

Lecture 5

Proof of Theorem 26, Part 3. We already have unique factorization for integral ideals. To factor and invert an arbitrary fractional ideal, we use the following lemma to reduce to the case of integral ideals.

Lemma 27. *If L is any fractional ideal of A , there exist integral ideals I, J such that $I \cdot L = J$.*

Proof. Let $J = L \cap I \subseteq A$, which is an integral ideal. Our result follows from the following sublemma. \square

Lemma 28. *If J and L are fractional ideals such that $J \subseteq L$, then there exists an integral ideal I such that $I \cdot L = J$.*

Proof. By our notes in Lecture 1, since A and L are both lattices, there exists nonzero rational number α such that $\alpha L \subseteq A$. It follows that $\alpha J \subseteq \alpha L \subseteq A$. Since αJ and αL are therefore integral ideals in A , there are prime ideals P_1, \dots, P_m and Q_1, \dots, Q_n such that $\alpha J = P_1 \cdots P_m$ and $\alpha L = Q_1 \cdots Q_n$. The containment $\alpha J \subseteq \alpha L$ and the proof of Proposition 24, show that (after rearranging the P_i) $Q_1 = P_1$. Thus, we multiply by P_i^{-1} and get $\alpha J' \subseteq \alpha L' = Q_2 \cdots Q_n \subseteq A$. Continuing this process, we see that

$$\alpha J = P_1 \cdots P_m = Q_1 \cdots Q_n P_{n+1} \cdots P_m = \alpha L P_{n+1} \cdots P_m$$

which implies that $J = L \cdot I$ where $I = P_{n+1} \cdots P_m$. \square

The rest of the theorem now follows. We notice that $I \subseteq J$ if and only if $\text{ord}_P(I) \geq \text{ord}_P(J)$ for all prime ideals P . \square

Definition. The set \mathbf{P} of principal fractional ideals $\mathbf{P} = \{\alpha A : \alpha \in k^\times\}$ is a subgroup of the group \mathbf{I} of all fractional ideals, since $(\alpha A)(\beta A) = (\alpha\beta)A$ and $(\alpha A)^{-1} = \alpha^{-1}A$. We define the *ideal class group* of A (or k) as the quotient $C = \mathbf{I}/\mathbf{P}$.

Proposition 29. *If k is a number field with ring of integers A , and \mathbf{I} and C are as above, then we have a long exact sequence*

$$1 \rightarrow A^\times \xrightarrow{\iota} k^\times \xrightarrow{\epsilon} \mathbf{I} \xrightarrow{\rho} C \rightarrow 1$$

where ι is the natural inclusion, ρ is the natural projection and ϵ is given by $\alpha \mapsto \alpha A$.

Proof. It is straightforward to check exactness at each point, except maybe at k^\times . An element $\alpha \in k^\times$ is in $\ker(\epsilon)$ if and only if $\alpha A = A$. This occurs if and only if α and α^{-1} are in A , since $1 \in A$, and this occurs if and only if $\alpha \in A^\times$. \square

We note, for the people who know some K -theory, that this comes from the long exact sequence in K -theory.

$$\begin{array}{ccccccccc} K_1(A) & \rightarrow & K_1(k) & \rightarrow & \overbrace{\oplus_P K_0(A/P)}^{=\mathbb{Z}} & \rightarrow & K_0(A) & \rightarrow & K_0(k) & \rightarrow & 0 \\ \parallel & & \parallel & & \parallel & & \parallel & & \parallel & & \\ A^\times & \longrightarrow & k^\times & \longrightarrow & \mathbf{I} & \longrightarrow & \mathbb{Z} + C & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

which continues to the left as

$$\begin{array}{ccccccc} K_2(A) & \longrightarrow & K_2(k) & \xrightarrow{\beta} & \oplus_P K_1(A/P) & \longrightarrow & \\ & & \parallel & & \parallel & & \\ & & (k^\times \otimes k^\times)/S & \longrightarrow & \oplus_P (A/P)^\times & \longrightarrow & \end{array}$$

where S is the subgroup generated by the Steinberg relations and β is the tame symbol.

Theorem 30. *If k is a number field with ring of integers A , and \mathbf{I} and C are as above, then C is finite and A^\times is finitely generated.*

Example. It is a very special property of number fields that C is finite and A^\times is finitely generated. We give an example to show that this is not true in general. Let $\Lambda \subset \mathbb{C}$ be a lattice, that is, a discrete, co-compact, additive subgroup. Fix nonzero complex numbers w_1, w_2 such that $w_1/w_2 \notin \mathbb{R}$ and $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$. Let $E = \mathbb{C}/\Lambda$ and let A denote the ring of meromorphic functions $E \rightarrow \mathbb{P}^1(\mathbb{C})$ whose only poles lie in Λ . Then

$$A = H^0(E \setminus \{0\}, \mathcal{O}_E) = \mathbb{C}[p, p'] / ((p')^2 = 4p^3 - g_2p - g_3)$$

For any $z \in E \setminus \{0\}$, let

$$P_z = \{f \in A : f(z) = 0\} \subset A.$$

Each P_z is a maximal ideal in A with $A/P_z \xrightarrow{\cong} \mathbb{C}$ given by $f \mapsto f(z)$. When is $\prod_z P_z^{m(z)}$ principal, given by gA ? If $g : E \rightarrow \mathbb{P}^1(\mathbb{C})$ has a pole at 0 and zeroes of order $m(z)$ at $z \in E \setminus \{0\}$, then the divisor of g is

$$\operatorname{div}(g) = \sum_{z \in E \setminus 0} m(z)z - \sum_{z \in E \setminus 0} m(z)(0).$$

Abel's Theorem says that $\operatorname{div}(g) = \sum_{P \in E} m_P P$ satisfies the relations

$$\sum_P m_P = 0 \quad \text{and} \quad \sum_z m_z z \equiv 0 \pmod{\Lambda}.$$

Thus, $\prod_z P_z^{m(z)} = gA$ if and only if $\sum_z m_z z \in \Lambda$. The exact sequence from Proposition 29 is then

$$1 \rightarrow \mathbb{C}^\times \rightarrow \mathbb{C}(p, p') \rightarrow \bigoplus_{z \in E \setminus 0} \mathbb{Z} \rightarrow E \rightarrow 0$$

$\mathbb{C}^\times = A^\times$ is not finitely generated and $E = C$ is not finite.

