Basic Facts and Notations

(Version of 9/11/04)

1 Places, Decomposition Groups and Normalised Absolute Values

1.1 Definition of Places

A place v of a number field k can be defined as 'equivalence classes of non-trivial absolute values of k'

More concretely, we define 3 types of place:

v **finite:** $v = \mathfrak{p}$ where $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_k$

v **infinite, real** $v = \iota$ where $\iota : k \to \mathbb{C}$ and $\iota(k) \subset \mathbb{R}$

v **infinite, complex** $v = \{\iota, \bar{\iota}\}$ where $\iota : k \to \mathbb{C}$ and $\iota(k) \not\subset \mathbb{R}$ (so $\bar{\iota} :=$ cx. conj. $\circ\, \iota \neq \iota$)

1.2 Places above Places

Suppose v is a place of k and L/k finite. A place w of L divides (or lies above) v as follows:

- $v = \mathfrak{p}$ is finite, then $w|v \Leftrightarrow w = \mathfrak{P}$ for some prime $\mathfrak{P}|\mathfrak{p}$ in L
- $v = \iota$ or $\{\iota, \bar{\iota}\}$ is infinite, then $w|v \Leftrightarrow w = \iota$ or $\{\tilde{\iota}, \bar{\tilde{\iota}}\}$ for some $\tilde{\iota} : L \to \mathbb{C}$ extending ι

Note: v real $\Rightarrow w$ real or complex, but v complex $\Rightarrow w$ complex

1.3 Galois Action

Assume L/k Galois. Then $\Rightarrow \mathrm{Gal}(L/k)$ acts on places of L as follows:

- $w = \mathfrak{P}$ implies $g(w) = g(\mathfrak{P})\ \forall\, g \in \mathrm{Gal}(L/k)$
- $w = \tilde{\iota}$ (*resp.* $\{\tilde{\iota}, \bar{\tilde{\iota}}\}$) implies $g(w) = \tilde{\iota} \circ g$ (*resp.* $\{\tilde{\iota} \circ g, \bar{\tilde{\iota}} \circ g\}$) for all $g \in \mathrm{Gal}(L/k)$
- orbits of $\mathrm{Gal}(L/k)$ are sets $\{w : w|v\}$ for places v of L

1.4 Decomposition Groups

- Decomposition subgroup $D_w(L/k) \subset \mathrm{Gal}(L/k)$ is stabiliser $\{g \in \mathrm{Gal}(L/k) \,:\, gw = w\}$
- $D_{hw}(L/k) = hD_w(L/k)h^{-1}$

Assuming henceforth $\mathrm{Gal}(L/k)$ *is abelian*, we can write $D_v(L/k)$ $(= D_w(L/k)\ \forall\, w|v)$

$$D_v(L/k) = \{1\} \Leftrightarrow \#\{w : w|v\} = [K : k] \Leftrightarrow v \text{ 'splits (completely)' in } L$$

• v infinite $\Rightarrow D_v(L/k) = \{1\}$ *unless* $v = \iota$ is real and $w = \{\tilde{\iota}, \bar{\tilde{\iota}}\}$ is complex for some (hence all) $w|v$

In the latter case $D_v(L/k) = \{1, \tau_w\}$ where τ_w satisfies $\bar{\tilde{\iota}} = \tilde{\iota} \circ \tau_w$ *i.e.* $\tau_w =$ *complex conjugation at* w (depends only on v since ab.)

• $v = \mathfrak{p}$ finite, $\mathfrak{p} \notin S_{\mathrm{ram}}(L/K) \Rightarrow D_v(L/k) = \langle \sigma_{\mathfrak{p},L/k} \rangle$

• If $L \supset L' \supset k$ then the restriction map $\pi_{L/L'} : \mathrm{Gal}(L/k) \to \mathrm{Gal}(L'/k)$ sends $D_v(L/k)$ *onto* $D_v(L'/k)$.

