The Ideal Class Group

Definition

A domain. Let $\mathcal{M}(A) = \{0 \neq I \subseteq A \mid I \text{ ideal}\}$. Endow $\mathcal{M}(A)$ with multiplication via the usual product of ideals. Note that $\langle 1 \rangle = A$ is an identity element.

Remark

Note that $\mathcal{M}(A)$ is a monoid. Unless A is a field $\mathcal{M}(A)$ is not a group. Indeed, take $a \in A \setminus \{0\}$ not a unit. Then $\langle a \rangle I \neq A \quad \forall I \in \mathcal{M}(A)$.

Definition

Let $\mathcal{P}(A) = \{\text{non-zero principal ideals of } A\}$.

Note that $\mathcal{P}(A)$ is a submonoid of $\mathcal{M}(A)$.

Definition

everything is always commutative

Let M be a monoid. A congruence relation on M is an equivalence relation $\equiv$ s.t. $\forall I, I', J, J' \in M$ $\quad I \equiv I'$ & $J \equiv J' \implies IJ \equiv I'J'$

Let $\bar{M} = M/\equiv$. If $\equiv$ is congruence then $\bar{M}$ is also a monoid:

$$\bar{M} \times \bar{M} \longrightarrow \bar{M}$$

$$\begin{pmatrix}\text{class} \\ \text{of } I\end{pmatrix} \cdot \begin{pmatrix}\text{class} \\ \text{of } J\end{pmatrix} \longmapsto \begin{pmatrix}\text{class of} \\ IJ\end{pmatrix}$$

For $\bar{M}$ to be a group it is necessary & sufficient that $\forall I \in M$ $\exists J \in M$ s.t. $IJ \equiv 1$. Then (class of J) = (class of I)$^{-1}$.

Let $\mathcal{M}$ monoid, P submonoid. P naturally defines a congruence relation on $\mathcal{M}$:

$$I, J \in \mathcal{M} \qquad I \equiv J \iff \exists\, \alpha, \beta \in P \text{ s.t. } \alpha I = \beta J.$$

Definition

A domain. We define the relation on the monoid $\mathcal{M}(A)$ by

$$I \equiv J \iff \exists\, \alpha, \beta \in A \setminus \{0\} \text{ s.t. } \langle \alpha \rangle I = \langle \beta \rangle J.$$

By the above, $\mathcal{M}(A)/\equiv$ is a monoid which we denote by $Cl(A)$.

Claim

If A D.D then $Cl(A)$ is a group.

Proof

Take $I \in \mathcal{M}(A)$. We may assume $I \neq A$. Let $0 \neq \alpha \in I$. Then, by UFI $\langle \alpha \rangle = IJ$ for some $J \in \mathcal{M}(A)$. Or $\langle \alpha \rangle \langle 1 \rangle = \langle 1 \rangle IJ \implies IJ \equiv \langle 1 \rangle$. ∎

Definition

A D.D. The group $Cl(A)$ is called the ideal class group of A.

Lemma

A domain. $Cl(A) = \{(1)\} \iff A$ PID.

Proof

$\Leftarrow$ A PID $\Rightarrow$ $\forall I \in \mathcal{M}(A)$ $I = \langle \alpha \rangle$ that is $\langle 1 \rangle I = \langle \alpha \rangle \langle 1 \rangle$.

$\Rightarrow$ Take $I \in \mathcal{M}(A)$. Then, $\exists \alpha, \beta \in A$ $\langle \alpha \rangle I = \langle \beta \rangle$ $\Rightarrow$ $\exists \gamma \in I$ $\beta = \alpha \gamma$. We show that $I = \langle \gamma \rangle$. Indeed $\langle \gamma \rangle \subseteq I$. Take now $x \in I$. Then $\alpha x = \beta \delta$ for some $\delta \in A$.

$\Rightarrow$ $\alpha x = \alpha \gamma \delta$ $\Rightarrow$ $\alpha (x - \gamma \delta) = 0$. Since A domain, $x = \gamma \delta \in \langle \gamma \rangle$.

Consider an injective hom $\varphi: A \to B$. It induces a natural map of monoids

$$\varphi_{\mathcal{M}}: \mathcal{M}(A) \longrightarrow \mathcal{M}(B)$$
$$I \longmapsto \varphi(I)B$$

$\varphi_{\mathcal{M}}$ in turn induces a map

$$\varphi_{Cl}: Cl(A) \longrightarrow Cl(B)$$
$$\text{class of } I \longmapsto \text{class of } \varphi_{\mathcal{M}}(I)$$

as indeed, if $\alpha I = \beta J$ then $\varphi(\alpha)\varphi(I)B = \varphi(\beta)\varphi(J)B$

When $A \subseteq B$ we denote the latter map by $i_{B/A}: Cl(A) \to Cl(B)$.

Now, assume A D.D. $k = \operatorname{Frac} A$. Let L/k be a finite separable ext. B = i.c. of A in L. Recall the ideal norm map $N_{B/A}: \mathcal{M}(B) \longrightarrow \mathcal{M}(A)$.

Recall that $\forall \alpha \in B$ $\quad N_{B/A}(\alpha B) = N_{L/K}(\alpha)A$. Hence if $I, J \in \mathcal{M}(B)$ and $\alpha, \beta \in B$ then

$$\begin{aligned} N_{B/A}(\alpha I) &= N_{B/A}(\alpha)\, N_{B/A}(I) = N_{L/K}(\alpha)\, N_{B/A}(I) \\ &\parallel \\ N_{B/A}(\beta J) &= N_{B/A}(\beta)\, N_{B/A}(J) = N_{L/K}(\beta)\, N_{B/A}(J). \end{aligned}$$

So, $I \equiv J$ in $\mathcal{M}(B)$ $\Rightarrow$ $N_{B/A}(I) \equiv N_{B/A}(J)$ in $\mathcal{M}(A)$. That is, the ideal norm map induces a natural map of abelian groups

$$\begin{aligned} N_{B/A} : Cl(B) &\longrightarrow Cl(A) \\ \text{class of } I &\longmapsto \text{class of } N_{B/A}(I) \end{aligned}$$

Note further that $N_{B/A} \circ i_{B/A} : Cl(A) \longrightarrow Cl(A)$ maps class of $I \longmapsto (\text{class of } I)^{[L:K]}$.