Algebraic number theory Assignment 03

N'Dah Jean KOUAGOU

January 26, 2019

$d = 58$.
d and $-d$ are not $1 (mod\ 4)$. So we consider the two rings $A = \mathbb{Z}[\sqrt{58}]$ and $B = \mathbb{Z}[\sqrt{-58}]$.

Class group $Cl(A)$

Minkowski bound: $1 \times \sqrt{58} \simeq 7.62 \leq 8$.
So $Cl(A)$ is generated by prime ideals of norm at most 7. Then we consider the prime numbers $2, 3, 5$ and 7.
• 2
$58 \equiv 0 (mod\ 2)$, 0 is a square. So we consider the homomorphism:

$h_2 : \mathbb{Z}[\sqrt{58}] \to \mathbb{Z}/2\mathbb{Z}$
$a + b\sqrt{58} \mapsto \bar{a} + \bar{b}.\bar{0} = \bar{a}$.
We have $P_2 = ker\ h_2 = (2, \sqrt{58})$ and $(2) = P_2^2$

• 3
$58 \equiv 1 (mod\ 3)$, 1 is a square. So we consider the two homomorphisms:

$h_3 : \mathbb{Z}[\sqrt{58}] \to \mathbb{Z}/3\mathbb{Z}$
$a + b\sqrt{58} \mapsto \bar{a} + \bar{b}.\bar{1} = \bar{a} + \bar{b}$

$h'_3 : \mathbb{Z}[\sqrt{58}] \to \mathbb{Z}/3\mathbb{Z}$
$a + b\sqrt{58} \mapsto \bar{a} + \bar{b}.(\bar{-1}) = \bar{a} - \bar{b}$.
We have $P_3 = ker\ h_3 = (3, \sqrt{58} - 1)$ and $Q_3 = ker\ h'_3 = (3, \sqrt{58} + 1)$. So $(3) = P_3 Q_3$

• 5
$58 \equiv 3 (mod\ 5)$, 3 is not a square (mod 5). Thus 5 is inert.

• 7 $58 \equiv 1 (mod\ 3)$, 1 is a square. So we consider the two homomorphisms:

$h_7 : \mathbb{Z}[\sqrt{58}] \to \mathbb{Z}/7\mathbb{Z}$
$a + b\sqrt{58} \mapsto \bar{a} + \bar{b}.\bar{3} = \bar{a} + \bar{3}\bar{b}$

$h'_7 : \mathbb{Z}[\sqrt{58}] \to \mathbb{Z}/7\mathbb{Z}$
$a + b\sqrt{58} \mapsto \bar{a} + \bar{b}.(\bar{-3}) = \bar{a} - \bar{3}\bar{b}$
We have $P_7 = ker\ h_7 = (7, \sqrt{58} - 3)$ and $Q_7 = ker\ h'_7 = (7, \sqrt{58} + 3)$. So $(7) = P_7 Q_7$

The irreducible polynomial of $\sqrt{58}$ in $\mathbb{Z}[X]$ is $f = X^2 - 58$.
We consider the table below giving the norm $N(k - \sqrt{58})$ of some $k \in \mathbb{Z}$:

k	2	3	4	8
f(k)	-54	-49	-42	6
f(k)	$-1 \cdot 2 \cdot 3^3$	$-1 \cdot 7^2$	$-1 \cdot 2 \cdot 3 \cdot 7$	$2 \cdot 3$

From the table we have:
• $(8 - \sqrt{58})(8 + \sqrt{58}) = P_2^2 P_3 Q_3$. Moreover $h'_3(8 - \sqrt{58}) = 0$.
So $8 - \sqrt{58} \in Q_3$ and we have $(8 - \sqrt{58}) = P_2 Q_3$.
It follows that $[P_2] + [Q_2] = 0$ and we can delete Q_3 from the generators.
Since $[P_3] + [Q_3] = 0$ we also delete P_3 from the generators.
• $(4 - \sqrt{58})(4 + \sqrt{58}) = P_2^2 P_3 Q_3 P_7 Q_7$