1.5 Cyclotomic Example

$D_\infty(K_f/\mathbb{Q}) = \{1, \sigma_{-\bar{1}}\}$

If p prime, $f = p^t f'$, $p \nmid f'$ then all primes above p ramify totally in $K_f/K_{f'}$

$\Rightarrow D_p(K_f/\mathbb{Q}) \supset \mathrm{Gal}(K_f/K_{f'})$

$\Rightarrow D_p(K_f/\mathbb{Q}) = \{\sigma_{\bar{a}} \in G_f \,:\, a \equiv p^i \pmod{f'} \text{for some } i \in \mathbb{Z}\}$

1.6 Normalised Absolute Values

For a place w of a number field k, the associated *normalised* absolute value $|\cdot|_v$ on k is defined by $|0|_v = 0$ and, for $a \in k^\times$:

$$|a|_v := \begin{cases} N\mathfrak{p}^{-\mathrm{ord}_{\mathfrak{p}}(a)} & \text{if } v = \mathfrak{p} \text{ (non-zero prime ideal of } \mathcal{O}_k) \\ |\iota(a)| & \text{if } v = \iota \text{ is real} \\ |\iota(a)|^2 = |\iota(a)||\bar{\iota}(a)| & \text{if } v = \{\iota, \bar{\iota}\} \text{ is complex} \end{cases}$$

• $|\cdot|_v$ obeys the triangle inequality and restricts to a homomorphism $k^\times \to \mathbb{R}^\times_{>0}$

• If $a \in k^\times$ then $|a|_v = 1$ for all but finitely many v and clearly

$$\prod_{v \text{ finite}} |a|_v = (Na\mathcal{O}_k)^{-1} = |N_{k/\mathbb{Q}}(a)|^{-1} = \left(\prod_{v \text{ infinite}} |a|_v \right)^{-1}$$

hence the *Product Formula*

$$\prod_v |a|_v = 1 \qquad \forall a \in k^\times$$

• $|a|_v = 1 \ \forall v \Leftrightarrow a \in \mu(k)$ (roots of unity in k)

• If L/k is finite and v is a place of k then for all $b \in L$

$$|N_{L/k}(b)|_v = \prod_{w|v} |b|_w$$

and for all $a \in$ k
$$|a|_w = |a|_v^{[L_w:k_v]}$$
where L_w, k_v are the *completions* at $|\cdot|_w$, $|\cdot|_v$ (so $L_w \supset k_v$)

More concretely: $[L_w : k_v] = e_{\mathfrak{P}}(L/k) f_{\mathfrak{P}}(L/k)$ if $v = \mathfrak{p}$, $w = \mathfrak{P}$ while $L_w = \mathbb{R}$ if w is real, $L_w = \mathbb{C}$ if w is complex (same for k_v).

• If L/k is Galois and w is a place of L then $|gb|_{gw} = |b|_w \ \forall b \in L, \ g \in \mathrm{Gal}(L/k)$

Alternatively, $|gb|_w = |b|_{g^{-1}w} \ \forall b \in L, \ g \in \mathrm{Gal}(L/k)$

2 Global Class Field Theory

2.1 Cycles and Ray-Class groups

• Let k be a number field. A *cycle* $\mathfrak{m}$ for k is a formal product over all the places v of k
$$\mathfrak{m} = \prod_v v^{n_v} \quad \text{where } n_v \in \begin{cases} \mathbb{Z}_{\geq 0} & \text{if } v = \mathfrak{p} \text{ (non-zero prime ideal of } \mathcal{O}_k) \\ \{1, 0\} & \text{if } v \text{ is real} \\ \{0\} & \text{if } v = \text{is complex} \end{cases}$$
and n_v=0 for all but finitely many places v (write $v|\mathfrak{m}$ iff $n_v > 0$)

• Alternatively we can think of $\mathfrak{m}$ as
$$\mathfrak{m} = \prod_{v \text{ finite}} v^{n_v} \prod_{v \text{ real}} v^{n_v} = \mathfrak{f}\mathfrak{z}$$
where $\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ is a non-zero ideal of $\mathcal{O}_k$ and $\mathfrak{z}$ can also be thought of as as the *set* of real places dividing $\mathfrak{m}$ (*i.e.* with $n_v = 1$).

