Quadratic and Cyclotomic fields

Dinesh S. Thakur

As a complement to Sury's lectures on Dedekind domains, we will now give an example oriented introduction to quadratic and cyclotomic fields. In the workshop, the two series of talks went in parallel. So we might use terminology defined carefully in Sury's talks. We have omitted simple details which were usually worked out in problem sessions and are also given in many texts. Since the repetition usually helps, we have not tried for an efficient or a general treatment.

Apart from $\mathbf{Q}$, the simplest class of number fields are the *quadratic* fields i.e., the degree 2 extensions (so that there are no non-trivial subfields) obtained by solving a quadratic and hence (by completing the square) of the form $K = \mathbf{Q}(\sqrt{a/b})$. Multiplying by b and getting rid of the squares under the square-root, we can write it as $K = \mathbf{Q}(\sqrt{m})$, where m is square-free. (So these are special Kummer extensions). These fields are then distinct for distinct m. These are Galois extensions, with Galois conjugate of a general element $r + s\sqrt{m}$ ($r, s \in \mathbf{Q}$) being $r - s\sqrt{m}$. The norm and the trace are essentially just the coefficients of the minimal polynomial in this case.

What are the *algebraic integers*? By making a common denominator, we can write a general element of the field as $(a + b\sqrt{m})/c$, with integral a, b, c with the GCD $(a, b, c) = 1$. Since the trace and norms are usual integers, we have $c|2a$ and $c^2|a^2 - mb^2$. So if we let $d = (a, c)$, then d^2 divides a^2, b^2 and $a^2 - mb^2$ and hence mb^2. Since m is square-free, d divides b, so that $d = 1$. Therefore, c divides $2a$ now implies c divides 2 and hence c is 1 or 2 without loss of generality. (Another way to see this is that if x is an algebraic integer in the field, $x^2 + Bx + C = 0$, hence $x = (-B \pm \sqrt{B^2 - 4C})/2$). If $c = 2$, then a is odd and $mb^2 \equiv a^2 \equiv 1$ modulo 4 and hence $m \equiv 1$ modulo 4 and b is odd.

So (exercise: finish the details) the $\mathbf{Z}$-*basis* of $\mathcal{O}_K$ is $1, (1 + \sqrt{m})/2$ or $1, \sqrt{m}$ depending on whether $m \equiv 1$ modulo 4 or not. If we write $K = \mathbf{Q}(\sqrt{d})$, where d is the discriminant, which is always $\equiv 0, 1$ modulo 4 (and is either m or $4m$), then we can say that the basis is always $1, (d + \sqrt{d})/2$.

What are the *units*? If α is a unit, it divides 1 and hence its norm being a rational integer dividing 1 is ± 1. Further, if $d < 0$ (the imaginary quadratic fields), the norm is positive, so is 1.

So (exercise) the only units in the imaginary quadratic fields are ± 1, except for $\mathbf{Q}(\sqrt{-1}) = \mathbf{Q}(\zeta_4)$, $\mathbf{Q}(\sqrt{-3}) = \mathbf{Q}(\zeta_6)$, where we have 4 and 6 units (which are the obvious roots of unity) respectively.

In the real quadratic case, we are led to equations such as $x^2 - my^2 = \pm 1$, called Pell equation (or rather Brahmagupta-Bhaskara-Fermat-Pell equation). For example, for $\mathbf{Q}(\sqrt{2})$, we see a solution $x = y = 1$ and get corresponding unit $w = 1 + \sqrt{2}$. Since this is not a root of unity, we get infinitely many units $\pm(1 + \sqrt{2})^n$, $n \in \mathbf{Z}$. In fact, these are all the units in this case: In general, if a unit other than ± 1 exists, then a smallest unit $\epsilon > 1$ exists (otherwise both the conjugates $x \pm y\sqrt{d}$ get close to 1 which forces x close to 1 and y close to 0, so equal to it) and is called the *fundamental unit*. It is easy to see that all the units are then given by $\pm\epsilon^n$. In our case, if $1 < x + y\sqrt{2} = \epsilon < w$, then $x^2 - 2y^2 = \pm 1$ implies $-1 < x - y\sqrt{2} < 1$. Adding the two, we get $0 < 2x < 1 + w$, so that $x = 1$ giving a contradiction $1 < 1 + y\sqrt{2} < 1 + \sqrt{2}$.

