7.5 Hilbert's Theorem 90

Prop 7.20 (Independence of Characters) Let $(M,\cdot)$ be a monoid, L a field, $f_1,\dots,f_n : M \to L^\times$ pairwise distinct monoid hom's.
Then $f_1,\dots,f_n$ are L-linearly independent as elts of the L-vector space $\mathrm{Hom}_{\mathrm{Set}}(M,L)$.

Proof: (Lit. L7.10) Suppose $\sum_{i=1}^{m} a_i f_i = 0$, wlog $a_1 \neq 0$, m minimal

$\forall x \in M$: $\sum_{i=1}^{m} a_i f_i(x) = 0$. Let $y \in M$ s.t. $f_1(y) \neq f_2(y)$

$\Rightarrow \sum_{i=1}^{m} a_i f_i(x) f_i(y) = \sum_{i=1}^{m} a_i f_i(xy) = 0$ and $\sum_{i=1}^{m} a_i f_i(x) f_1(y) = 0$

$\rightarrow \sum_{i=2}^{m} a_i (f_i(y) - f_1(y)) f_i = 0$ ↯ minimality of m □

Thm 7.21 (Hilbert-Noether) If L/K is Galois, $G = \mathrm{Gal}(L/K)$, then $H^1(G, L^\times) = \{1\}$.

Proof: Let $f \in Z^1(G, L^\times)$, i.e. $f : G \to L^\times$ s.t.

$\forall \sigma,\tau \in G$: $1 = \delta^1(f)(\sigma,\tau) = \sigma(f(\tau))\, f(\sigma\tau)^{-1} f(\sigma)$

$\Leftrightarrow f(\sigma\tau) = \sigma(f(\tau)) \cdot f(\sigma) = f(\sigma) \cdot \sigma(f(\tau))$

$\overset{P7.20}{\Longrightarrow}$ $G \subseteq \mathrm{Hom}_{\mathrm{Set}}(L,L)$ is L-linearly independent

$\Rightarrow 0 \neq \sum_{\tau \in G} f(\tau)\tau$. Let $b \in L$ s.t. $0 \neq \sum_{\tau \in G} f(\tau)\tau(b) =: a$

$\Rightarrow \sigma(a) = \sum_{\tau \in G} \sigma(f(\tau))\,\sigma(\tau(b)) = \frac{1}{f(\sigma)} \sum_{\tau \in G} f(\sigma\tau)\,\sigma(\tau(b)) = \frac{a}{f(\sigma)}$

$\Rightarrow f(\sigma) = \frac{a}{\sigma(a)} = \frac{\sigma(a^{-1})}{a^{-1}} = \delta^0(a^{-1}) \Rightarrow f \in B^1(G, L^\times)$. □

L/K is **cyclic** if L/K is Galois with $G := Gal(L/K)$ cyclic, say generated by σ, $G = \{id, \sigma, \dots, \sigma^{n-1}\}$, $n = [L:K]$

$N_{L/K} : L \to K$ is defined by $N_{L/K}(x) = \prod_{i=0}^{n-1} \sigma^i(x)$

(fixed by σ, so in K)

Thm 7.22 (Hilbert's Thm 90) Let L/K be cyclic, $Gal(L/K) = \langle \sigma \rangle$, $a \in L^\times$. Then $N_{L/K}(a) = 1 \iff \exists b \in L^\times : a = \frac{\sigma(b)}{b}$.

Proof: ($\Rightarrow$ is non-trivial)

1-coboundaries: $b \in L^\times = C^0(G, L^\times)$: $(\delta^0 b)(\sigma^i) = \frac{\sigma^i(b)}{b}$

$\delta^0 b$ fully determined by $(\delta^0 b)(\sigma) = \frac{\sigma(b)}{b}$, bec. $\frac{\sigma^{i+1}(b)}{\sigma^i(b)} = \sigma^i\left(\frac{\sigma(b)}{b}\right)$

so $B^1(G, L^\times) \overset{bij}{\leftrightarrow} \left\{ \frac{\sigma(b)}{b} : b \in L^\times \right\}$.

1-cocycles: $f \in Z^1(G, L^\times) \iff f(\sigma^{i+j}) = \sigma^i(f(\sigma^j)) \cdot f(\sigma^i)$

Since $f(\sigma^{i+1}) = \sigma(f(\sigma^i)) f(\sigma) = \sigma^{i-1}(a) \cdots \sigma(a) a$ w. $a := f(\sigma) \in L^\times$,

$f(\sigma)$ fully determines f.

