Computing class groups

Notation: Given a nb field K, let $M_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\Delta(K)|}$

where $n = [K:\mathbb{Q}]$

$2r_2 = \#$ of nonreal $K \hookrightarrow \mathbb{C}$

$\Delta(K) =$ disc. of K.

M_K: "Minkowski constant"

$Cl(K)$: class group of K

$N(\mathfrak{a})$: absolute norm of $\mathfrak{a}$

$N_{K/\mathbb{Q}}(\alpha)$: norm of $\alpha \in K$

$h_K = \# Cl(K)$: class nb of K.

$C_n =$ cyclic group of order n

$[I]$: class of the fractional ideal I in $Cl(K)$

ex.: ① $K = \mathbb{Q}(\sqrt{5})$

Then $M_K = 1.118\ldots$

so $M_K < 2$, & every $[\mathfrak{a}] \in Cl(K)$ is represented by an integral ideal I of norm $N(I) \leq M_K < 2$.

So $I = \mathcal{O}_K$. So $[\mathfrak{a}] = 1$ & $\boxed{Cl(K) = 1}$

ex.: ② $K = \mathbb{Q}(\sqrt{-5})$

Then $M_K = 2.84\ldots$

So, only $p < M_K$ is $p = 2$

$\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, so to factor $p=2$ in $\mathcal{O}_K$

look at $x^2+5 \pmod 2$

$x^2+5 = x^2+1 = (x+1)^2$

so $2\mathcal{O}_K = (2, 1+\sqrt{-5})^2$

so $N((2, 1+\sqrt{-5})) = N(2\mathcal{O}_K)^{1/2} = 4^{1/2} = 2$

Is $I = (2, 1+\sqrt{-5})$ principal?

If so $\exists \alpha \in I$ s.t. $|N_{K/\mathbb{Q}}(\alpha)| = N(I) = 2$.

$N_{K/\mathbb{Q}}(a+b\sqrt{-5}) = a^2+5b^2 \stackrel{?}{=} 2$

Then $b=0$ so $a^2=2$. Nope!

so I is not principal, so $h_K = 2$, so $\boxed{Cl(K) \cong C_2}$

ex.: ③ $K = \mathbb{Q}(\sqrt{-10})$

$M_K = 4.026\ldots$

so $p < M_K$ are $p = 2, 3$

$\mathcal{O}_K = \mathbb{Z}[\sqrt{-10}]$, so to factor $p=2$ in $\mathcal{O}_K$

look at $x^2+10 \pmod 2$

$x^2+10 = x^2$

so $2\mathcal{O}_K = (2, \sqrt{-10})^2$. Let $I = (2, \sqrt{-10})$

so $N(I) = 4^{1/2} = 2$. $N(a+b\sqrt{-10}) = a^2+b^2 \cdot 10$ so no elements of norm 2, so I is not principal ex.: (3) (cont'd) What about $p=3$?

$\Delta(K)=-40$: $\left(\frac{-40}{3}\right)=\left(\frac{-1}{3}\right)\left(\frac{2}{3}\right)\left(\frac{5}{3}\right)$

$=\left(\frac{-1}{3}\right)\left(\frac{2}{3}\right)^2=\left(\frac{-1}{3}\right)=-1$

so 3 is inert in K, so $3\mathcal{O}_K$ is prime

& $N(3\mathcal{O}_K)=9>M_K$. So nothing to check

& $h_K=2$, so $\boxed{Cl(K)=C_2}$

ex.: (4) $K=\mathbb{Q}(\sqrt{-11})$

$M_K=2.111\ldots$ $\quad\Delta(K)=-11$: $\left(\frac{-11}{2}\right)=-1$ since $-11\equiv 5 \pmod 8$

so only $p=2<M_K$. $\quad$ so 2 is inert, so $2\mathcal{O}_K$ is prime & $N(2\mathcal{O}_K)=4>M_K$. (& principal anyway)

~~$\mathcal{O}_K=\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$, so to factor $p=2$, can't look at $x^2+11 \pmod 2$,~~
~~need to look at $x^2-x+3 \pmod 2$ (This is the min. poly. of $\frac{1+\sqrt{-11}}{2}$). $=x^2+x+1$. Irred~~