Dirichlet's theorem guarantees existence of a fundamental unit in the real quadratic case. We will just state a recipe: The continued fraction of $\sqrt{d} + \lfloor\sqrt{d}\rfloor$ is purely periodic with period vector $(a_0, \cdots a_{r-1})$ and p_{nr-1} and q_{nr-1} (the numerators and denominators of the convergents), are all the solutions of $x^2 - dy^2 = 1$ for even r or for odd r with even n and are solutions of $x^2 - dy^2 = -1$ (which has no solutions, if r is even) when both r and n are odd. The fundamental solution corresponds to $n = 1$.

(Exercise): For the imaginary quadratic fields, the integers sit discretely in $\mathbf{C}$, where as they are dense in $\mathbf{R}$ in the real quadratic fields.

Usual proof of the fact that $\mathbf{Z}$ is a principal ideal domain and unique factorization domain uses the *division algorithm*: The smallest positive element in the ideal is its generator by the division algorithm. Let us see how often the division algorithm works in the imaginary quadratic case, where the size comparisons are now done using the norm: Let $0 > m = -\mu$. If there is a division algorithm, given a, b we get a quotient q such that $a = qb + r$, with a 'smaller' remainder. This translates to norm of $a/q - b$ being smaller than 1. Translating to usual integers, given rationals r and s, we can find x and y such that $|(r - x)^2 - m(s - y)^2| < 1$, with x, y integers, if $m \not\equiv 1$ modulo 4 and half-integers otherwise. Choosing $r = s = 1/2$, in the first case, we see that $1/4 + \mu/4 < 1$, so that $\mu = 1$ or 2. In the second case, similarly, we get $1/16 + \mu/16 < 1$ giving $\mu = 3$, 7 or 11. So there are exactly 5 imaginary (and in fact, 16 real) quadratic fields which are *Euclidean* (for the size given by the norm function). There are four more unique factorizations domains, with $\mu = 163$ being the largest.

As an exercise in manipulations with ideals, let us see how ideals restore unique factorization in our example:

$$\begin{aligned} 6 &= 2\times 3 \\ &= (1+\sqrt{-5})(1-\sqrt{-5}) \\ &= (2,1+\sqrt{-5})(2,1-\sqrt{-5})(3,1+\sqrt{-5})(3,1-\sqrt{-5}). \end{aligned}$$

Note $I|J$ if and only if $J\subset I$, i.e., the multiples of J are contained in the multiples of I. Verify that $(2,1+\sqrt{-5})(3,1+\sqrt{-5})=(1+\sqrt{-5})$. Also note that $(2,1+\sqrt{-5})=(2,1-\sqrt{-5}+2\sqrt{-5})=(2,1-\sqrt{-5})$, so that 2 is a square (and a norm) of an ideal (it ramifies). (The discriminant of $\mathbf{Q}(\sqrt{-5})$ is -20, so that 2 and $5=-(\sqrt{-5})^2$ ramify.) There is no element of norm 2, otherwise we would have integral solution to $2=x^2+5y^2$. Hence, our ideal is non-principal. In fact, the class group is of order 2 in this case (exercise).

Let us use this fact to show that $x^3=y^2+5$ has no integral solutions: Looking at modulo 4 possibilities for an assumed solution, we see that y (which is seen to be prime to 5 also) is even, and so the GCD of the two factors $y\pm\sqrt{-5}$, which has to divide 2, can in fact be assumed to be 1. As the class number is prime to 3, each factor is a cube of an ideal. Since the units here are ± 1, which are also cubes, we get $y+\sqrt{-5}=(a+b\sqrt{-5})^3=a^3-5b^2+\sqrt{-5}b(3a^2-5b^2)$, where a and b are (rational) integers. Comparing the imaginary parts, we see that $b=\pm 1$, so that $1=\pm(3a^2-5)$, which is a contradiction.