$\rightarrow 1 = f(id) = f(\sigma^n) = N_{L/K}(a)$, so necessarily $N_{L/K}(a) = 1$.

Also sufficient: if $N_{L/K}(a) = 1$, then $f(\sigma^i) = \sigma^{i-1}(a) \cdots \sigma(a) a$ is a 1-cocycle

$\overset{T7.21}{\Rightarrow} Z^1(G, L^\times) = B^1(G, L^\times)$ so

$\forall a \in L^\times$: $N_{L/K}(a) = 1 \iff a = \frac{\sigma(b)}{b}$ for some $b \in L^\times$. $\square$

8. Direct-sum Decompositions of Modules

R ring

Def: $M \in \text{Mod-}R$ is *indecomposable* if $M \neq 0$ and whenever $M \cong M_1 \oplus M_2$, then $M_1 = 0$ or $M_2 = 0$. Otherwise M is *decomposable*.

Exm:
- M_R simple $\Rightarrow$ M_R indecomposable
- $\mathbb{Z}_{\mathbb{Z}}$ is indecomposable but not simple
- If R is a commutative domain, every nonzero ideal is indecomposable.
  [$I = J_1 + J_1 \Rightarrow 0 \neq J_1 J_2 \subseteq J_1 \cap J_2$]
- If R semisimple, M_R indecomposable $\Leftrightarrow$ M_R simple [T2.12]
  and every f.g. module is a direct sum of indecomposable modules (unique up to order and isomorphism)

·) $R = \mathbb{Z}$: not semisimple. Simple modules: $\mathbb{Z}/p\mathbb{Z}$, p prime
F.g. modules are of form $\mathbb{Z}^r \oplus \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_s^{e_s}\mathbb{Z}$, p_i primes, $e_i \geq 1$, $r \geq 0$ (Structure Thm for f.g. abelian groups).
Indecomposables: $\mathbb{Z}$, $\mathbb{Z}/p^e\mathbb{Z}$ with p prime, $e \geq 1$.
Every f.g. is still uniquely a direct sum of indecomposables!

Prop 8.1 R ring. If M_R is noetherian or artinian, then M is a finite direct sum of indecomposable submodules.

Lemma 8.2: If $0 \neq M_R$ is noetherian or artinian, it has an indecomposable direct summand.

Proof: Say M_R noetherian (the other case is analogous). Consider

$\Omega = \{ X_R \subsetneq M_R : X_R \text{ is direct summand of } M \}$, $0 \in \Omega \Rightarrow \Omega \neq \emptyset$

Let $X_R \in \Omega$ be maximal (by noetherianity), $M_R = X_R \oplus Y_R$, $Y_R \neq 0$

Then Y_R is indecomposable, as otherwise $Y_R = Y_1 \oplus Y_2$, $Y_1, Y_2 \neq 0$, so

$X \oplus Y_1 \supsetneq X$ is a direct summand of M $\lightning$ max. of X $\square$

Proof of P8.1: $M = 0$ ✓, wlog $M \neq 0$. Then $\exists Z_1 \leq M$ s.t.

$M = Z_1 \oplus M_1$, Z_1 indecomposable [I 8.2].

If $M_1 \neq 0$, we can repeat with M_1: $M = Z_1 \oplus Z_2 \oplus M_2$, Z_1, Z_2 indec.

etc.

If M is noetherian, $Z_1 \subsetneq Z_1 \oplus Z_2 \subsetneq \dots$ implies $M_n = 0$ and $M = Z_1 \oplus \dots \oplus Z_n$

after fin. many steps. If M is artinian, $M \supsetneq M_1 \supsetneq M_2 \supsetneq \dots$ is a descending

chain as long as $M_i \neq 0$, so again $M_n = 0$ after fin. many steps. $\square$

Exm $R = \mathbb{C}[x,y]$, $I = (x,y)$, $J = (x, y-1)$

$\Rightarrow I + J = R$. If $a \in I$, $b \in J$ s.t. $a + b = 1$, then

$$\varphi: \begin{cases} I \oplus J \xrightarrow{\sim} R \oplus (I \cap J) \\ (x,y) \longmapsto (x+y,\ bx - ay) \end{cases} \qquad \varphi^{-1}: \begin{cases} R \oplus (I \cap J) \to I \oplus J \\ (w,z) \longmapsto (aw + z,\ bw - z) \end{cases}$$

are isomorphisms.