As in the previous case, $4-\sqrt{58}$ is an element of P_3, and Q_7.
So $(4-\sqrt{58}) = P_2P_3Q_7$, implying $[P_2]+[P_3]+[Q_7]=0$ and $[Q_7]=-[P_2]-[P_3]$. Then we delete Q_7 and P_7 from the generators.
As a result, P_3, Q_3, P_7, Q_7 have been deleted from the list of generators.
Therefore the only remaining generator is $P_2 = (2, \sqrt{58})$.
Now shall check if P_2 is principal.
Suppose it is the case. Then, either $\sqrt{58}$ is a multiple of 2 in which case $P_2 = (2)$, either (2) is a multiple of $\sqrt{58}$ in which case $P_2 = (\sqrt{58})$.

- If $\sqrt{58}$ is a multiple of 2, there is $\alpha = a + b\sqrt{58} \in \mathbb{Z}[\sqrt{58}]$ such that $\sqrt{58} = 2\alpha$.

Then:

$$\begin{aligned}
&\sqrt{58} = 2(a+b\sqrt{58}) \\
&\quad \Rightarrow \begin{cases} \sqrt{58} = 2b\sqrt{58} \\ 0 = 2a \end{cases} \\
&\quad \Rightarrow \begin{cases} 2b = 1 \\ 0 = 2a, \text{ there is a contradiction because } b \in \mathbb{Z} \end{cases}
\end{aligned}$$

- If 2 is a multiple of $\sqrt{58}$, there is $\beta = c + d\sqrt{58} \in \mathbb{Z}[\sqrt{58}]$ such that $2 = \beta\sqrt{58}$.

Then:

$$\begin{aligned}
&2 = \sqrt{58}(c+d\sqrt{58}) \\
&\Rightarrow 2 = c\sqrt{58} + 58d \\
&\Rightarrow \begin{cases} c\sqrt{58} = 0 \\ 58d = 2 \end{cases} \\
&\Rightarrow \begin{cases} c = 0 \\ 58d = 2, \text{ there is a contradiction because } d \in \mathbb{Z} \end{cases}
\end{aligned}$$

Therefore P_2 is not principal and since $P_2^2 = (2)$ is principal then $[P_2]$ is of order 2 in $Cl(A)$.
We conclude that $Cl(A) =< [P_2] >$ is a group of order 2 and is therefore isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Unit group A^*

From the table, we have $N(2-\sqrt{58}) = -2 \times 3^3$. So $(2-\sqrt{58})(2+\sqrt{58}) = P_2^2P_3^3Q_3^3$.
But $h'_3(2-\sqrt{58}) = 0$ and so $2-\sqrt{58} \in Q_3$.
Thus $(2-\sqrt{58}) = P_2Q_3^3$ and then $(2)(2-\sqrt{58}) = (4-2\sqrt{58}) = P_2^2P_2Q_3^3 = P_2^3Q_3^3$.
We saw above that $(8-\sqrt{58}) = P_3Q_3$. So $(4-2\sqrt{58}) = (8-\sqrt{58})^3$.
It follows that $\frac{(8-\sqrt{58})^3}{4-2\sqrt{58}}$ is a unit.
Let's compute that unit. We have:

$$\begin{aligned}
\frac{(8-\sqrt{58})^3}{4-2\sqrt{58}} &= \frac{(64-16\sqrt{58}+58)(8-\sqrt{58})}{4-2\sqrt{58}} \\
&= \frac{1904-250\sqrt{58}}{4-2\sqrt{58}} \\
&= \frac{(1904-250\sqrt{58})(4+2\sqrt{58})}{-216} \\
&= -\frac{7616+3808\sqrt{58}-1000\sqrt{58}-29000}{216} \\
&= \frac{21384-2808\sqrt{58}}{216} \\
&= 99-13\sqrt{58}
\end{aligned}$$

Verification:

$$\begin{aligned}
(99-13\sqrt{58}) \times (99+13\sqrt{58}) &= 99^2 - 13^2 \times 58 \\
&= 9801 - 9802 \\
&= -1
\end{aligned}$$

We conclude that
$$A^* = \left\{ \pm \epsilon^k : k \in \mathbb{Z} \right\}, \quad \text{with } \epsilon = 99 - 13\sqrt{58}$$
.