Proof of Theorem 30. The fact that A^\times is finitely generated is the Unit Theorem, which we shall prove in Lecture 8. For now we prove that the ideal class group is finite.

The norm which we defined on integral ideals $\mathbb{N}(I) = (A : I)$ extends to the set of all fractional ideals in a well-defined manner. If I is a fractional ideal with prime factorization $I = \prod_i P_i^{a_i}$, then we define $\mathbb{N}(I) = \prod \mathbb{N}(P_i)^{a_i}$. This agrees with the original definition for integral ideals, by a composition series argument as in the proof of Proposition 24.

Furthermore, we note that since A/P_i is a finite field, say with $q_i = p_i^{b_i}$ elements, $\mathbb{N}(P_i) = (A : P_i) = q_i$. As we observed previously, the norm of an element of k^* is not necessarily the same as the norm of the principal ideal it generates. However, $\mathbb{N}(\alpha A) = |\mathbb{N}(\alpha)|$. For an integral ideal I , we compute the discriminant, as a lattice: $\text{disc}(\alpha A) = \text{disc}(A)(\mathbb{N}(\alpha A))^2$. Finally, it is clear that the norm map, as defined, extends to a homomorphism of abelian groups $\mathbb{N} : \mathbf{I} \rightarrow \mathbb{Q}_+^\times$. Our result will follow from the following theorem.

Theorem 31. *Every ideal class $c \in C$ is represented by an integral ideal I such that $\mathbb{N}(I) \leq e(k)$ where*

$$e(k) = \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^{r_2} |d|^{1/2}$$

and $d = \text{disc}(A)$.

Before we prove Theorem 31, we see that it implies Theorem 30, as follows. The cardinality of C is at most the cardinality of the set of integral ideals I such that $(A : I) = \mathbb{N}(I) \leq e(k)$. In turn, this is at most the cardinality of the set of lattices in $A \cong \mathbb{Z}^n$ of index at most $e(k)$. By the theory of finitely generated abelian groups, this cardinality is finite, so C is finite. \square

Proof of Theorem 31. Let J be a fractional ideal in the class c , and consider the lattice J^{-1} . By Theorem 17, there exists a nonzero element α of the lattice J^{-1} such that

$$|\mathbb{N}(\alpha)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^{r_2} |\text{disc}(J^{-1})|^{1/2} = \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^{r_2} \frac{|d|^{1/2}}{\mathbb{N}(J)}$$

Since $\alpha \in J^{-1}$, $\alpha A \subseteq J^{-1}$ and $I = \alpha J \subseteq A$. Thus, I and J are in the same class of C , since they differ by the principal fractional ideal αA . And

$$\mathbb{N}(I) = |\mathbb{N}(\alpha)| \cdot \mathbb{N}(J) \leq \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^{r_2} \frac{|d|^{1/2}}{\mathbb{N}(J)} \cdot \mathbb{N}(J) = e(k)$$

as desired. \square

Definition. The *class number* of a number field k is denoted $h = h(k)$ and is defined to be the cardinality of the ideal class group C of k .

Example. If $n = 1$ (so that $k = \mathbb{Q}$) then $r_1 + 2r_2 = n = 1 \Rightarrow r_2 = 0$ and $|d| = 1$ so that $e(k) = 1$. Since every element of C is represented by an integral ideal of norm at most 1, it follows that $C = (1)$.

If $n = 2$ then k is a quadratic extension. If $d < 0$ then $D < 0$ so that k is not a real field. That is, $r_2 = 1$. Then $e(k) = \frac{2}{\pi} |d|^{1/2}$ which is strictly less than 2 for the allowable discriminants $d = -3, -4, -7, -8$. In this case, $C = (1)$ again, and this implies that every fractional ideal is principal. In particular, each such $A = \mathbb{Z} + \mathbb{Z}(\frac{d+\sqrt{d}}{2})$ is a principal ideal domain. If $d > 0$, then $r_2 = 0$ and $e(k) < 2$ for $d = 5, 8, 12, 13$, and the rings of integers in these cases are also principal ideal domains.

If $e(k) < 3$, then every nontrivial class in C is represented by an integral ideal I such that $\mathbb{N}(I) = 2$. Since this index is prime, there are no lattices strictly between I and A . In

particular, $I = P$ is prime and A/P is the field of two elements. When $n = 2$ and $d < 0$ we see that $2 \leq e(k) < 3$ when $d = -11, -15, -19, -20$. In these cases

$$A = \mathbb{Z} + \mathbb{Z}\left(\frac{d + \sqrt{d}}{2}\right) = \mathbb{Z}[x]/(x^2 - dx + \frac{d^2-d}{4})$$

We wish to know when, under these assumptions, there is a prime ideal P with $\mathbb{N}(P) = 2$. This occurs if and only if there is a surjection $A \rightarrow \mathbb{Z}/2\mathbb{Z}$. To find such a surjection, it is equivalent to find a solution of the congruence $x^2 - dx + \frac{d^2-d}{4} \equiv 0 \pmod{2}$, so that we know where to send x , since the image of \mathbb{Z} is already determined. Furthermore, the number of distinct solutions (mod 2) is exactly the number of such maps, and therefore the number of such prime ideals. We check this by cases.