$\rightarrow R \oplus (I \cap J) \cong I \oplus J$, but $I \neq R$, $J \neq R$ since I, J are non-principal.

$0, 1$ are the trivial idempotents of a ring.

Lemma 8.3: Let $M_R \neq 0$. Then M_R indecomposable $\Leftrightarrow$ $End(M_R)$ only has trivial idempotents.

Proof: Show: M_R decomposable $\Leftrightarrow$ $\exists$ non-trivial idempotent $e \in End(M_R)$

"$\Rightarrow$": $M = M_1 \oplus M_2$, $M_1, M_2 \neq 0$. Let $\pi: M \to M_1$ be the projection along M_2, i.e., $\pi|_{M_1} = id_{M_1}$, $\pi|_{M_2} = 0$.

Let $j: M_1 \hookrightarrow M$ be the embedding, $e := j \circ \pi \in End(M_R)$

Then $e^2 = j \circ \underbrace{\pi \circ j}_{= id_{M_1}} \circ \pi = j \circ \pi = e$ and $e \neq 0, id_M$.

"$\Leftarrow$": Let $e = e^2 \in End(M_R)$. Let $M_1 := im(e)$, $M_2 = ker(e)$

$M_1 \cap M_2 = 0$: Let $x \in M_1 \cap M_2 \Rightarrow x = e(y), y \in M \Rightarrow x = e^2(y) = e(x) = 0$ ($x \in M_2$)

$M_1 + M_2 = M$: Let $x \in M \Rightarrow x = \underbrace{e(x)}_{\in M_1} + (x - e(x))$

$e(x - e(x)) = e(x) - e(x) = 0 \Rightarrow x - e(x) \in M_2$. □

8.1 Local Rings

Def: A ring R is local if $R/J(R)$ is a division ring.

Exm: R division ring, $R = \mathbb{Z}/p^n\mathbb{Z}$, $R = \mathbb{Z}_p$ (p-adic numbers), $R = S_{\mathfrak{p}}$ with S commutative ring, $\mathfrak{p}$ max. ideal.

Prop 8.4 For $R \neq 0$, TFAE:

(a) R is local

(b) R has a unique max. right ideal.

(c) — " — left ideal.

(d) $R \setminus R^\times$ is an ideal of R

(e) If $a, b \in R$ are s.t. $a+b \in R^\times$, then $a \in R^\times$ or $b \in R^\times$

Proof: (a) $\Rightarrow$ (b) If M is a max. right ideal of R, then

$J(R) \subseteq M \subsetneq R \Rightarrow M/J(R) \subsetneq R/J(R)$ is a right ideal $\Rightarrow M/J(R) = 0$, i.e.,

$J(R) = M$.

(b) $\Rightarrow$ (a) $M = J(R)$ is the unique max. right ideal.

Suppose $a \in R \setminus J(R) \rightarrow aR + M = R \rightarrow \bar{a}$ right invertible in $R/J(R)$

$\Rightarrow R/J(R)$ div. ring.

(a) $\Leftrightarrow$ (c) by symmetry w. (a) $\Leftrightarrow$ (b).

(a) $\Rightarrow$ (d) Since unib left module $J(R)$ [P3.4], $R \setminus J(R) \subseteq R^\times$.

$R^\times \subseteq R \setminus J(R)$ holds because $J(R) \subsetneq R$. So $R \setminus J(R) = R^\times$, i.e. $R \setminus R^\times = J(R)$

(d) $\Rightarrow$ (e) If $a, b \in R \setminus R^\times$, then $a+b \in R \setminus R^\times$ by (d)

(e) $\Rightarrow$ (a) let $a \in R \setminus J(R) \Rightarrow \exists r \in R: 1 - ra \notin R^\times$ [L3.1]

$1 = (1-ra) + ra \overset{(e)}{\Rightarrow} ra \in R^\times \Rightarrow \bar{a}$ left invertible in $R/J(R)$.

Since this holds for all $\bar{0} \neq \bar{a}$, $R/J(R)$ is a division ring. $\square$

Prop 8.5 If $0 \neq R$ and every $a \in R \setminus R^\times$ is nilpotent, then R is local.