Now let us look at the basic properties about the *cyclotomic* fields: We denote a primitive n-th root of unity by ζ_n. As a complex number, it is $e^{2\pi ik/n}$, with $(k,n)=1$. Since $1=kr+cn$, each of this is a power of any other, so that $K=\mathbf{Q}(\zeta_n)$ is a Galois extension. The minimal polynomial of ζ_n is called the n-th cyclotomic polynomial and is given by (verify irreducibility) $\Phi_n(x)=\prod_{1\le k\le n,(k,n)=1}(x-\zeta_n^k)$. Its degree is $\phi(n)$. Recall that for $n=\prod p_i^{n_i}$, we have $\phi(n)=\prod(p_i-1)p_i^{n_i-1}$.

The *Galois group* can be identified with $(\mathbf{Z}/n\mathbf{Z})^*$, with the action the automorphism σ_k corresponding to k being defined by $\sigma_k(\zeta_n)=\zeta_n^k$. In Galois theory, we have learned the correspondence between subgroup structure of the Galois group and the *subfield structure* of the field. In particular, since the group is abelian, all the subfields are Galois (with abelian Galois group). Let us find them explicitly for $\mathbf{Q}(\zeta_p)$, for p a prime: We know (exercise) that the Galois group $(\mathbf{Z}/p\mathbf{Z})^*$ is cyclic, say with generator g. So for $e|(p-1)$, we will have a unique sub-extension of degree e. For example, if $e=(p-1)/2$, then it is $\mathbf{Q}(\zeta_p)^+:=\mathbf{Q}(\zeta_p+\zeta_p^{-1})=\mathbf{Q}(\cos(2\pi/p))$, which is the maximal real subfield (and is obtained by averaging with respect to the complex conjugate). In general, we write $ef = p-1$ and define the so-called *periods* $\eta_i := \sum_{j=0}^{f-1} \zeta_p^{g^{ej+i}}$. We see that $\sigma_g(\eta_i) = \eta_{i+1}$, where i runs modulo e. So that there are e periods, all conjugate and distinct (as the minimal equation of ζ_p has all the $p-1$ powers occurring in it, whereas $\eta_i - \eta_j$ has fewer). Since each is left invariant with respect to the subgroup $H = \langle \sigma_g^e \rangle$, $\mathbf{Q}(\eta_i) = \mathbf{Q}(\eta_0)$ is the degree e sub-extension we want. The periods are useful in the construction of regular polygons, because they give explicit subfield structure needed in the problem.

What is the *quadratic subfield* of $\mathbf{Q}(\zeta_p)$? It is $\mathbf{Q}(\sqrt{(-1)^{(p-1)/2}p})$. One way to see this is to evaluate the corresponding period: $\sum \zeta_p^{g^{2j}} = \sum \zeta_p^k$, where k runs through quadratic residues and this relates to quadratic Gauss sum evaluated in Adhikari's lectures. Another way is to note that, in general, the discriminant which is square of the product of the differences of the conjugates, and it belongs to the base, its square root belongs to the field (Galois), giving a quadratic extension, if it is not a square. In our case, the discriminant is $\prod_{i<j}(\zeta_p^i - \zeta_p^j)^2$. Taking out the roots of unity, we see that the power of $(1-\zeta_p)$ is $2(1+2+\cdots+(p-2)) = (p-1)(p-2)$, so that the discriminant is (using $(p) = (1-\zeta_p)^{p-1}$ proved below) $\pm p^{p-2}$. Easy way to fix (and remember) the sign is to note that the maximal real subfield $\mathbf{Q}(\zeta_p)^+$ has has degree $(p-1)/2$, which is odd if $p \equiv 3$ modulo 4 and hence can not have quadratic subfield. So in this case, the subfield is imaginary quadratic.

What are the *algebraic integers* in $K = \mathbf{Q}(\zeta_n)$? In fact, $\mathcal{O}_K = \mathbf{Z}[\zeta_n]$. (See the proof in Sury's notes in this volume or in Washington[1]). One way inclusion is clear and since K is a quadratic field for $n \leq 4$ and $n = 6$, we can already verify the claim in those cases.

