$G \hookrightarrow (R[G])^\times,\ g \mapsto g$ $\quad R \hookrightarrow R[G] = \{ \sum'_{g\in G} a_g g \mid a_g \in R, \text{ almost all } 0 \}$.
$a \mapsto a\cdot 1$

10.4 Kummer theory

First consider a commutative unitary ring R and a group G. Then giving an R-module with a left G-action is equivalent to giving a left module over the group ring $R[G]$. Giving a G-equivariant homomorphism of such R-modules is equivalent to giving a homomorphism of left $R[G]$-modules. We will always mean left modules below.

Proposition-Definition 10.4.1: To any $R[G]$-module M we associate

(a) the R-module of *G-invariants M^G* $:= \{m \in M \mid \forall g \in G\colon gm = m\}$, and

(b) the R-module of *G-coinvariants M_G* $:= M / \sum_{g\in G}(g-1)M$.

Here

(c) M^G is the largest $R[G]$-submodule of M, on which G acts trivially; and

(d) M_G is the largest $R[G]$-factor module of M, on which G acts trivially.

Any $R[G]$-module homomorphism $f\colon M \to N$ induces R-module homomorphisms

$$f^G\colon M^G \to N^G \qquad \text{and} \qquad f_G\colon M_G \to N_G.$$

$m \mapsto f(m)$ $\qquad [m] \mapsto [f(m)]$

$[(g-1)m] \mapsto [f((g-1)m)] = [(g-1)(f(m))] = [0]$

$\forall m \in M\ \forall g \in G$:
$g[m] = [gm] = [m]$
$\Rightarrow$ G acts trivially on M_G.
If $N \subset M$ is a submodule with trivial action of G on M/N $\Rightarrow$ $\forall m \in M$: $(g-1)m \in N$.
$\Rightarrow$ $M_G \twoheadrightarrow M/N$.

Proposition 10.4.2: Let G be a finite group of order d, such that d is invertible in R. Then for any exact sequence of $R[G]$-modules $M \xrightarrow{f} N \xrightarrow{h} L$ the induced sequences

$$M^G \xrightarrow{f^G} N^G \xrightarrow{h^G} L^G \qquad \text{and} \qquad M_G \xrightarrow{f_G} N_G \xrightarrow{h_G} L_G$$

are exact.

Proof: Let $t := \frac{1}{d} \cdot \sum_{g \in G} g \in R[G]$. $\Rightarrow \forall g' \in G:\ g't = tg' = t$

(a) $\forall m \in M:\ tm \in M^G$.

(b) $\forall m \in M^G:\ tm = \frac{1}{d} \cdot \sum_{g \in G} gm = \frac{1}{d} \sum_g m = m$.

Claim: $h^G \circ f^G = 0$.

Take $n \in \ker(h^G)$.

$\Rightarrow h(n) = 0$

$\Rightarrow n = f(m)$ for some $m \in M$.

$\Rightarrow n \overset{(b)}{=} tn = tf(m) = f(tm)$

with $tm \in M^G$ by (a).

$\Rightarrow \ker(h^G) = \operatorname{im}(f^G)$.

Claim: $h_G \circ f_G = 0$.

Take $[n] \in N_G$ with $h_G([n]) = 0 = [h(n)]$

$\Rightarrow h(n) = \sum_{g \in G}' (g-1) \ell_g$ for some $\ell_G = L$

$\Rightarrow h(tn) = \sum_{g \in G} \underbrace{t(g-1)}_{0} \ell_g = 0$

$\Rightarrow tn = f(m)$ for some $m \in M$.

$\Rightarrow [n] \overset{(b)}{=} t[n] = [tn] = [f(m)] = f_G([m])$

$\Rightarrow \ker(h_G) = \operatorname{im}(f_G)$.

qed.

Now consider an integer n ≥ 1 and a field K of chacteristic not dividing n. Let L/K be the maximal abelian galois extension whose galois group has exponent dividing n.

Proposition 10.4.3: If K contains all n-th roots of unity μ_n, then L is generated by the n-th roots of all elements of $K^\times$ and there is a natural isomorphism

$$\boxed{\begin{aligned} \operatorname{Gal}(L/K) &\xrightarrow{\sim} \operatorname{Hom}(K^\times, \mu_n), \\ \gamma &\longmapsto \left(x \mapsto \frac{\gamma \sqrt[n]{x}}{\sqrt[n]{x}} \right) \end{aligned}}$$

for any choice of $\sqrt[n]{x} \in L$.

Proof: $L = \bigcup L'$, L'/K finite abelian of exponent dividing n.
Each L' is generated by cyclic extensions L'' of ...
Algebra II $\Rightarrow$ $L'' = K(\sqrt[n]{x})$ for some $x \in K^\times$.
Also $\forall x \in K^\times$: $K(\sqrt[n]{x})/K$ is cyclic of exponent dividing n.
$\Rightarrow$ L is generated by $\sqrt[n]{x}$ for all $x \in K^\times$.