- (a) If $d \equiv 0 \pmod{4}$, then the congruence is $x^2 + \frac{d}{4} \equiv 0 \pmod{2}$, which has exactly one solution. Otherwise, $d \equiv 1 \pmod{4}$.
- (b) If $d \equiv 1 \pmod{8}$, then the congruence is $x^2 - x \equiv 0 \pmod{2}$, which has exactly two solutions.
- (c) If $d \equiv 5 \pmod{8}$, then the congruence is $x^2 - x + 1 \equiv 0 \pmod{2}$, which has no solutions.

We correlate this with our possibilities for d .

- (a) If $d = -20$, then there is exactly one prime ideal with norm 2.
- (b) If $d = -15$, then there are exactly two prime ideals with norm 2.
- (c) If $d = -11, -19$, then there are no prime ideals with norm 2.

Thus, for $d = -3, -4, -7, -8, -11, -19$ the class number is $h = 1$. For the cases $d = -20, -15$, we have more work to do.

For $d = -20$, $h = 2$. The generator of the class group in this case is a prime P of norm 2. In this case, $A = \mathbb{Z} + \mathbb{Z}(\sqrt{-5})$ and it follows that P is not principal. If P were principal, say $P = (a + b\sqrt{-5})A$, then $2 = \mathbb{N}(P) = a^2 + 5b^2$ which is impossible since a and b are integers. Since C has order 2, the class of P has order 2, so that P^2 is principal. The congruence we solve to find P in this case is $x^2 - 5 \equiv x^2 + 1 \equiv 0 \pmod{2}$. It follows that $x \mapsto \bar{1} \in \mathbb{Z}/2\mathbb{Z}$ and the kernel is $P = \langle 2, x - 1 \rangle$. It is straightforward to verify that $P^2 = 2A$ which has index 4 in A since $\mathbb{N}(2) = 4$.

For $d = -15$, we know that $h \leq 3$. In this case $A = \mathbb{Z}[\frac{1+\sqrt{-15}}{2}]$, and the prime ideals of index 2 are $P = \langle 2, x \rangle$ and $P' = \langle 2, x - 1 \rangle$. Every class in C is represented by A, P or P' , and the same check of norms as above shows that neither prime ideal is principal. Thus, $h = 2$ or 3 . Even though we have two distinct prime ideals of index 2 in A , it turns out that they represent the same nontrivial class in C and $h = 2$. Let $\alpha = 2$, $\beta = \frac{1+\sqrt{-15}}{2}$ and $\gamma = \frac{1-\sqrt{-15}}{2}$ in A . Each element has norm 4, and the ideals generated by these elements are all distinct, since none of the pairwise quotients are in A . It ends up that

$$PP' = \alpha A \quad P^2 = \beta A \quad (P')^2 = \gamma A$$

so that in the class group $[P][P'] = [P][P]$ which implies that $[P'] = [P]$. Another way to see the fact that C has order 2 is to observe that if it had order 3, then each nontrivial element would have order 3, which does not hold in this case.

We should observe that for quadratic fields with negative discriminants, it has been proven that the only examples with trivial class group are those with

$$d = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

However, for positive discriminant the list seems infinite. Whether or not the list is actually infinite is still an open question.

The case $d = -163$ is particularly interesting. If $\alpha = \frac{1+\sqrt{-163}}{2}$, then $A = \mathbb{Z} + \mathbb{Z}\alpha$. The minimal polynomial of α is $f_\alpha(x) = x^2 + x + 41$. The interesting fact here is that the values $f_\alpha(0), f_\alpha(1), \dots, f_\alpha(40)$ are all prime numbers. Of course, $f_\alpha(41) = 41(41 + 1 + 1)$ is not prime, but people considered functions of this type when trying to find prime-generating functions.

Definition. We are interested in finding the prime ideals of an order B . We define the *characteristic* of a prime ideal P to be the characteristic of its residue field B/P .

Lecture 6

Let k be a number field with ring of integers A , and let B be any order in k . The prime ideals P of B with characteristic p are exactly the maximal ideals containing pB , as $\text{char}(P) = p$ if and only if, under the natural projection $B \rightarrow B/P$, the number $p \mapsto 0$, which occurs if and only if $p \in P$ or equivalently that $pB \subseteq P$.

Since the elements which occur in the Jordan-Hölder series for $pB \subseteq B$ are exactly the prime ideals which contain pB , the above remarks show that the prime ideals in B of characteristic p are exactly the primes which occur in the product $P_1 \cdots P_t \subseteq pB$ from Proposition 24. In particular, there are only finitely many primes in B having a prescribed characteristic. Let P_1, \dots, P_u be the prime ideals of characteristic p . Then there are positive integers e_1, \dots, e_u such that $P_1^{e_1} \cdots P_u^{e_u} \subseteq pB$. (e_i is the multiplicity with which P_i occurs as a Jordan-Hölder factor in B/pB .) Since each P_i has characteristic p , the field B/P_i has order p^{f_i} for some positive integer f_i . Since B is a lattice of rank n , pB has index p^n in B , so

$$p^n = (B : pB) = \prod_{i=1}^u \mathbb{N}(P_i)^{e_i} = \prod_{i=1}^u (p^{f_i})^{e_i} = p^{(\sum_i e_i f_i)}$$

from which it follows that $n = \sum_{i=1}^u f_i e_i \geq u$. That is, there are at most n prime ideals of characteristic p in B .