Let us write $\zeta = \zeta_p$ for this paragraph. We have $\Phi_p(x) = \prod(x - \zeta^i) = (x^p - 1)/(x-1) = x^{p-1} + \cdots + 1$, so that putting $x = 1$, we see that $p = \prod(1-\zeta^i) = Norm(1-\zeta)$. Now $(1-\zeta^i)/(1-\zeta)$ clearly belongs to $\mathbf{Z}[\zeta]$ and so does its inverse (which is obtained by just relabelling the primitive root!), so these are units. Hence we get $p\mathcal{O}_K = (1-\zeta)^{p-1}$ as ideals, so that p is totally ramified in $\mathbf{Q}(\zeta)$ with $(1-\zeta)$ being the prime above p. The story for $n = p^m$ is similar (exercise). On the other hand if two distinct primes p and q divide n, then since $1-\zeta_n$ divides $1-\zeta_p$ and $1-\zeta_q$, it divides p and q and hence is a unit. Together with the roots of unity and monomials in these, we get a readily available supply of units called cyclotomic units.

More precisely, the group of *cyclotomic units* for $K = \mathbf{Q}(\zeta_n)$ or $K = \mathbf{Q}(\zeta_n)^+$ is defined to be $C_n = \langle \pm\zeta_n, 1-\zeta_n^k \rangle \cap \mathcal{O}_K^*$. (For the intermediate

[1] For such references the reader may look into the general bibliography at the end of this volume.

extensions it is better to modify the definition by taking norms from the full cyclotomic extension, see Washington). For $n = p^m$, Washington Lemma 8.1 shows that the cyclotomic units are generated by

ζ_{p^m}, -1 and $\zeta_{p^m}^{(1-a)/2}(1-\zeta_{p^m}^a)/(1-\zeta_{p^m})$, for $1 < a < p^m/2$, $(a,p)=1$.

The latter are $\phi(p^m)/2-1 = r_2-1$ of them and in fact they are independent, giving the full rank of the unit group given by the Dirichlet theorem. In fact, the index of the cyclotomic units subgroup in the full unit group is the size of the class group of $\mathbf{Q}(\zeta_{p^m})^+$. So in some sense, the amount of failure of unique factorization is linked to amount of failure of capturing all units from these readily available cyclotomic ones! For n not a prime power, the story is more complicated. We will study the Ramachandra units for the general case in R. Balasubramanian's lectures[2].

Now we look at *how the usual primes factor*, when we go up in quadratic or cyclotomic extensions:

Claim: For the *quadratic field K* of discriminant d, and for an odd prime p, we have (i) $p\mathcal{O}_K = \wp^2$, $\wp$ prime if and only if $p|d$ i.e., $(d/p) = 0$, (ii) $p\mathcal{O}_K = \wp_1\wp_2$, $\wp_i$ distinct primes if and only if $(d/p) = 1$ and (iii) $p\mathcal{O}_K = \wp$ prime if and only if $(d/p) = -1$, where (d/p) is the Legendre symbol.

For the proof as well as $p = 2$ case, see TIFR pamphlet, pp. 63-64. Note that $\wp = (p, \sqrt{d})$ in case (i) and $\wp_i = (p, a \pm \sqrt{d})$ in case (ii), where $a^2 \equiv d$ modulo p.

Claim: For the *cyclotomic field $K = \mathbf{Q}(\zeta_n)$*, and for a prime p, we have (i) p is ramified if and only if $p|n$ and (ii) If p does not divide n, then $p\mathcal{O}_K = \wp_1 \cdots \wp_g$, with $\wp_i$ distinct primes of residue degree f and $g = \phi(n)/f$. Here f is the order of p modulo n i.e., f is the smallest positive integer such that $p^f \equiv 1$ modulo n.

Proof: Since p divides n if and only if it divides the discriminant, we know from the general theory covered in Sury's lectures that (i) holds (we have also seen that if $p|n$, then p is ramified, at least for n a prime power) and (ii) holds except possibly for the last statement. Suppose the residue degree is f_1, so that $Norm(\wp_i) = p^{f_1} = |\mathcal{O}_K/\wp_i|$. Then by Fermat's little theorem we have $\alpha^{p^{f_1}} \equiv \alpha$ modulo $\wp_i$, and f_1 is smallest with this property, as the multiplicative group of the finite field $\mathcal{O}_K/\wp_i$ is cyclic. On the other hand, by the definition of f, we have $\zeta_n^{p^f} = \zeta_n$ and since any $\alpha \in \mathcal{O}_K$ can be written as $\sum a_i\zeta_n^i$, we have $\alpha^{p^f} \equiv \alpha$ modulo $\wp_i$. So $f_1 \leq f$. But if $f_1 < f$, then $\zeta_n^{p^{f_1}}$ is distinct from ζ_n and $\wp_i$ divides $\zeta_n^{p^{f_1}} - \zeta_n$ which occurs as a factor of the discriminant, and hence p divides a discriminant, which is a contradiction proving $f_1 = f$ as claimed.