Proof: Show: $R\setminus R^\times \subseteq J(R)$ (then $J(R) = R\setminus R^\times$)

Let $a \in R\setminus R^\times$, $m \geq 1$ minimal with $a^m = 0$

$\Rightarrow \forall r \in R$: $ra \notin R^\times$ [If $ra \in R^\times$, then $(ra)a^{m-1} = 0 \Rightarrow a^{m-1} = 0$ ↯].

$\rightarrow Ra \subseteq R\setminus R^\times \Rightarrow Ra$ is nil (left) ideal $\Rightarrow Ra \subseteq J(R)$ [L3.5]. □

Prop 8.6 If R is local, it has only trivial idempotents

Proof Let $e \in R$ with $e = e^2$.

$1 = e + (1-e) \overset{[P9.4]}{\Longrightarrow} e \in R^\times$ or $1-e \in R^\times$

$0 = e(1-e) \Rightarrow e = 0$ or $1-e = 0$ □

8.2 Local endomorphism rings

Def R ring. $M \in$ Mod-R is strongly indecomposable if $\mathrm{End}(M_R)$ is local

Exm: •) If M_R is simple, $\mathrm{End}(M_R)$ is a div. ring, hence local.

•) $\mathbb{Z}_\mathbb{Z}$ is indecomposable, but not strongly indecomposable:

$\mathrm{End}(\mathbb{Z}_\mathbb{Z}) = \mathbb{Z}$.

Thm 8.7 (Krull-Remak-Schmidt-Azumaya, KRSA)

Let $M \in$ Mod-R. If $M \cong M_1 \oplus \dots \oplus M_r \cong N_1 \oplus \dots \oplus N_s$ with N_i indecomposable, M_i strongly indecomposable (for all i), then $r = s$ and $M_i \cong N_{\sigma(i)}$ for some permutation σ.

Proof: By induction on r. $r = 0, 1$ ✓. $r \geq 2$.

Wlog $M = M_1 \oplus \dots \oplus M_r = N_1 \oplus \dots \oplus N_s$ (internal direct sum).

Let $\alpha_i : M \to M_i \hookrightarrow M$, $\beta_i : M \to N_i \hookrightarrow M$ be the projections corresponding to the decompositions. ($\alpha_i|_{M_j} = 0$ for $j \neq i$, $\beta_i|_{N_j} = 0$ for $j \neq i$)

$\Rightarrow \quad id_M = \alpha_1 + \dots + \alpha_r = \beta_1 + \dots + \beta_s \in End(M_R)$.

$\Rightarrow \quad \alpha_1 = \alpha_1 \circ \beta_1 + \dots + \alpha_1 \circ \beta_s \in End(M_R)$

Restricting to M_1 (note $im(\alpha_1 \circ \beta_j) \subseteq M_1$)

$$id_{M_1} = \alpha_1|_{M_1} = \alpha_1 \circ \beta_1|_{M_1} + \dots + \alpha_1 \circ \beta_s|_{M_1} \in End(M_1)$$

$End(M_1)$ local $\Rightarrow \exists j$: $\alpha_1 \circ \beta_j|_{M_1}$ is an endomorphism of M_1.

Wlog $j = 1$ after renumbering.

$\Rightarrow \quad \beta_1|_{M_1} : M_1 \to N_1$ is a split monomorphism

$\Rightarrow \quad \beta_1(M_1)$ is a direct summand of $N_1 \overset{N_1 \text{ indec.}}{\Longrightarrow} N_1 = \beta_1(M_1)$

$\Rightarrow \quad \beta_1|_{M_1} : M_1 \xrightarrow{\sim} N_1$ is an isomorphism.

Claim (*): $M = M_1 \oplus N_2 \oplus \dots \oplus N_s$, then $M/M_1 \cong M_2 \oplus \dots \oplus M_r \cong N_2 \oplus \dots \oplus N_s$, and the IH implies the claim of the thm.

(*): Since $\beta_1|_{M_1}$ is injective, $0 = M_1 \cap \ker(\beta_1) = M_1 \cap (N_2 \oplus \dots \oplus N_s)$.

Let $n \in N_1$. To show: $n \in M_1 + N_2 + \dots + N_s$.

Let $n = \beta_1(m)$ with $m \in M_1 \Rightarrow \beta_1(n - m) = n - \beta_1(m) = n - n = 0$

$\Rightarrow n - m \in \ker(\beta_1) = N_2 + \dots + N_s$, so $n \in M_1 + N_2 + \dots + N_s$. $\square$