Infamous Property and an Application

Ferran Espuña Bertomeu

January 2, 2024

Remark. In the proof of the following claim, we use repeatedly tha fact that if $K \subset L$ is a field extension and $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ are ideals, then $(\mathfrak{a}\mathfrak{b})\mathcal{O}_L = (\mathfrak{a}\mathcal{O}_L)(\mathfrak{b}\mathcal{O}_L)$. To avoid writing this repeatedly, we will signal its uses with the color blue.

Claim 1. *Let $K \subset L$ be number fields. Let $\mathcal{P}_i \subset \mathcal{O}L_i$ be prime ideals, $\mathfrak{p}_i \coloneqq \mathcal{P}_i \cap \mathcal{O}K$ and $f_i \coloneqq f(\mathcal{P}_i \mid \mathfrak{p}_i)$. if $J \coloneqq \mathcal{P}_1^{m_1} \cdots \mathcal{P}_k^{m_k}$ is principal, then $I \coloneqq \mathfrak{p}_1^{f_1 m_1} \cdots \mathfrak{p}_k^{f_k m_k}$ is principal.*

Proof. As suggested, I have taken inspiration in the guided exercises in the book by Daniel Marcus.

We will start dealing with the case in which $L \mid K$ is Galois. In that case, for $1 \leq i \leq k$, $\mathfrak{p}_i\mathcal{O}_L = (\mathcal{P}_{i,1} \cdots \mathcal{P}_{i,g_i})^{e_i}$ where $\mathcal{P}_{i,j}$ are the primes above $\mathfrak{p}_i$ (including $\mathcal{P}_i$). Because the Galois group of the extension acts transitively on this set of primes (say, for $1 \leq j \leq g_i$, $\sigma_j(\mathcal{P}_i) = \mathcal{P}_{i,j}$), then the subset of $\mathrm{Gal}(L \mid K)$ sending $\mathcal{P}_i$ to $\mathcal{P}_{i,j}$ is $\sigma_j D_{\mathcal{P}_i|\mathfrak{p}_i}$ which has $e_i f_i$ elements. All in all, ${\mathfrak{p}_i}^{f_i}\mathcal{O}_L = (\mathfrak{p}_i\mathcal{O}_L)^{f_i} = \prod_{\sigma \in \mathrm{Gal}(L|K)} \sigma(\mathcal{P}_i)$. This means that

$$I\mathcal{O}_L = \prod_{\sigma \in \mathrm{Gal}(L|K)} \sigma(J) = \prod_{\sigma \in \mathrm{Gal}(L|K)} (\sigma(\alpha)) = \left(\prod_{\sigma \in \mathrm{Gal}(L|K)} \sigma(\alpha) \right) = (N_{L|K}(\alpha))\mathcal{O}_L$$

To finish, we just need to show that this implies $I = (N_{L|K}(\alpha))$. This is true for any two ideals of $\mathcal{O}_K$: we can reconstruct the factorization of any ideal $\mathfrak{a} \subset \mathcal{O}_K$ into primes from that of $\mathfrak{a}\mathcal{O}_L \subset \mathcal{O}_L$, because each prime in $\mathcal{O}_L$ is above a unique prime in $\mathcal{O}_K$ and always appears in its extension with a fixed exponent. Therefore, $\mathfrak{a}\mathcal{O}_L = \mathfrak{b}\mathcal{O}_L \Rightarrow \mathfrak{a} = \mathfrak{b}$.

Remark. In fact, because it is well known that $\mathfrak{a}\mathcal{O}_L = ((\mathfrak{a}\mathcal{O}_L) \cap \mathcal{O}_K)\mathcal{O}_L$, we can conclude that $\mathfrak{a} = (\mathfrak{a}\mathcal{O}_L) \cap \mathcal{O}_K$.

Now, let us consider the general case. Let M be the Galois closure of $L \mid K$. Then, $M \mid K$ is Galois, so we can apply the previous result to the ideal $(\alpha)\mathcal{O}_M$ and $M \mid K$. Let $\mathcal{P}_i\mathcal{O}_M = \mathcal{Q}_{i,1}^{\tilde{e}_i} \cdots \mathcal{Q}_{i,\tilde{g}_i}^{\tilde{e}_i}$. For a given prime $\mathcal{Q}_{i,j}$ in M above $\mathcal{P}_i$, $\mathcal{Q}_{i,j} \cap \mathcal{O}_L = \mathcal{P}_i \Rightarrow \mathcal{Q}_{i,j} \cap \mathcal{O}_K = \mathfrak{p}_i$. We get that

$$(N_{M|K}(\alpha)) = \mathfrak{p}_1^{\hat{f}_1 \tilde{e}_1 \tilde{g}_1 m_1} \cdots \mathfrak{p}_k^{\hat{f}_k \tilde{e}_k \tilde{g}_k m_k}$$

where $\hat{f}_i$ is the inertia degree of $\mathfrak{p}_i$ in $M \mid K$. We know that $\hat{f}_i = \tilde{f}_i f_i$ (where $\tilde{f}_i \coloneqq f(\mathcal{Q}_{i,j} \mid \mathcal{P}_i)$ for any j), and also $\tilde{e}_i \tilde{g}_i \tilde{f}_i = [M : N]$. All together, we get that

$$(N_{M|K}(\alpha)) = (\mathfrak{p}_1^{f_1 m_1} \cdots \mathfrak{p}_k^{f_k m_k})^{[M:N]} = I^{[M:N]}$$