[2] The text of these lectures was not available for these proceedings. – Editors

Let us see how the *quadratic reciprocity law*: $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$ for odd distinct primes p and q gets a natural proof when you compare the factorization of a prime in a quadratic field above with the recipe of the cyclotomic field factorization applied to its quadratic sub-extension:

We have, $1 = ((-1)^{(p-1)/2}p/q) = (-1)^{(p-1)(q-1)/4}(p/q)$ if and only if q splits in the quadratic field K of discriminant $d := (-1)^{(p-1)/2}p$ if and only if K is the unique quadratic subfield of the decomposition field, which is of degree g if and only if g is even if and only if $q^{(p-1)/2} \equiv (q^f)^{g/2} \equiv 1^{g/2} \equiv 1$ modulo p if and only if $(q/p) = 1$.

We can also see this without using the concepts of the decomposition field, its degree and so on: If q splits in quadratic extension, then since each of those two conjugates primes decompose the same way in the cyclotomic field containing this quadratic field, the corresponding g is even (in other words, g multiplies in tower) and hence q is a quadratic residue modulo p as above. By symmetry, this takes care of all cases except possibly $p \equiv q \equiv 3$ modulo 4 and (p/q) and (q/p) are 1. We leave this as an exercise (use that f also multiplies in tower together with $q^{(p-1)/2} \equiv 1$ and p does not split in $\mathbf{Q}(\sqrt{-q})$ to get a contradiction).

Another 'quick' and natural way: Let $q = Q_1Q_2$. Let h be the class number of K and write $Q_1^h = ((x + \sqrt{d}y)/2)$. Multiplying by the conjugate (i.e., taking norm), we get $\pm 4q^h = x^2 - dy^2 \equiv x^2$ modulo p. Now 4 is a square, -1 is a square modulo p, if $p \equiv 1$ modulo 4 and otherwise the right hand side is positive, so that the sign on left is also positive. Hence q^h is a square modulo p. Now it is a (hard) fact of the genus theory of quadratic fields (see TIFR pamphlet for the details) that h is odd (when the discriminant of the quadratic field consists of a single prime). So this implies that q is a square modulo p as required. This proof is harder, but shows the reciprocity connection quickly and uses only quadratic theory.

Another way uses index 2 (rather than degree 2) subfields of the cyclotomic fields and norms: Note that $(p-1)/2$ occurring in the quadratic reciprocity law is the degree of the index 2 subfield $\mathbf{Q}(\zeta_p)^+$ and consider the compositum L of $\mathbf{Q}(\zeta_p)^+$ and $\mathbf{Q}(\zeta_q)^+$. Then $\pi_p := (1-\zeta_p)(1-\zeta_p^{-1})$ is the norm of $1-\zeta_p$ from L to $\mathbf{Q}(\zeta_p)^+$. Define π_q similarly. Let $N(x)$ denote the norm of x from L to $\mathbf{Q}$.

Claim: $N(\pi_p - \pi_q) = (p/q)$. Assuming this, the quadratic reciprocity follows by interchanging p and q, as $N(-1) = (-1)^{[L:\mathbf{Q}]} = (-1)^{(p-1)(q-1)/4}$.

Proof: We have $\eta := \pi_p - \pi_q \equiv \pi_p$ modulo (π_q). For any $\sigma \in Gal(L/\mathbf{Q})$, we have $(\pi_q)^\sigma = (\pi_q)$ as ideal, as $\zeta_q^\sigma = \zeta_q^a$ for some a prime to q. Hence $N(\eta) \equiv N(\pi_p)$ modulo (π_q) and hence modulo q, as both the sides are in $\mathbf{Q}$.

But now $N(\pi_p)$ is the norm from $\mathbf{Q}(\zeta_p)^+$ to $\mathbf{Q}$ of $\pi_p^{(q-1)/2}$ so equals $p^{(q-1)/2}$ which is congruent to (p/q) modulo q. This congruence implies equality, because $N(\eta) = \pm 1$, as $\eta = \zeta_q^{-1}(1 - \zeta_p\zeta_q)(1 - \zeta_p^{-1}\zeta_q)$ is a unit.

