & \downarrow \exists! \\ & & P \end{array}$$

$\otimes$: $R$-linear

not done

**Theorem.** $(M,N) \longmapsto M \otimes N$ is a "bifunctor".

---

**Example.** $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n \cong \mathbb{Q}^n$ "Extension of scalars". ($\mathbb{Q}^n$: a $\mathbb{Q}$-module!)

In general, given $\phi: R \to S$ a ring morphism, $S$ is an $R$ module & set $M_S := S \otimes_R M$. Then $M_S$ is an $S$-module and $R^n_S = S^n$.

---

Prop. For any domain $R$ there is a unique field $Q(R)$ s.t. $R \xrightarrow{1\text{-}1} Q(R)$, $\exists!$ $\downarrow$, $R \to F$ — "The Field of Fractions"

proof later.

Claim If $M$ is torsion $\left[\forall m \in M\ \exists r \in R\setminus\{0\},\ rm = 0\right]$ then $M_{Q(R)} = 0$.

Prop If $M \cong R^k \oplus \bigoplus R/\langle p_i^{s_i}\rangle$, then

1. $\dim_{Q(R)} M_{Q(R)} = k$
2. $\dim_{R/\langle p\rangle} M_{R/\langle p\rangle} = k + |\{i : p_i \sim p\}|$
3. $\dim_{R/\langle p\rangle} \mathrm{im}(m \mapsto p^s m)_{R/\langle p\rangle} = k + |\{i : p_i \sim p \ \&\ s < s_i\}|$

not done

as $\mathrm{im}(m \mapsto p^s m) \cong$
$\begin{cases} p^s R \cong R & \text{on } R \\ R/\langle q^t\rangle & \text{on } R/\langle q^t\rangle \quad q \not\sim p \\ 0 & \text{on } R/\langle p^t\rangle \quad s \geq t \\ R/\langle p^{t-s}\rangle & \text{on } R/\langle p^t\rangle \quad s < t \end{cases}$

and $\ker(m \mapsto p^s m) \cong$
$\begin{cases} 0 & \text{on } R \\ 0 & \text{on } R/\langle q^t\rangle \quad q \not\sim p \\ R/\langle p^t\rangle & \text{on } R/\langle p^t\rangle \quad s \geq t \\ R/\langle p^s\rangle & \text{on } R/\langle p^t\rangle \quad s < t \end{cases}$

$R/\langle p^s\rangle \hookrightarrow \ker$ by $[r] \mapsto [p^{t-s} r]$

So such a decomposition is unique!

Localization & Fields of Fractions. Let $R$ be a commutative domain

Def A multiplicative subset $S$ of $R\setminus\{0\}$. (contains 1, closed under $\times$)

Examples $R\setminus\{0\}$, $R\setminus P$ ($P$ prime), Powers of $a \neq 0$.

Definition $S^{-1}R = \{\frac{r}{s}\}/\frac{r_1}{s_1} \sim \frac{r_2}{s_2}$ if $r_1 s_2 = r_2 s_1$

$\left[\frac{r_1}{s_1} \sim \frac{r_2}{s_2},\ \frac{r_2}{s_2} \sim \frac{r_3}{s_3} \Rightarrow r_1 s_2 = r_2 s_1,\ r_2 s_3 = r_3 s_2 \Rightarrow\right.$

$\left. r_1 s_2 s_3 = r_2 s_1 s_3 = s_1 r_3 s_2 \Rightarrow r_1 s_3 = r_3 s_1\right]$

$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \ldots$

$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \ldots$

$R\setminus\{0\}$ — "Field of Fractions $Q(R)$"

$R\setminus P$ — "localization at $P$"

$R \to S^{-1}R$ is injective

$R \setminus P$ – "localization at $P$" is injective

$\{2^n\}$ – "dyadic rationals"

dont line

Abelian groups & the mult. groups of finite fields

$$A \cong \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/p_i^{s_i} \cong \mathbb{Z}^k \oplus \mathbb{Z}/a_1 \oplus \mathbb{Z}/a_2 \oplus \dots$$

$$a_1 \mid a_2 \mid a_3 \dots$$

Theorem If $F$ is finite, $F^*$ is cyclic.

Proof otherwise, $x^{a_1} - 1$ has too many roots.

(Aside: $\lambda$ is a root of $f \in F[x] \iff x - \lambda \mid f$, so $f$ may have at most $\deg(f)$ roots)