Map well defined:

$$\frac{\gamma \sqrt[n]{xy}}{\sqrt[n]{xy}} = \frac{\gamma\sqrt[n]{x}}{\sqrt[n]{x}} \cdot \frac{\gamma\sqrt[n]{y}}{\sqrt[n]{y}} \Rightarrow \text{homo in } x$$

(Homo in γ: $\forall \gamma, \delta \in \operatorname{Gal}(L/K)$:

$$\frac{\gamma\delta \sqrt[n]{x}}{\sqrt[n]{x}} = \frac{\gamma\sqrt[n]{x}}{\sqrt[n]{x}} \cdot \gamma \underbrace{\left(\frac{\delta\sqrt[n]{x}}{\sqrt[n]{x}}\right)}_{\in \mu_n \text{ fixed by } \gamma} \Rightarrow \text{homo in } \gamma$$

$\forall \gamma \in \ker$: $\gamma \sqrt[n]{x} = \sqrt[n]{x}$ for all x
$\Rightarrow \gamma = \mathrm{id}$.

$$\operatorname{Hom}(K^\times, \mu_n) = \operatorname{Hom}(\underbrace{K^\times/(K^\times)^n}, \mu_n)$$

$$= \varprojlim_{H < K^\times/(K^\times)^n \text{ finite subgroups}} \operatorname{Hom}(H, \mu_n)$$

$H \cong \times_i C_{n_i} \qquad n_i \mid n$

$\mathrm{Hom}(H, \mu_n) \cong \times_i \mathrm{Hom}(C_{n_i}, \mu_n) \cong \times_i C_{n_i}$

$\Rightarrow$ enough to show that $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Hom}(H, \mu_n)$.

Reduce to $n = \text{prime} = p$.

$H \subset K^\times/(K^\times)^p$ is an $\mathbb{F}_p$-subspace.

If not surjective, then image $= \mathrm{Hom}(\bar{H}, \mu_n)$ for $H \xrightarrow{\pi} \bar{H}$

For any $[x] \in \ker(\pi)$: $[x] \in K^\times/(K^\times)^p$ is nonzero $\Rightarrow K(\sqrt[p]{x}) \neq K$

$\Rightarrow \exists\, \sigma \in \mathrm{Gal}(L/K)$: $\sigma \sqrt[p]{x} \neq \sqrt[p]{x}$

$\Rightarrow$ Contradiction!

So homo is surjective.

qed

Proposition 10.4.4: In general, if $n = p$ is a prime, the above map induces a natural isomorphism

$$\boxed{\mathrm{Gal}(L/K) \;\cong\; \mathrm{Hom}(K(\mu_p)^\times, \mu_p)_{\mathrm{Gal}(K(\mu_p)/K)}}$$

Proof: $\mathrm{char}(K) \neq p$. Set $K' := K(\mu_p) \Rightarrow \Delta := \mathrm{Gal}(K'/K) \hookrightarrow \mathbb{F}_p^\times$ cyclic of order prime to p.

Let L' be the max. abelian extension of K' of exponent dividing p. Then L'/K is galois.

and $1 \to \underbrace{\mathrm{Gal}(L'/K')}_{\text{exponent} \mid p} \to \mathrm{Gal}(L'/K) \to \underbrace{\mathrm{Gal}(K'/K) = \Delta}_{\text{cyclic of order prime to } p} \to 1$ exact. $\exists$ section

$\Rightarrow \mathrm{Gal}(L'/K) \cong \mathrm{Gal}(L'/K') \rtimes \Delta$.

$$\begin{tikzcd}
L' \arrow[d, dash] \arrow[dr, dash] & \\
LK' \arrow[d, dash] \arrow[dr, dash] & L'' \\
K' \arrow[dr, dash, "\text{abelian}"'] & L \arrow[d, dash, "\text{abelian}"] \\
 & K
\end{tikzcd}$$

L/K abelian of exponent $\mid p$

$\Rightarrow LK'/K'$ abelian of exponent $\mid p$

$\Rightarrow LK' \subset L'$

$K' \cap L = K$

$\Rightarrow K'$ and L are lin. disjoint over K.

$\Rightarrow \mathrm{Gal}(LK'/K) \cong \underbrace{\mathrm{Gal}(L/K) \times \mathrm{Gal}(K'/K)}_{\text{abelian!}}$, $\mathrm{Gal}(K'/K) = \Delta$

$\uparrow$ $\mathrm{Gal}(L'/K)$

$$\begin{tikzcd}
\mathrm{Gal}(L'/K') \arrow[rr, two heads] \arrow[dr] & \arrow[d, phantom, "\cong"] & \mathrm{Gal}(L/K) \\
 & \mathrm{Gal}(L'/K')_\Delta \arrow[ur] &
\end{tikzcd}$$

Let $L'/L''/LK'$ be the intermediate field with $\mathrm{Gal}(L''/K') = \mathrm{Gal}(L'/K')_\Delta$.