~~$x^2-x=x(x-1)$~~

~~so $2\mathcal{O}_K=\left(2,\frac{1+\sqrt{-11}}{2}\right)\left(2,\frac{1+\sqrt{-11}}{2}\right)$. Need to check I_1 & I_2 since $N(I_1)N(I_2)=N(2)=4$~~
~~so $N(I_1)=2$~~

~~Is there $\alpha\in I_1$ with $N(\alpha)=N(I_1)=2$?~~

~~$N\left(a+b\left(\frac{1+\sqrt{-11}}{2}\right)\right)$~~

so nothing to check! $h_K=1$, $\boxed{Cl(K)=1}$

ex.: (5) $K=\mathbb{Q}(\sqrt{-163})$

$M_K=8.127\ldots$

so check $p=2,3,5,7$. $\Delta(K)=-163$. We'll see that these p are all inert. Since inert primes are principal, there's nothing to check & $\boxed{h_K=1}$

$\left(\frac{-163}{2}\right)=-1$ since $-163\equiv -3\ (8)$

$\left(\frac{-163}{3}\right)=\left(\frac{-10}{3}\right)=\left(\frac{2}{3}\right)=-1$

$\left(\frac{-163}{5}\right)=\left(\frac{-3}{5}\right)=\left(\frac{2}{5}\right)=-1$

$\left(\frac{-163}{7}\right)=\left(\frac{-23}{7}\right)=\left(\frac{5}{7}\right)=\left(\frac{7}{5}\right)=\left(\frac{2}{5}\right)=-1$.

ex.: (6) $K=\mathbb{Q}(\sqrt[3]{2})$

$M_K = 2.94\ldots$

so only $p=2 < M_K$.

$\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ so look at $x^3-2 \pmod 2$ $= x^3 \pmod 2$

so $2\mathcal{O}_K = (2, \sqrt[3]{2})^3$

since $2=(\sqrt[3]{2})^3$

Clearly, $(2,\sqrt[3]{2}) = (\sqrt[3]{2})$

so $\boxed{h_K = 1}$

ex: (7) $K=\mathbb{Q}(\sqrt{-23})$

$M_K = 3.05$ $\Delta(K) = -23$, so $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$

so $p=2,3 < M_K$. so must look at $x^2-x+6 \pmod 2$ to factor $p=2$

$x^2-x+6 \equiv x^2-x \equiv x(x-1) \pmod 2$

so $2\mathcal{O}_K = \underbrace{\left(2, \frac{1+\sqrt{-23}}{2}\right)}_{I_1}\underbrace{\left(2, \frac{-1+\sqrt{-23}}{2}\right)}_{I_2}$

for $p=3$, $x^2+23 \bmod 3$ $\equiv x^2-1 = (x+1)(x-1)$

so $3\mathcal{O}_K = \underbrace{(3, 1+\sqrt{-23})}_{J_1}\underbrace{(3, -1+\sqrt{-23})}_{J_2}$

Are J_k, I_k principal? $N(I_k)=2$ $N(J_k)=3$, $N_{K/\mathbb{Q}}\left(a+b\frac{1+\sqrt{-23}}{2}\right) = a^2+ab+6b^2$

The quadratic form $Q(x,y) = x^2+xy+6y^2$ is (pos. def.) reduced in the sense of Gauss & hence in the sense of Minkowski, Thus 1 (= the coeff. of x^2) is the least norm & 6 (= the coeff of y^2) is the least norm of a vector v_2, s.t. $\{v_1, v_2\}$ is a basis of $\mathbb{Z}^2$ & $\|v_1\| \le \|v_2\|$. So if $v \in \mathbb{Z}^2$ has norm <6, then $v = (\pm 1, 0)$ & $\|v\|=1$, or $v=(x,y)$ with $\gcd(x,y)>1$, so $Q(x,y)$ is divisible by a square. Thus $\mathcal{O}_K$ has no elements of norm 2 or 3 & I_k & J_k are <u>not</u> princ.