We will see one more proof using quadratic Gauss sums in Adhikari's lectures.

Finally, we *compare unit groups and class groups* of $K := \mathbf{Q}(\zeta_n)$ to those of $K^+ := \mathbf{Q}(\zeta_n)^*$: For a number field K, let U_K denote its unit group, μ_K its subgroup consisting of all roots of unity in K, C_K its class group and $C_K^{(p)}$ its p-primary part.

Claim: The index $[U_K : \mu_K U_{K^+}]$ is 1 or 2 according as whether n is a prime power or not.

Proof: Consider the homomorphism $\psi : U_K \to \mu_K$ defined by $\psi(u) = \overline{u}/u$. (Recall that algebraic integer with all its absolute values being one is a root of unity). This induces injective homomorphism from U_K/U_{K^+} to μ_K. It follows from the definition that $\psi(U_{K^+}\mu_K) = \mu_K^2$. Since μ_K/μ_K^2 is of order 2, it follows that the index is 2 or 1 according as whether ψ is surjective or not. If n is not a prime power, then $1 - \zeta_n$ is a unit which maps to $-\zeta_n^{-1}$, and hence ψ is surjective. On the other hand, suppose n is a prime power, and ψ is surjective, with $\psi(u) = -\zeta_n^{-1}$. Put $\alpha := (1 - \zeta_n)/u$. Then $\overline{\alpha} = \alpha$, so that α is real. But α being a prime element of K can not lie in K^+. This contradiction finishes the proof of the claim.

The unit groups in K and K^+ are thus not much different and thus the regulators are essentially the same and thus taking ratio of the corresponding zeta functions we get a formula for the relative class number, by getting rid of the usually hard to handle regulators.

To start comparing the class groups, we start with a weaker result in more general situation:

Claim: If L is a Galois extension of degree d of a number field K, and if a prime p does not divide d, then the natural map $C_K^{(p)} \to C_L^{(p)}$ is injective and the map $C_L^{(p)} \to C_K^{(p)}$ induced by the norm is surjective.

Proof: If I is an ideal of $\mathcal{O}_K$ representing a class in $C_K^{(p)}$ such that $I\mathcal{O}_L = (\alpha)$, then $I^d = (Norm_K^L(\alpha))$ is principal, which implies I is principal, as p does not divide d. This proves the first part. On the other hand, if p does not divide d, every element in $C_K^{(p)}$ is a d-th power, this proves surjectivity, since $I^d = Norm(I\mathcal{O}_L)$.

Claim: Natural map $C_{K^+} \to C_K$ is injective (so h^+ divides h).

Proof: If I is an ideal of $\mathcal{O}_{K^+}$, such that $I\mathcal{O}_K = (\alpha)$, then $\overline{I\mathcal{O}_K} = (\overline{\alpha}) = I\mathcal{O}_K$. Hence $\alpha/\overline{\alpha}$ is a unit with all its conjugates having absolute value 1 and hence it is a root of unity. If n is not a prime power, since ψ

is surjective, we can write it as $\overline{u}/u$. This implies that αu is real, but then $I = (\alpha u)$ proves what we want. If n is a prime power, put $\lambda := 1 - \zeta_n$. Then $\lambda/\overline{\lambda} = -\zeta_n$, which is a generator of μ_K. Hence $\overline{\alpha}/\alpha = (\lambda/\overline{\lambda})^d$ for some d. Now λ-adic valuation takes even values on K^+, and $\alpha\lambda^d$ and I are real. Hence, $d = v_\lambda(\alpha\lambda^d) - v_\lambda(\alpha) = v_\lambda(\alpha\lambda^d) - v_\lambda(I)$ is even. This implies $\alpha/\overline{\alpha} = (-\zeta_n)^d \in \mu_K^2$ and hence equals $\zeta/\overline{\zeta}$ by above. This means $\alpha\zeta$ is real and $I = (\alpha\zeta)$ finishes the proof.

(Exercise) Compare the questions and arguments above with those encountered in Hilbert 90, in Narlikar and Nitsure lectures.

Dinesh Thakur
Department of Mathematics
University of Arizona
Tucson, AZ 85721
USA
e-mail: thakur@math.arizona.edu