$\Rightarrow LK' \subset L''$.

Claim: $L'' = LK'$. Proof: $\mathrm{Gal}(L''/K)$ is an extension of $\mathrm{Gal}(L''/K')$ and Δ

$\Rightarrow$ abelian $\Rightarrow \mathrm{Gal}(L''/K) \cong \mathrm{Gal}(L''/K') \times \Delta$.

$\Rightarrow \exists \tilde{L} \subset L''$ with $\mathrm{Gal}(L''/\tilde{L}) \cong \Delta$ and $\mathrm{Gal}(\tilde{L}/K) \cong \underbrace{\mathrm{Gal}(L''/K')}_{\text{abelian of exponent } \mid p}$.

$\Rightarrow \tilde{L} = L$ and $LK' = L''$. $\underline{\text{qed}}$.

So $\mathrm{Gal}(L/K) \overset{\sim}{=} \mathrm{Gal}(LK'/K') = \mathrm{Gal}(L''/K') = \mathrm{Gal}(L'/K')_\Delta$.

10.4.3 $\Rightarrow$ $\overset{\sim}{=} \mathrm{Hom}(K'^{\times}, \mu_p)_\Delta$

11.6 Abelian extensions of $\mathbb{Q}_p$

Fix a prime number p.

Proposition 11.6.1: For any $m \geqslant 1$ and any primitive p^m-th root of unity ζ we have:

(a) $\mathbb{Q}_p(\mu_{p^m})/\mathbb{Q}_p$ is totally ramified of degree $(p-1)p^{m-1}$.

(b) $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^m})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$.

(c) $\mathbb{Z}_p[\zeta]$ is the valuation ring of $\mathbb{Q}_p(\mu_{p^m})$.

(d) $1-\zeta$ is a prime element of $\mathbb{Z}_p[\zeta]$ with norm p.

Recall: $\mathbb{Q}(\mu_{p^m})/\mathbb{Q}$ is galois with group $\cong (\mathbb{Z}/p^m\mathbb{Z})^\times$

(p) is totally ramified, $(p) = (1-\zeta)^{p^{m-1}\cdot(p-1)}$

$\mathcal{O}_{\mathbb{Q}(\mu_{p^m})} = \mathbb{Z}[\zeta]$

Proposition 11.6.2: The maximal abelian extension L of $\mathbb{Q}_p$ whose galois group has exponent p has degree p^3 if $p = 2$, respectively p^2 if $p > 2$.

Proof: $p=2$: $\mathrm{Gal}(L/\mathbb{Q}_p) \cong \mathrm{Hom}(\mathbb{Q}_p^\times, \mu_p) = \mathrm{Hom}(\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2, \mu_2)$

$$\mathbb{Q}_2^\times = 2^{\mathbb{Z}} \times \mu_2 \times \underbrace{(1+4\mathbb{Z}_2)}_{\text{iso via exp, log}} \qquad \cong \mathrm{Hom}_{\mathbb{F}_2}(\mathbb{F}_2^3, \mathbb{F}_2) \cong \mathbb{F}_2^3.$$

$4\mathbb{Z}_2$

$$\Rightarrow \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong C_2 \times C_2 \times C_2$$

$p>2$: $K' := \mathbb{Q}_p(\mu_p)$, $\Delta' := \mathrm{Gal}(K'/\mathbb{Q}_p) \cong \mathbb{F}_p^\times$

$$\mathcal{O}_{K'} = \mathbb{Z}_p[\zeta] \supset \mathfrak{m} = (1-\zeta)$$

$$(K')^\times = (1-\zeta)^{\mathbb{Z}} \times \mu_{p-1} \times \mu_p \times (1+\mathfrak{m}^2)$$

$$\Rightarrow (K')^\times/((K')^\times)^p \cong C_p \times 1 \times \mu_p \times \mathfrak{m}^2/p\cdot\mathfrak{m}^2$$

$1 + 0 + 1 + p-1$

$=$ an $\mathbb{F}_p$-vector space of dimension $p+1$.

$$\Rightarrow \mathrm{Hom}((K')^\times, \mu_p) = \ldots$$

$$\mathrm{Gal}(L/\mathbb{Q}_p) \cong \mathrm{Hom}((K')^\times, \mu_p)_\Delta = \mathbb{F}_p\text{-space of dim} \le p+1.$$

$$1+\mathfrak{m}^2 \underset{\exp}{\overset{\log}{\rightleftarrows}} \mathfrak{m}^2 \quad (\sim)$$

$\mathcal{O}_{K'} \cong \mathbb{Z}_p^{p-1}$ as $\mathbb{Z}_p$-module

$\Rightarrow \mathfrak{m}^2 \cong \mathbb{Z}_p^{p-1}$ ....