Guiding this document are two problems:

Exercise. *Prove quadratic reciprocity by considering the splitting of a prime p in $\mathbb{Q}(\sqrt{\pm q})$.*

and

Exercise. *Construct an explicit example of a number field $K/\mathbb{Q}$ such that $\mathcal{O}_K$ is not generated by a single element.*

First, a warmup: proving the -1 case of quadratic reciprocity:

Theorem. *Let p be an odd prime. Then $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.*

Proof. Consider the ideal $p\mathbb{Z}[i] \subseteq \mathbb{Z}[i]$. Since $p \nmid 4 = \operatorname{disc}(\mathbb{Z}[i])$, we have that p is unramified, so p splits as a product

$$p\mathbb{Z}[i] = P_1 \cdots P_r$$

in $\mathbb{Z}[i]$. Then, the sum of the inertial degrees is 2 since we have a degree 2 extension. I.e. we either have $p\mathbb{Z}[i] = P_1P_2$ with $f(P_1|p) = f(P_2|p) = 1$ or else $P_1 = p\mathbb{Z}[i]$ is itself prime of inertial degree 2. In either case, we compute the inertial degree directly.

Namely, let P be a prime lying over p, and let f be the inertial degree. Then, by definition, $\mathbb{Z}[i]/P$ is a degree f extension of $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. We thus know that the Galois group is generated by the Frobenius automorphism $x \mapsto x^p$. But any map of $\mathbb{Z}[i]/P$ is determined by the image of i, and $i^p = \pm i$ with the plus sign holding iff $p \equiv 1 \pmod 4$. Thus, f, the order of the Galois group, is 1 iff $p \equiv 1 \pmod 4$.

That is, we have $p \equiv 1 \pmod 4$ iff $p\mathbb{Z}[i]$ is not prime. But we can characterize this as well:

$$\mathbb{Z}[i]/p\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1, p) \cong \mathbb{F}_p[x]/(x^2+1)$$

so $p\mathbb{Z}[i]$ is not prime iff x^2+1 is reducible in $\mathbb{F}_p$. Since it is of degree 2, this can only happen by having a root, i.e. $p \equiv 1 \pmod 4$ iff there is some $a \in \mathbb{F}_p$ with $a^2+1 = 0$, i.e. $a^2 = -1$, so -1 is a quadratic residue. This gives the result. □

The general case is similar, except that we don't have the coincidence that $\sqrt{-1} = \zeta_4$. I.e. if we adjoin a square root of $\pm q$, it may not be easy to understand its multiplicative order mod a prime in that ring, whereas understanding powers of $\sqrt{-1}$ is quite easy. This is the additional work, for which we embed in a cyclotomic field.

Theorem. *Let p, q be distinct odd primes. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.*

Proof. Let q^* denote $\pm q$ with the plus sign holding iff $q \equiv 1 \pmod 4$. Then, note that

$$K = \mathbb{Q}(\sqrt{q^*}) \subseteq \mathbb{Q}(\zeta_q) = L$$

as we've previously shown. We have $\operatorname{disc}(\zeta_q) = \pm q^{q-2}$ is not divisible by p, and so p is unramified in L, whence it is also unramified in K since ramification indices are multiplicative in towers. Since $L/\mathbb{Q}$ is Galois, $p\mathbb{Z}[\zeta_q]$ is the product of $r = (q-1)/f$ distinct primes, where f is the common inertial degree of all primes of $\mathbb{Z}[\zeta_q]$ lying over p. Fix such a prime P.

Now, we consider automorphisms of two related fields. First, we have that $\mathbb{Z}[\zeta_q]/P$ is a degree f extension of $\mathbb{F}_p$, and so the Galois group is generated again by the Frobenius map $\sigma(x) = x^p$. Second, we have an automorphism τ of $L/\mathbb{Q}$ given by $\zeta_q \mapsto \zeta_q^p$. I claim these maps have the same order in their respective groups. The order of σ is f, and let u be the order of τ.