Class group $Cl(B)$

Minkowski bound: $\frac{4}{\pi} \times \sqrt{58} \simeq 9.7 \leq 10$.
So $Cl(B)$ is generated by prime ideals of norm at most 9. Then we consider the prime numbers $2, 3, 5$ and 7.
• 2
$-58 \equiv 0(mod\ 2)$, 0 is a square. So we consider the homomorphism:

$H_2 : \mathbb{Z}[\sqrt{-58}] \to \mathbb{Z}/2\mathbb{Z}$
$a + b\sqrt{-58} \mapsto \bar{a} + \bar{b}.\bar{0} = \bar{a}$.
We have $P_2 = ker\ H_2 = (2, \sqrt{-58})$ and $(2) = P_2^2$

• 3
$-58 \equiv 2(mod\ 3)$, 2 is not a square (mod 3). So 3 is inert.

• 5
$-58 \equiv 2(mod\ 5)$, 2 is not a square (mod 5). So 5 is inert.

• 7
$-58 \equiv 5(mod\ 7)$, 5 is not a square (mod 7). So 7 is inert.
So $Cl(B)$ is generated by $P_2 = (2, \sqrt{-58})$.
Let's check if P_2 is principal.
Suppose P_2 is principal. Then, either $\sqrt{-58}$ is a multiple of 2 in which case $P_2 = (2)$, either (2) is a multiple of $\sqrt{-58}$ in which case $P_2 = (\sqrt{-58})$.
• If $\sqrt{58}$ is a multiple of 2, there is $\alpha = a + b\sqrt{-58} \in \mathbb{Z}[\sqrt{-58}]$ such that $\sqrt{-58} = 2\alpha$.
Then:

$$\begin{aligned} \sqrt{-58} &= 2(a + b\sqrt{-58}) \\ &\Rightarrow \begin{cases} \sqrt{-58} = 2b\sqrt{-58} \\ 0 = 2a \end{cases} \\ &\Rightarrow \begin{cases} 2b = 1 \\ 0 = 2a, \text{ there is a contradiction because } b \in \mathbb{Z} \end{cases} \end{aligned}$$

• If 2 is a multiple of $\sqrt{-58}$, there is $\beta = c + d\sqrt{-58} \in \mathbb{Z}[\sqrt{-58}]$ such that $2 = \beta\sqrt{-58}$.
Then:

$$\begin{aligned} 2 &= \sqrt{-58}(c + d\sqrt{-58}) \\ &\Rightarrow 2 = c\sqrt{-58} - 58d \\ &\Rightarrow \begin{cases} c\sqrt{-58} = 0 \\ -58d = 2 \end{cases} \\ &\Rightarrow \begin{cases} c = 0 \\ -58d = 2, \text{ there is a contradiction because } d \in \mathbb{Z} \end{cases} \end{aligned}$$

Therefore P_2 is not principal and since $P_2^2 = (2)$ is principal then $[P_2]$ is of order 2 in $Cl(B)$.
We conclude that $Cl(B) =< [P_2] >$ is a group of order 2 and is therefore isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Unit group B^*

Let $X = x + y\sqrt{-58} \in B$.
Note in our case the norm is positive.

So we have:

$$\begin{aligned} X \in B^* &\Leftrightarrow N(X) = 1 \\ &\Leftrightarrow x^2 + 58y^2 = 1 \\ &\Leftrightarrow \begin{cases} x = \pm 1 \\ y = 0 \end{cases} \\ &\Leftrightarrow X = \pm 1 \end{aligned}$$

We conclude that

$$\boxed{B^* = \left\{ \pm 1 \right\}}$$