However, $\alpha \in L$ so $N_{M|K}(\alpha) = N_{L|K}(N_{M|L}(\alpha)) = N_{L|K}(\alpha^{[M:L]}) = N_{L|K}(\alpha)^{[M:L]}$ so (for example, by unique factorization into primes), $I = (N_{L|K}(\alpha))$, just like in the Galois case. $\square$

Remark. Let $K = \mathbb{Q}\left(\sqrt{-23}\right)$. Because $-23 \equiv 1 \pmod 4$, $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$ and

$$\operatorname{disc}(K) = \left(\frac{1+\sqrt{-23}}{2} - \frac{1-\sqrt{-23}}{2}\right)^2 = -23$$

Furthermore, it is generated over $\mathbb{Q}$ by a complex conjugate pair of elements, so its signature is $(0,1)$. Therefore, the Minkowski bound for K is $M_K = \frac{2}{\pi}\sqrt{23} < 4$.

Claim 2. *The ideal class group of $K = \mathbb{Q}\left(\sqrt{-23}\right)$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.*

Proof. By the Minkowski bound calculated above, all ideal classes will have a representative with norm less than 4. This means that the norm of this representative (except in the trivial case of the whole ring of integers, which is principal) is 2 or 3, and therefore it is a prime ideal above 2 or 3. We will apply the Kummer-Dedekind theorem to these primes with $\alpha = \frac{1+\sqrt{-23}}{2} \Rightarrow f(X) = X^2 - X + 6$. Both modulo 2 and modulo 3, f it splits as $X(X-1)$ so our candidate primes are $\mathfrak{p}_2 = (2, \alpha)$, $\mathfrak{q}_2 = (2, \alpha - 1)$, $\mathfrak{p}_3 = (3, \alpha)$ and $\mathfrak{q}_3 = (3, \alpha - 1)$.

Notice that $[\mathfrak{p}_2\mathfrak{q}_2] = [(2)] = [(1)]$ and $[\mathfrak{p}_3\mathfrak{q}_3] = [(3)] = [(1)]$. We can also compute $\mathfrak{p}_2\mathfrak{p}_3 = (2,\alpha)(3,\alpha) = (6, 3\alpha, 2\alpha, \alpha^2) = (\alpha)$ so $[\mathfrak{p}_2\mathfrak{p}_3] = [(1)]$ and $[\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1} = [\mathfrak{q}_2] \Rightarrow [\mathfrak{q}_3] = [\mathfrak{p}_2]$. All in all, $\mathrm{Cl}(K) = \{[(1)], [\mathfrak{p}_2], [\mathfrak{q}_2]\}$. Now we only need to show that $\mathfrak{p}_2^2$ is not principal. This will mean that the order of $[\mathfrak{p}_2]$ is not 1 or 2, and therefore it is 3. The norm of $\mathfrak{p}_2$ is 2, so the norm of $\mathfrak{p}_2^2$ is 4. If it were principal, it would be generated by an element of norm 4. The norm of an element $a + b\alpha$ of $\mathcal{O}_K$ is $\left(a + \frac{b}{2} + \frac{b}{2}\sqrt{-23}\right)\left(a + \frac{b}{2} - \frac{b}{2}\sqrt{-23}\right) = a^2 + ab + 6b^2$. Equating this to 4 we get $a^2 + ab + 6b^2 = 4 \Rightarrow a^2 + ab + (6b^2 - 4) = 0 \Rightarrow a = \frac{-b \pm \sqrt{16 - 23b^2}}{2}$. The only possibility for this to be a real number is $b = 0$, but then $a = \pm 2$. However, this would mean that $\mathfrak{p}_2^2 = (2)$, which is not the case, as we have already factorized (2) as $\mathfrak{p}_2\mathfrak{q}_2$.

$\square$

Claim 3. *$L \coloneqq \mathbb{Q}(\zeta_{23})$ has $h_L \geq 3$.*

Proof. Because $23 \equiv 3 \pmod 4$, $K \coloneqq \mathbb{Q}\left(\sqrt{-23}\right)$ is a subfield of L. Following the notation in Claim 2, let us check that the order of $[\mathfrak{p}_2\mathcal{O}_L]$ in $\mathrm{Cl}(L)$ is greater than 2. To apply Claim 1, we note that $\mathfrak{p}_2$ is prime in $\mathcal{O}_K$, and because $[L:K] = \frac{22}{2} = 11$, so if $\mathfrak{p}_2\mathcal{O}_L = (\mathcal{P}_1 \cdots \mathcal{P}_g)^e$, and $f \coloneqq f(\mathcal{P}_i \mid \mathfrak{p}_2)$, then $efg = 11$. Therefore, if $(\mathfrak{p}_2\mathcal{O}_K)^m$ is principal, then $\mathfrak{p}_2^{11m}$ is principal, but we have seen that $\mathfrak{p}_2$ has order 3, so $3 \mid 11m \Rightarrow 3 \mid m$. $\square$

Remark. To do the calculations above I have used the fact that $L \mid K$ is a Galois extension. This is in fact not necessary, and we can just replace 11 by the degree of the extension (not necessarily Galois) because of the usual formula $\sum_i e_i f_i = [L:K]$.