One direction is clear. Since $\tau^u = 1$,

$$\zeta_q = \tau^u(\zeta_q) = \zeta_q^{p^u}$$

Since σ is a map from $\mathbb{Z}[\zeta_q]/P$, it is determined by the image of (the coset) $\zeta_q + P$. But

$$\sigma^u(\zeta_q + P) = \zeta_q^{p^u} + P = \zeta_q + P$$

so we must have $\sigma^u = 1$ as well. Thus $f \mid u$. Conversely, since $\sigma^f = 1$, we have $\zeta_q + P = \sigma^f(\zeta_q + P) = \zeta_q^{p^f} + P$, so $\zeta_q(\zeta_q^n - 1) \in P$ for $n = p^f - 1$. Since P is prime, one of these factors is in P, but ζ_q is a unit, so it cannot be in P. Thus $\zeta_q^n - 1 \in P$. This only depends on the residue of n mod q, and so $\zeta_q^n - 1$ is one of the terms:

$$\zeta_q^0 - 1, \zeta_q^1 - 1, \ldots, \zeta_q^{q-1} - 1$$

If it is not the first of these, then we get that the product of the remaining ones is also in P. I.e., P contains:

$$\prod_{i=1}^{q-1}(\zeta_q^i - 1) = q$$

But then P contains both p and q, and so it contains $\gcd(p,q) = 1$ since the gcd is a $\mathbb{Z}$-linear combination of its arguments, contradicting the properness of P. Thus we must have that $\zeta_q^n - 1 = \zeta_q^0 - 1 = 0$, so that

$$\tau^f(\zeta_q) = \zeta_q^{p^f} = \zeta_q^{n+1} = \zeta_q$$

so that $\tau^f = 1$. So $u \mid f$ and we get $u = f$ as claimed.

With this established, let us first consider the case that $\left(\frac{p}{q}\right) = 1$. Then τ is contained in the (unique) index 2 subgroup H of the Galois group of $L/\mathbb{Q}$. So, the fixed fields are contained in the reverse order. The fixed field of τ is the unique subfield of L of degree $(q-1)/f = r$ over $\mathbb{Q}$, and the fixed field of H is the unique subfield of L of degree 2 over $\mathbb{Q}$. The former field must be L_D, the decomposition field of P over p, and the latter must be K. So, we get that $K \subseteq L_D$. Since inertial degrees are multiplicative in towers and each prime of L_D lying over p has inertial degree 1, this gives that each prime lying over p in K also has inertial degree 1. Thus, there must be two primes there, i.e. $p\mathcal{O}_K = P_1P_2$. Then $p\mathcal{O}_K$ is not prime, and so

$$\mathcal{O}_K/p\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{q^*}}{2}\right]\Big/(p) \cong \mathbb{Z}[x]\Big/\left(x^2 - x + \frac{1-q^*}{4}, p\right) \cong \mathbb{F}_p[x]\Big/\left(x^2 - x + \frac{1-q^*}{4}\right)$$

is not a domain, i.e. the last polynomial has a root $a \in \mathbb{F}_p$. Then,

$$(2a-1)^2 = 4a^2 - 4a + 1 = (q^* - 1) + 1 = q^*$$

so that $\left(\frac{q^*}{p}\right) = 1$.

But this proof essentially also works in reverse. Indeed, if $\left(\frac{q^*}{p}\right) = 1$, then there is some $b \in \mathbb{F}_p$ with $b^2 = q^*$, whence

$$\left(\frac{1+b}{2}\right)^2 - \left(\frac{1+b}{2}\right) + \frac{1-q^*}{4} = \frac{1+2b+b^2}{4} - \frac{2+2b}{4} + \frac{1-q^*}{4} = 0$$

so that $x^2 - x + (1-q^*)/4$ is reducible. Thus $\mathcal{O}_K/p\mathcal{O}_K$ is not a domain, so $p\mathcal{O}_K$ is not prime, and since p is unramified, the only possibility is that $p\mathcal{O}_K = P_1P_2$ for some distinct primes P_1, P_2 of $\mathcal{O}_K$. But L_D is the largest subfield of L with ramification index and inertial degree 1, so this gives that $K \subseteq L_D$, and so $H \supseteq D$, where D is the decomposition group. But the order of τ is $f = |D|$, and since there is a unique subgroup of this order, we must have τ generates D. In particular, it is an element of D, and so $\tau \in H$. But the elements of H are precisely the squares, so $\tau = \gamma^2$ for some automorphism γ. Every automorphism of $L/\mathbb{Q}$ is of the form $\zeta_q \mapsto \zeta_q^t$, and so for these to be the same automorphism we must have $p \equiv t^2 \pmod{q}$, so that $\left(\frac{p}{q}\right) = 1$.

So, we've shown $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$. This completes the proof. Indeed, if $q \equiv 1 \pmod{4}$, then $q^* = q$, and so

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)\left(\frac{q^*}{p}\right) = 1 = (-1)^{(p-1)(q-1)/4}$$

since p is odd. On the other hand, if $q \equiv 3 \pmod{4}$, then $q^* = -q$ and we know $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. So,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)\left(\frac{q^*}{p}\right)\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{(p-1)(q-1)/4}$$

since $(q-1)/2$ is odd. □

Note that in the proof we've shown that for p, q distinct primes (and p not necessarily odd) that if $P \subseteq \mathbb{Z}[\zeta_q]$ lies over p, then $f(P|p)$ is the multiplicative order of p modulo q, since this is the common value f of the orders of σ, τ above. This will be useful for the other stated exercise: namely, the existence of non-monogenic rings of integers.