We consider these ideas in the simplest of cases. Assume that α is an algebraic integer with minimal polynomial $f(x)$ of degree n . Then $B = \mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 + \cdots + \mathbb{Z}\alpha^{n-1}$ is an order in $k = \mathbb{Q}(\alpha)$. For example, if $n = 2$, then every order B is of this form with $\alpha = \frac{d_B + \sqrt{d_B}}{2}$ where $d_B = \text{disc}(B)$. Then $B \cong \mathbb{Z}[x]/(f(x))$ and

$$B/pB = \mathbb{Z}[x]/(p, f(x)) = (\mathbb{Z}/p\mathbb{Z}[k])/(\tilde{f}(x)) = \prod_i (\mathbb{Z}/p\mathbb{Z}[k])/(g_i(x)^{e_i})$$

where $\tilde{f}(x)$ is the reduction of $f(x)$ modulo p and $\tilde{f}(x) = \prod_i g_i(x)^{e_i}$ is the prime factorization of $\tilde{f}(x)$. It follows that the set of maximal ideals P_i of characteristic p with multiplicity e_i in the Jordan-Hölder decomposition are exactly the ideals $\langle p, \hat{g}_i(x) \rangle$ where $\hat{g}_i(x) \in \mathbb{Z}[x]$ is a lift of $g_i(x)$, and that under this correspondence (with the previous notation) $f_i = \deg(g_i(x))$. Thus, we have all the machinery to prove the following.

Corollary 32. *If $k = \mathbb{Q}(\alpha)$ where α is an algebraic integer, and p is a prime whose square does not divide $\text{disc}(\alpha) = \text{disc}(\mathbb{Z}[\alpha]) \in \mathbb{Z} \setminus \{0\}$, then $pA = \prod P_i^{e_i}$ mirrors the factorization*

of $f_\alpha(x)$ modulo p . More precisely, if $\deg(P_i) = f_i$ where $\#(A/P_i) = p^{f_i}$, then $\deg(P_i) = \deg(\tilde{g}_i(x))$ and the number of times that P_i occurs as a factor in the Jordan-Hölder series for A/pA is exactly e_i , the multiplicity of the factor $g_i(x)$ in $\tilde{f}(x)$. Moreover, if p does not divide $\text{disc}(\alpha)$, then all the $e_i = 1$.

Definition. In this notation, we call e_i the *ramification index* of P_i over p , and we call f_i the *residue degree*. If $e_i \geq 2$, then we say that P_i is *ramified* over p .

Proof. We claim that the index N of $\mathbb{Z}[\alpha]$ in A is prime to p . The formula $N^2 \text{disc}(A) = \text{disc}(\mathbb{Z}[\alpha]) = \text{disc}(\alpha)$ shows that if p divides N then p^2 divides $\text{disc}(\alpha)$, a contradiction. Fixing integers r, s such that $1 = pr + Ns$, it is straightforward to check that the map $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \rightarrow A/pA$ is an isomorphism. The previous discussion and the results on prime factorization in A imply the result. \square

Example. Assume that k is a cubic extension of \mathbb{Q} with ring of integers A such that $2A$ is a product of three distinct primes $2A = P_1 P_2 P_3$. For any $\alpha \in A \setminus \mathbb{Z}$, $k = \mathbb{Q}(\alpha)$ since the degree is prime. However, $\mathbb{Z}[\alpha] \subsetneq A$, because if they were equal, then the factorization of $f_\alpha(x)$ with coefficients reduced modulo 2 would have three distinct linear factors. This is a contradiction since there are only two distinct linear polynomials in $\mathbb{Z}/2\mathbb{Z}[x]$. An example where this occurs is when k is the unique cubic extension of \mathbb{Q} contained in the cyclotomic field $\mathbb{Q}(\zeta_{31})$, where ζ_{31} is a primitive 31st root of unity. The essential reason why $2A$ factors as claimed is in the congruence $2 \equiv 7^3 \pmod{31}$. We shall discuss this example in more detail in the future.

Next, we want to investigate the relation between $d = d_A = \text{disc}(A)$ and the e_i . We recall that the dual lattice of A is defined to be $A^* = \{\beta \in k : \text{Tr}(\beta A) \subseteq \mathbb{Z}\}$. By Proposition 1, $|d|$ is the index $(A^* : A)$.

Definition. We define the *different* of A to be the integral ideal $\mathcal{D} = (A^*)^{-1} \subseteq A^{-1} = A$. By Lemma 2, $\mathbb{N}(\mathcal{D}) = (A : \mathcal{D}) = |d|$. We adopt the following notation. Let P have characteristic p and let e_P denote the number of times P occurs as a factor in the Jordan-Hölder series for A/pA .

Proposition 33. $\mathcal{D} = \prod_P P^{m_P}$ for nonnegative integers m_P , and $m_P \geq e_P - 1$ with equality if and only if $\text{char}(P) \nmid e_P$.

Definition. If $m_P > e_P - 1$, then we say that P is *wildly ramified*. Otherwise, we say that P is *tamely ramified*.

Before we prove the proposition, we list some consequences.

Corollary 34. If k is quadratic, then the only primes p which have a ramified factor P in A are the primes dividing d .

Proof. We assume that $k = \mathbb{Q}(\sqrt{D})$ where D is square-free, and recall from Theorem 11 that $d \equiv 0, 1 \pmod{4}$ is as square-free as possible. Also, if $d \equiv 1 \pmod{4}$ then $d = D = \pm \prod_{\text{odd}} p_i$, and if $d \equiv 0 \pmod{4}$ then $d = 4D = \pm 2^a \prod_{\text{odd}} p_i$ where a is 2 or 3. If $\eta = \frac{d+\sqrt{d}}{2}$, then $A = \mathbb{Z} + \mathbb{Z}\eta$.