• For any such cycle $\mathfrak{m} = \mathfrak{f}\mathfrak{z}$ we define a subgroup of the group $I(k)$ of fractional ideals of k
$$I_{\mathfrak{f}} = I_{\mathfrak{f}}(k) := \{\text{fractional ideals of } k \text{ prime to } \mathfrak{f}\}$$
and a subgroup of the group $P(k)$ of principal fractional ideals of k
$$P_{\mathfrak{m}} = P_{\mathfrak{m}}(k) := \{a\mathcal{O}_k \ : \ a \in k^\times, \ \mathrm{ord}_{\mathfrak{p}}(a-1) \geq n_{\mathfrak{p}} \ \forall \mathfrak{p}|\mathfrak{f}, \ \mathrm{sgn}_v(a) = 1 \ \forall v|\mathfrak{z}\}$$
where $\mathrm{sgn}_v(x) = \pm 1$ is the *sign* of the embedding of $x \in k^\times$ in $\mathbb{R}$ associated to a real place v.

• Example: if $\mathfrak{f} = \mathcal{O}$, $\mathfrak{z} = \varnothing$ then $I_{\mathfrak{f}}(k) = I(k) \supset P_{\mathfrak{m}} = P(k)$ and $I_{\mathfrak{f}}/P_{\mathfrak{m}} = \mathrm{Cl}(k)$ (*the class group*).

• More generally, for any $\mathfrak{m} = \mathfrak{f}\mathfrak{z}$ we have $I_{\mathfrak{f}} \supset P_{\mathfrak{m}}$ and the quotient $\mathrm{Cl}_{\mathfrak{m}}(k) := I_{\mathfrak{f}}/P_{\mathfrak{m}}$ is a finite abelian group (*the ray-class group of k modulo* $\mathfrak{m}$).

• If $\mathfrak{m}' = \mathfrak{f}'\mathfrak{z}'$ divides $\mathfrak{m} = \mathfrak{f}\mathfrak{z}$ (in the obvious sense) then the inclusion $I_{\mathfrak{f}} \hookrightarrow I_{\mathfrak{f}'}$ induces a surjective hom. $\mathrm{Cl}_{\mathfrak{m}}(k) \to \mathrm{Cl}_{\mathfrak{m}'}(k)$. In particular, $\mathrm{Cl}(k)$ is always a quotient of $\mathrm{Cl}_m(k)$.

2.2 Artin Maps and Conductors

Now suppose that K is an abelian extension of k with group G and that $\mathfrak{f}$ is divisible by all prime ideals ramified in K/k

• Then for every prime ideal $\mathfrak{p} \nmid \mathfrak{f}$ there is a well-defined *Frobenius* element $\sigma_{\mathfrak{p}} = \sigma_{\mathfrak{p},K/k} \in G$ and the *Artin map* is the homorphism

$$\begin{array}{rcrcl} \sigma_{K/k} & : & I_{\mathfrak{f}}(k) & \longrightarrow & G \\ & & \mathfrak{a} & \longmapsto & \sigma_{\mathfrak{a},K/k} = \prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})} \end{array}$$

• The Artin map is surjective

• There exist cycles $\mathfrak{m} = \mathfrak{f}\mathfrak{z}$ with $\mathfrak{f}$ as above such that $P_{\mathfrak{m}}(k) \subset \ker \sigma_{K/k}$ so we get a surjection $\mathrm{Cl}_{\mathfrak{m}}(k) \to G$ sending $[\mathfrak{a}]$ to $\sigma_{\mathfrak{a},K/k}$. (Not injective in gen., but one can describe its kernel).

• There exists a unique minimal such cycle $\mathfrak{m}$ (w.r.t. divisibility of cycles), called *the conductor of* k and denoted $\mathfrak{m}(K/k) = \mathfrak{f}(K/k)\mathfrak{z}(K/k)$. (So $P_{\mathfrak{m}}(k) \subset \ker \sigma_{K/k} \Leftrightarrow \mathfrak{m}(K/k)|\mathfrak{m}$.)

Note: some people call $\mathfrak{f}(K/k)$ the conductor of K/k.

• $\mathfrak{p}$ divides $\mathfrak{f}(K/k)$ iff $\mathfrak{p}$ is ramified in K; v (real) divides $\mathfrak{f}(K/k)$ if one (hence every) w of K above v is complex (*i.e.* $D_v(K/k) \neq \{1\}$).