First, note that Marcus' Number Fields gives such an example explicitly (with no mention on how to find such examples for oneself):

Exercise (2.30). *Let $K = \mathbb{Q}[\sqrt{7}, \sqrt{10}]$ and fix any $\alpha \in \mathbb{A} \cap K$. We will show that $\mathbb{A} \cap K \neq \mathbb{Z}[\alpha]$. Let f denote the monic irreducible polynomial for α over $\mathbb{Z}$ and for each $g \in \mathbb{Z}[x]$ let $\overline{g}$ denote the polynomial in $\mathbb{Z}_3[x]$ obtained by reducing coefficients* $(\mathrm{mod}\ 3)$.

(a) Show that $g(\alpha)$ is divisible by 3 in $\mathbb{Z}[\alpha]$ iff $\overline{g}$ is divisible by $\overline{f}$ in $\mathbb{Z}_3[x]$.

(b) Now suppose $\mathbb{Z} \cap K = \mathbb{Z}[\alpha]$. Consider the four algebraic integers

$$\alpha_1 = (1+\sqrt{7})(1+\sqrt{10})$$
$$\alpha_2 = (1+\sqrt{7})(1-\sqrt{10})$$
$$\alpha_3 = (1-\sqrt{7})(1+\sqrt{10})$$
$$\alpha_4 = (1-\sqrt{7})(1-\sqrt{10})$$

Show that all products $\alpha_i\alpha_j$ $(i \neq j)$ are divisible by 3 in $\mathbb{Z}[\alpha]$, but that 3 does not divide any power of any α_i.

(c) Let $\alpha_i = f_i(\alpha)$, $f_i \in \mathbb{Z}[x]$ for each $i = 1, 2, 3, 4$. Show that $\overline{f} \mid \overline{f_i f_j}$ $(i \neq j)$ in $\mathbb{Z}_3[x]$ but $\overline{f} \nmid \overline{f_i}^n$. Conclude that for each i, $\overline{f}$ has an irreducible factor (over $\mathbb{Z}_3$) which does not divide $\overline{f_i}$ but which does divide all $\overline{f_j}$, $j \neq i$.

(d) This shows that $\overline{f}$ has at least four distinct irreducible factors over $\mathbb{Z}_3$. On the other hand f has degree at most 4. Why is that a contradiction?

Proof. We show the first claim. Suppose $g(\alpha)$ is divisible by 3. Then there is some $\beta \in \mathbb{Z}[\alpha]$ with $g(\alpha) = 3\beta$, and $\beta = h(\alpha)$ for some $h \in \mathbb{Z}[x]$. Then α is a root of $g(x) - 3h(x)$, so $f \mid g - 3h$. Reducing mod 3 gives $\overline{f} \mid \overline{g}$ as claimed. Each of these steps is reversible: if $\overline{f} \mid \overline{g}$, then $f \mid g + 3h$ for some h, whence $g(\alpha) + 3h(\alpha) = 0$, i.e. $g(\alpha) = -3h(\alpha)$ is a multiple of 3.

For the second, note that $(1+\sqrt{7})(1-\sqrt{7}) = -6$ and $(1+\sqrt{10})(1-\sqrt{10}) = -9$ are both multiples of 3, so each product $\alpha_i\alpha_j$ is a multiple of 3 since each product consists of at least one of these pairs of terms. On the other hand, we do have that the α_i are a full set of conjugates, so the trace of α_i^n is

$$\alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n$$

On the other hand, we have

$$4^n = (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^n = \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n + \cdots$$

where the excluded terms, from the binomial theorem, each include the product of two different terms. In other words, each term in the "$\cdots$" is a multiple of 3 in $\mathbb{Z}[\alpha]$, so we can write the trace as $1 + 3\beta$ for some $\beta \in \mathbb{Z}[\alpha]$. By unique representation of numbers in $\mathbb{Q}(\alpha)$, we thus have that $\beta \in \mathbb{Z}$, since the trace is an integer. I.e. the trace is 1 mod 3 and therefore not a multiple of 3. So, α_i^n is not a multiple of 3 in $\mathbb{Z}[\alpha]$.