We claim that $\mathcal{D} = \sqrt{d}A \subset A$ and that the index is $\mathbb{N}(\mathcal{D}) = (A : \mathcal{D}) = |d|$. The first claim follows from the fact that $A^* = \frac{1}{\sqrt{d}}A$, which the interested reader is invited to check. The second claim follows from Proposition 1, since $\mathbb{N}(\mathcal{D}) = (\mathcal{D} : A) = (A^* : A) = |d|$.

As before, $pA = \prod_i P_i^{e_i}$ where $\sum_i e_i f_i = n = 2$. Then P is a ramified factor of p if and only if $P = P_1$ and $e_1 = 2$. This implies that $m_P \geq e_P - 1 = 1$ so that P occurs in the factorization of \mathcal{D} . Thus, $d = \mathbb{N}(\mathcal{D})$ is divisible by $\mathbb{N}(P)$, which is a power of p . \square

By the proof, if k is quadratic, then \mathcal{D} is principal so that its class in the class group \mathcal{C} is zero. In general, this is not the case. However, we have the following theorem, which we shall not prove (c.f. André Weil *Basic Number Theory*, Theorem XIII.12.13).

Theorem. If k is a number field, then the class of the different \mathcal{D} in the class group \mathcal{C} is contained in $2\mathcal{C}$.

We shall use the following proposition to prove Proposition 33.

Proposition 35. Let B be an order in a number field with dual module B^* , p a prime number, and P_i the Jordan-Hölder factors of pA with multiplicities e_i . Then $\cap_i P_i \subseteq pB^*$, and $\cap_{i \neq i_0} P_i \subseteq pB^*$ if and only if $p|e_{i_0}$.

Proof. Let $I = \cap_i P_i$. We have the following chain of equivalences: $I \subseteq pB^*$ iff $\frac{1}{p}I \subseteq B^*$ iff $\text{Tr}(\frac{1}{p}I) \subseteq \mathbb{Z}$ iff $\text{Tr}(I) \subseteq p\mathbb{Z}$ iff for every $\alpha \in I$, $\text{Tr}(\alpha) \equiv 0 \pmod{p}$ iff for every $\alpha \in I$, the multiplication map $\tilde{\alpha} : B/pB \rightarrow B/pB$ has trace zero. The map $\tilde{\alpha}$ is a linear endomorphism of the n -dimensional vector space B/pB over $\mathbb{Z}/p\mathbb{Z}$. Using the Jordan-Hölder decomposition of B/pB , we can write a matrix for $\tilde{\alpha}$ consisting of diagonal blocks each of which gives the action on the corresponding B/P_i . Thus,

$$\text{Tr}(\tilde{\alpha} : B/pB \rightarrow B/pB) = \sum_i e_i \text{Tr}(\tilde{\alpha}_i : B/P_i \rightarrow B/P_i)$$

and $I \subseteq pB^*$ iff the sum $\sum_i e_i \text{Tr}(\tilde{\alpha}_i : B/P_i \rightarrow B/P_i) = 0$. Thus, if $\alpha \in I$ then each $\tilde{\alpha}_i = 0$ so that $\text{Tr}(\tilde{\alpha}_i) \equiv 0$ and $I \subseteq pB^*$.

Let $I_0 = \cap_{i \neq i_0} P_i$ and fix $\alpha \in I_0$. If $\alpha \in I$, then each $\text{Tr}(\tilde{\alpha}_i) \equiv 0$, so assume that $\alpha \notin I$. Then every such α is in pB^* iff the i_0 term in the sum $\sum_i e_i \text{Tr}(\tilde{\alpha}_i)$ is zero. It suffices to show that there is some such α with $\text{Tr}(\tilde{\alpha}_{i_0}) \not\equiv 0$ so that the previous condition is equivalent to $e_{i_0} \equiv 0 \pmod{p}$, as desired.

For $i \neq i_0$, $P_i + P_{i_0} = B$ by maximality, so the Chinese Remainder Theorem implies that $I_0 + P_{i_0} = B$. It follows that the projection map $I_0 \rightarrow B/P_{i_0}$ is surjective, and it suffices to find an element $\beta \in B/P_{i_0}$ such that $\text{Tr}(\beta : B/P_{i_0} \rightarrow B/P_{i_0}) \not\equiv 0$. Since B/P_{i_0} is a field, we just choose β to be a primitive element over $\mathbb{Z}/p\mathbb{Z}$ so that the corresponding trace is 1. \square

Proof of Proposition 33. Let $B = A$ in Proposition 35 so that $pA = \prod_i P_i^{e_i}$. Then since the P_i are maximal, $\cap_i P_i = \prod_i P_i \subseteq pA^* = \prod_i P_i^{e_i} \mathcal{D}^{-1}$. This implies that $\mathcal{D} \subseteq \prod_i P_i^{e_i - 1}$ with equality if and only if no e_i is divisible by p . \square

Example. We consider the factorization of the ideals pA in a quadratic field k . In particular, we prove the converse of Corollary 34. If $\alpha = \frac{d+\sqrt{d}}{2}$, then the minimal polynomial of α is

$f_\alpha(x) = x^2 - dx + \frac{d^2-d}{4}$ and the ring of integers of k is $A = \mathbb{Z} + \mathbb{Z}\alpha$. We apply Corollary 32 in two cases.