For an alternate proof that I_k and J_k are not principal, see page 5.

$J_1J_2 = (3)$ & $I_1I_2 = (2)$ so $[I_2] = [I_1]^{-1}$ & $[J_2] = [J_1]^{-1}$

<u>Claim</u>: $[J_2] = [I_1]^{-1}$ & $[J_2] = [I_2]^{-1}$

proof: $I_kJ_k = \left(2, \frac{\pm 1+\sqrt{-23}}{2}\right)\left(3, \pm 1+\sqrt{-23}\right) = \left(6, (\pm 1+\sqrt{-23})\cdot 2, \left(\frac{\pm 1+\sqrt{-23}}{2}\right)\cdot 3, \frac{(\pm 1+\sqrt{-23})^2}{2}\right)$

now, since $\left|N_{K/\mathbb{Q}}\left(\frac{\pm 1+\sqrt{-23}}{2}\right)\right| = 6$, $\frac{\pm 1+\sqrt{-23}}{2}$ divides 6, & hence every generator of I_kJ_k, so $\left(\frac{\pm 1+\sqrt{-23}}{2}\right) \supseteq I_kJ_k$. Both have norm 6, so they are equal.

Therefore $I_K J_K$ is principal so $[I_K][J_K]=1$. QED

Thus there are at most 3 classes in $Cl(K)$. And there are at least 2.

By the structure of groups of orders 2 & 3, it suffices to check if $[I_1]^3=1$ or $[I_1]$

Claim: $[I_1]^3 = 1$

proof: $N(I_1^3)=8$, so if we want I_1^3 to be principal there better be elements of norm 8.

There are 4: $\pm\frac{3}{2} \pm \frac{\sqrt{-23}}{2}$. Let $\theta = -\frac{3}{2} + \frac{\sqrt{-23}}{2}$

Note that & $\frac{1+\sqrt{-23}}{2} - 2 = \theta$. So $I_1 = (2, \theta)$

So $I_1^3 = (8, 4\theta, 2\theta^2, \theta^3)$. Since $|N_{K/\mathbb{Q}}\theta| = 8$, $\theta \mid 8$, so $I_1^3 \subseteq (\theta)$

$N(I_1^3) = 2^3 = 8 = |N_{K/\mathbb{Q}}(\theta)|$ so $I_1^3 = (\theta)$. QED

Therefore, $\boxed{h_K = 3,\ Cl(K) = C_3 = \langle [I_1] \rangle}$

You can find several more worked out examples in §12.6 of Alaca-Williams's book (Though they use a weaker Minkowski bound, & so do more work!) & in §6.5 of Murty-Esmonde's book.

ex: ⑦ Revisited:

Alternate answer to:

Are J_K & I_K principal?

$\mathcal{O}_K = \left\{ \frac{a}{2} + \frac{b}{2}\sqrt{-23} : a, b \in \mathbb{Z}, \ a \equiv b \pmod 2 \right\}$

$N_{K/\mathbb{Q}}\left(\frac{a + b\sqrt{-23}}{2} \right) = \frac{a^2 + 23b^2}{4}$

$N(I_K) = 2 \quad N(J_K) = 3$

If $I_K = (\alpha)$, then $N_{K/\mathbb{Q}}(\alpha) = 2$ & if $J_K = (\beta)$, then $N_{K/\mathbb{Q}}(\beta) = 3$

so try to solve $\frac{x^2 + 23y^2}{4} = 2$ or 3

$\frac{x^2+23y^2}{4} = 2 \Rightarrow x^2 + 23y^2 = 8$. If $y = 0$, $x^2 + 23y^2$ is a square so $\neq 8$

If $y \neq 0$, $x^2 + 23y^2 \geq 23 > 8$.

so $\nexists x, y \in \mathbb{Z}$ s.t. $x^2 + 23y^2 = 8$

so I_K is not principal

Similarly, $\frac{x^2+23y^2}{4} = 3 \Rightarrow x^2 + 23y^2 = 12$ & 12 is not a square & $23 > 12$

so J_K is not principal.