The next result is immediate by combining these two: for $\alpha_i = f_i(\alpha)$, we have that 3 divides $\alpha_i\alpha_j$, so $\overline{f}$ divides $\overline{f_i f_j}$ in $\mathbb{F}_3[x]$, and 3 does not divide α_i^n, so $\overline{f}$ does not divide $\overline{f_i^n}$. Since $\mathbb{F}_3[x]$ is a UFD (even a PID), we have that this latter statement implies that there is a prime π_i that divides $\overline{f}$ but not $\overline{f_i}$. But then π_i divides $\overline{f_i f_j}$, so it divides $\overline{f_j}$ for all $j \neq i$.

Finally, we have that $\overline{f}$ is divisible by the four (distinct) primes $\pi_1, \ldots, \pi_4$ and hence their product. These cannot all be degree 1, since there are only three degree 1 monic polynomials in $\mathbb{F}_3[x]$: $x, x+1, x+2$. So, at least one has degree 2, whence the product has degree at least $1+1+1+2 = 5$. But f is the minimal polynomial of α, and so has degree 4. This gives the contradiction. Thus the ring of integers is not monogenic. □

This exercise is relatively unenlightening at first, but let us recast it in the language of factorization of ideals: we've shown that for $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$, that 3 splits as the product of at least four different primes. Namely, for each i, there is a prime P_i lying over 3 that contains α_j for $j \neq i$ but doesn't contain α_i. Indeed, if α_i were in each prime lying over 3, and there are r of them (counting multiplicities), then α_i^r would be in their product, which is (3), contrary to assumption. So, there is a P_i lying over (3) with $\alpha_i \notin P_i$ and then for each j, $\alpha_i\alpha_j \in (3) \subseteq P_i$ implies that $\alpha_j \in P_i$.

Further, we have in the above case that 3 is unramified. One way to see this is to compute

$$\mathrm{disc}(1, \sqrt{7}, \sqrt{10}, \sqrt{70}) = 4^4 \cdot 7 \cdot 10 \cdot 70$$

which is not divisible by 3. Thus, $\operatorname{disc}(\mathcal{O}_K)$ is also not divisible by 3 (though it might not equal the above). Hence, the factorization is into at least 4 distinct primes. But because this is a degree four extension, there are exactly 4, each of inertial degree 1. That is,

$$3\mathcal{O}_K = P_1P_2P_3P_4$$

By the Chinese Remainder Theorem, this gives:

$$\mathcal{O}_K/3\mathcal{O}_K \cong \bigoplus_{i=1}^{4} \mathcal{O}_K/P_i \cong (\mathbb{F}_3)^4$$

Finally, assume that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ is monogenic. Then, we get a surjection $\mathbb{Z}[x] \to \mathcal{O}_K \to \mathcal{O}_K/3$ by mapping x to α and composing with the quotient map. But clearly 3 is in the kernel of this map, and from the above, we also see that $x^3 - x$ is in the kernel, since each element of $\mathbb{F}_3$ satisfies $t^3 - t$. So, the map factors as a surjection:

$$\mathbb{Z}[x]/(3, x^3 - x) \to (\mathbb{F}_3)^4$$

but the former has 3^3 elements while the latter has 3^4. This gives the contradiction.

More generally, if we can find a number field K such that $[K : \mathbb{Q}] > p$ for some prime p that splits completely, we'll have the same contradiction. Indeed, the above map will instead become a surjection:

$$\mathbb{Z}[x]/(p, x^p - x) \to (\mathbb{F}_p)^{[K:\mathbb{Q}]}$$

which is impossible. We'll use this to construct our own example for $p = 2$.

Theorem. *There exists (another) number field K with $\mathcal{O}_K$ not monogenic.*

Proof. Consider $L = \mathbb{Q}(\zeta_p)$ for an unspecified odd prime p. We'll construct K as an appropriate subfield of L. First, note that $\operatorname{disc}(\zeta_p) = p^{p-2}$, so that 2 is unramified in L and so will also be unramified in K. We'd also like the inertial degree to be 1 for any prime lying over 2, so we fix a prime Q of L lying over 2 and let K be the decomposition field of Q. Then, it is a standard result that $[K : \mathbb{Q}]$ is the number of prime factors appearing in the factorization of 2 in L, which equals $(p-1)/f$ for f the inertial degree of Q over 2. But f is also the multiplicative degree of 2 modulo p by our work above.

So, overall, we'd like 2 to have order f modulo p for some prime satisfying $f \mid p - 1$. Testing some primes directly, we see that $2^5 \equiv 1 \pmod{31}$, and $5 \mid 31 - 1 = 30$. So, we let $p = 5$.

In other words, let K be the unique subgroup of $\mathbb{Q}(\zeta_{31})$ of degree 6 over $\mathbb{Q}$. Then 2 splits completely in K and the remarks preceding the proof show that $\mathcal{O}_K$ is not monogenic. □