Case 1: $p = 2$. If $d \equiv 0 \pmod{4}$, then $f_\alpha(x)$ reduces to $x^2 - \frac{d}{4}$ which factors to x^2 or $(x+1)^2$ depending on whether $\frac{d}{4}$ is even or odd. Thus, $2A = P^2$. Also, $\text{ord}_2(\mathcal{D}) = 2$ or 3 since this is the exponent for the power of 2 dividing $d = (A : \mathcal{D})$. If $d \equiv 1 \pmod{4}$, then the reduction of $f_\alpha(x)$ modulo 2 is

$$\tilde{f}_\alpha(x) = \begin{cases} x^2 - x & \text{if } d \equiv 1 \pmod{8}, \\ x^2 - x + 1 & \text{if } d \equiv 5 \pmod{8} \end{cases}$$

If $d \equiv 1 \pmod{8}$, then $\tilde{f}_\alpha(x)$ has two distinct factors and $2A = P_1 P_2$ is a product of distinct primes. (In this case, we say that p is *split*.) If $d \equiv 5 \pmod{8}$, then $\tilde{f}_\alpha(x)$ is irreducible and $2A$ is prime. (In this case we say that p is *inert*.) Notice that since $2 \nmid d$, $\text{ord}_2(\mathcal{D}) = 0$.

Case 2: $p > 2$. If $p|d$, then modulo p , $\tilde{f}_\alpha(x) = x^2$ so that $pA = P^2$ and $\text{ord}_p(\mathcal{D}) = 1$ since d is as square-free as possible. If $p \nmid d$, then we notice that in $\mathbb{Z}/p\mathbb{Z}$ the roots of $\tilde{f}_\alpha(x)$ are $\frac{d \pm \sqrt{d}}{2}$, which makes sense if d is a square modulo p , since 2 is a unit in \mathbb{F}_p . Thus, if d is a square modulo p , then since $d \not\equiv 0$ and $p > 2$ we see that the zeros of $\tilde{f}_\alpha(x)$ are distinct and so p splits: $pA = P_1 P_2$. If d is not a square modulo p , then $\tilde{f}_\alpha(x)$ is irreducible and p is inert: $pA = P$.

We should note that we can use the Legendre symbol $\left(\frac{d}{p}\right)$ to summarize. Recall that if p is a prime which does not divide an integer a , then

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square modulo } p, \\ -1 & \text{if } a \text{ is not a square modulo } p \end{cases}$$

Thus, for any prime p

$$pA = \begin{cases} P^2 & \text{if } p|d, \\ P_1 P_2 & \text{if } p = 2 \text{ and } d \equiv 1 \pmod{8}, \text{ or if } p > 2 \text{ and } \left(\frac{d}{p}\right) = 1, \\ P & \text{if } p = 2 \text{ and } d \equiv 5 \pmod{8}, \text{ or if } p > 2 \text{ and } \left(\frac{d}{p}\right) = -1, \end{cases}$$

The basic properties of the Legendre symbol may be found in almost any basic text on number theory. Probably the most fundamental result is the Law of Quadratic Reciprocity.

Theorem. (Gauss) If p and q are distinct odd primes, then

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

from which it follows that

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4}, \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod{4} \end{cases}$$

Furthermore,

$$\left(\frac{2}{p}\right) = (-1)^{\left(\frac{p^2-1}{8}\right)}$$

It is unexpected but true that all cases of quadratic reciprocity are roughly equivalent to the fact that the factorization of p in A depends only on the residue class of p modulo d .

For example, if ℓ is an odd prime such that $\ell \equiv 1 \pmod{4}$ and $k = \mathbb{Q}(\sqrt{\ell})$, then the discriminant is $d = \ell$ and we have the following factorizations:

$$2A = \begin{cases} P_1 P_2 & \text{if } \ell \equiv 1 \pmod{8} \text{ iff } \left(\frac{2}{\ell}\right) = 1 \text{ by quadratic reciprocity} \\ P & \text{if } \ell \equiv 5 \pmod{8} \text{ iff } \left(\frac{2}{\ell}\right) = -1 \text{ by quadratic reciprocity} \end{cases}$$

and if p is an odd prime distinct from ℓ

$$pA = \begin{cases} P_1 P_2 & \text{if } \left(\frac{\ell}{p}\right) = 1 \text{ iff } \left(\frac{p}{\ell}\right) = 1 \text{ by quadratic reciprocity} \\ P & \text{if } \left(\frac{\ell}{p}\right) = -1 \text{ iff } \left(\frac{p}{\ell}\right) = -1 \text{ by quadratic reciprocity} \end{cases}$$

which shows that the factorization of pA (whether pA is split or inert) depends only on p modulo $\ell = d$.

If ℓ is an odd prime such that $\ell \equiv 3 \pmod{4}$ and $k = \mathbb{Q}(\sqrt{-\ell})$, then the discriminant is $d = -\ell \equiv 1 \pmod{4}$ and we have the following factorizations:

$$pA = \begin{cases} P_1 P_2 & \text{if } \left(\frac{-\ell}{p}\right) = 1 = \left(\frac{p}{\ell}\right) \\ P & \text{if } \left(\frac{-\ell}{p}\right) = -1 = \left(\frac{p}{\ell}\right) \end{cases}$$

which is the same behavior as the previous example.

Assume that $d = -4$, so that $k = \mathbb{Q}(i)$ and $A = \mathbb{Z}[i]$. Then for an odd prime p , pA is split iff $p \equiv 1 \pmod{4}$ and is inert iff $p \equiv 3 \pmod{4}$. The ideal $2A$ is ramified and $\mathcal{D} = 2A = P^2$.

In fact, for any quadratic field k , there exists a group homomorphism $\chi : (\mathbb{Z}/d\mathbb{Z})^\times \rightarrow \{\pm 1\}$ such that pA splits iff $\chi(p) = 1$, and pA is inert iff $\chi(p) = -1$. In the cases $\mathbb{Q}(\sqrt{\pm\ell})$ above, we see that $\chi(p) = \left(\frac{p}{\ell}\right) : (\mathbb{Z}/\ell\mathbb{Z})^\times \rightarrow \{\pm 1\}$. χ is necessarily unique, by the given property.

For any number field k , let T denote the set of nonzero prime ideals of A . Let U denote the prime numbers, and consider the following function of s :

$$\prod_{P \in T} \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1} = \prod_{p \in U} \underbrace{\left(\prod_{P \supseteq pA} \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1}\right)}_{\text{at most } n \text{ factors}}$$

For example, if $n = 1$ so that $k = \mathbb{Q}$ and $A = \mathbb{Z}$, then this function is

$$\prod_{p \in U} \left(1 - \frac{1}{p^s}\right)^{-1}$$

If $n = 2$, then there are three options for the factor corresponding to the prime number p :

$$\begin{aligned}
pA = P^2 & \quad \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1} = \left(1 - \frac{1}{p^s}\right)^{-1} & (1) \\
pA = P & \quad \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1} = \left(1 - \frac{1}{p^{2s}}\right)^{-1} \\
& \quad = \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{-1} \\
& \quad = \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \\
pA = P_1 P_2 & \quad \left(1 - \frac{1}{\mathbb{N}(P)^s}\right)^{-1} = \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{1}{p^s}\right)^{-1} \\
& \quad = \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}
\end{aligned}$$

Thus, in each unramified case, the factor corresponding to p is

$$\left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

Example. We consider the factorization of the ideals pA in a cyclotomic field. Let ℓ be an odd prime number, $\zeta = \zeta_\ell$ a primitive ℓ th root of unity, and $k = \mathbb{Q}(\zeta)$. Let $\phi(x) = x^{\ell-1} + x^{\ell-2} + \cdots + 1$ so that ζ satisfies the polynomial $x^\ell - 1 = (x-1)\phi(x)$. We claim that $\phi(x)$ is irreducible over \mathbb{Q} . To see this, let $\pi = \zeta - 1$, which satisfies the polynomial

$$\phi(1+y) = \frac{(1+y)^\ell - 1}{(1+y) - 1} = \frac{y^\ell + \binom{\ell}{1}y^{\ell-1} + \cdots + \ell y + 1 - 1}{y} = y^{\ell-1} + \binom{\ell}{1}y^{\ell-2} + \cdots + \ell$$

This polynomial is monic, ℓ divides all the non-leading coefficients and ℓ^2 does not divide the constant term. Therefore, by Eisenstein's criterion, $\phi(1+y)$ is irreducible over \mathbb{Q} , and the same is true for $\phi(x)$. Since $\phi(1+y)$ is the minimal polynomial of π and ℓ is odd, $\mathbb{N}(\pi) = \ell$ the constant term of $\phi(1+y)$. Similarly, $\mathbb{N}(\zeta) = 1$.

We note, for historical interest, that Kummer studied cyclotomic fields extensively. He discovered that the ring of integers in this case is not a principal ideal domain (although, not in those terms) and developed the theory of ideals as a result.

Lecture 7

We continue with the notation from the previous lecture. Let $\sigma_1, \dots, \sigma_{\ell-1}$ be the distinct \mathbb{Q} -embeddings of k into \mathbb{C} . If we assume that $\zeta \in \mathbb{C}$, then we may assume that $\sigma_i(\zeta) = \zeta^i$. Since $\ell = \mathbb{N}(\pi) = \prod_{i=1}^{\ell-1} \sigma_i(\pi) = \pi(\zeta^2 - 1) \cdots (\zeta^{\ell-1} - 1)$, we see that π divides ℓ in A . In particular, $\ell A \subseteq \pi A \subseteq A$.

Proposition 36. *The ring of integers in k is $A = \mathbb{Z}[\zeta] = \mathbb{Z}[\pi]$.*

Proof. The second equality is clear. Let $B = \mathbb{Z}[\zeta] = \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{\ell-2}$. Then $d_B = \text{disc}(B) = \det(\sigma_i(\zeta^j))^2$ as we noted in the proof of Proposition 10. This is exactly

$$d_B = \det \begin{pmatrix} 1 & \zeta & \zeta^2 & \cdots & \zeta^{\ell-1} \\ 1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{2(\ell-1)} \\ 1 & \zeta^3 & \zeta^6 & \cdots & \zeta^{3(\ell-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{\ell-1} & \zeta^{2(\ell-1)} & \cdots & \zeta^{(\ell-1)(\ell-1)} \end{pmatrix}^2 = \prod_{i < j} (\zeta^i - \zeta^j)^2$$

since this is the Vandermonde determinant. Using the fact that $\zeta^i - \zeta^j = \zeta^i(1 - \zeta^{j-i}) = -\sigma_i(\zeta)\sigma_{j-i}(\pi)$ and some bookkeeping, we see that

$$d_B = \prod_{i < j} (\zeta^i - \zeta^j)^2 = \pm (\mathbb{N}(\zeta))^{\ell-2} (\mathbb{N}(\pi))^{\ell-2} = \pm \ell^{\ell-2}$$

Since $\ell > 2$ is prime, all the embeddings of k are complex. Thus, $r_2 = \frac{\ell-1}{2}$ and Corollary 15 implies that $d_B = (-1)^{\binom{\ell-1}{2}} \ell^{\ell-2}$. By Proposition 1,

$$\ell^{\ell-2} = |d_B| = (B^* : B) = (B^* : A^*)(A^* : A)(A : B) \geq (A^* : A).$$

The following proposition will help us complete the proof.

Proposition 37. $\frac{\pi}{\ell}A \subseteq A^*$.

Before we prove Proposition 37, we complete the proof of Proposition 36. By Lemma 20, $(A : \pi A) = |\mathbb{N}(\pi)| = \ell$, and since A is a lattice of rank $\ell-1$, $(A : \ell A) = \ell^{\ell-1}$. The inclusions $\ell A \subseteq \pi A \subseteq A$ imply that $(\pi A : \ell A) = \ell^{\ell-2}$. Dividing the inclusion $\ell A \subseteq \pi A$ by ℓ gives $A \subseteq \frac{\pi}{\ell}A \subseteq A^*$ so that

$$\ell^{\ell-2} \geq (A^* : A) \geq \left(\frac{\pi}{\ell}A : A\right) = (\pi A : \ell A) = \ell^{\ell-2}$$

which implies equality. It follows that $A = B$ and $A^* = \frac{\pi}{\ell}A$. \square

Proof of Proposition 37. It suffices to show that $\text{Tr}(\frac{\pi}{\ell}A) \subseteq \mathbb{Z}$. This occurs if and only if $\text{Tr}(\pi A) \subseteq \ell\mathbb{Z}$. For $\alpha \in A$,

$$\begin{aligned} \text{Tr}(\pi\alpha) &= \text{Tr}((\zeta-1)\alpha) = \sum_{i=1}^{\ell-1} \sigma_i(\zeta-1)\sigma_i(\alpha) \\ &= \sum_{i=1}^{\ell-1} (\zeta^i - 1)\sigma_i(\alpha) = \sum_{i=1}^{\ell-1} (\zeta-1)(\zeta^{i-1} + \cdots + 1)\sigma_i(\alpha) \\ &\in \pi A \cap \mathbb{Z} \end{aligned}$$

so it suffices to show that $\pi A \cap \mathbb{Z} = \ell\mathbb{Z}$. Since $\pi A \cap \mathbb{Z}$ is an ideal in \mathbb{Z} and $\ell\mathbb{Z} \subseteq \pi A \cap \mathbb{Z}$ and $\ell\mathbb{Z}$ is maximal, either $\pi A \cap \mathbb{Z} = \mathbb{Z}$ or $\pi A \cap \mathbb{Z} = \ell\mathbb{Z}$. If $\pi A \cap \mathbb{Z} = \mathbb{Z}$ then π is a unit in A so that $\pi A = A$. But we have already seen that $(A : \pi A) = \ell > 2$, a contradiction. \square

It follows from the proof that $\mathcal{D} = (\frac{\ell}{\pi})A$.

We now return to the task of factoring the ideals pA . First, the ideal ℓA is completely ramified, in the sense that $\ell A = P^{\ell-1}$ where P has residue degree $f = 1$ and ramification index $e = \ell - 1 = n$, and $\mathbb{N}(P) = \ell$. Let $P = \pi A$, which is prime since $A/P = \mathbb{Z}[\pi]/(\pi) = \mathbb{F}_\ell$. Suppose that $\ell A = P^e \prod_i P_i^{e_i}$ with $e_i \geq 1$. Since $P \supseteq \ell A$, we know that $e \geq 1$. Furthermore, since P and each P_i has characteristic ℓ

$$\ell^{\ell-1} = \mathbb{N}(\ell) = \mathbb{N}(P^e \prod_i P_i^{e_i}) = \mathbb{N}(P)^e \prod_i \mathbb{N}(P_i)^{e_i} \geq \ell^{(e+\sum_i e_i)}$$

so that $e, e_i < \ell$. In particular, e and the e_i are not divisible by ℓ . By Proposition 33, we see that the factorization of \mathcal{D} contains P^{e-1} and $P_i^{e_i-1}$ so that

$$P^{e-1} \prod_i P_i^{e_i} = \frac{\ell}{\pi} A = \mathcal{D} \subseteq P^{e-1} \prod_i P_i^{e_i-1}$$

so that each $e_i \geq e_i - 1$, a contradiction. Thus, $\ell A = P^e$ and $\ell^{\ell-1} = \mathbb{N}(\ell) = \mathbb{N}(P)^e = \ell^e$ so that $e = \ell - 1$, as claimed.

If $p \neq \ell$, then by our computation in Proposition 37, $|d| = \ell^{\ell-2}$ so that $p \nmid d$. By Corollary 32, the ideal pA completely splits as $pA = \prod_i P_i$ and the factorization of pA mirrors the factorization of $\phi(x)$ modulo p . When does $\phi(x)$ have a linear factor modulo p ? This occurs iff there is an ℓ th root of unity in \mathbb{F}_p^\times . Since \mathbb{F}_p^\times is cyclic of order $p - 1$, such an element exists iff \mathbb{F}_p^\times contains a subgroup of order ℓ iff $\ell | p - 1$ iff $p \equiv 1 \pmod{\ell}$. In this case, though, \mathbb{F}_p^\times has $\ell - 1$ distinct elements of order ℓ and so $\phi(x)$ splits into distinct linear factors modulo p and $pA = P_1 \cdots P_{\ell-1}$.

In general, let f be the smallest integer such that $\ell | (p^f - 1)$, that is, f is the order of p in \mathbb{F}_ℓ^\times . Then $pA = P_1 \cdots P_g$ for distinct P_i such that $\mathbb{N}(P_i) = p^f$ and $g = \frac{\ell-1}{f}$. The same reasoning as above shows that $\phi(x)$ splits completely over \mathbb{F}_{p^f} . Each zero of $\phi(x)$ in \mathbb{F}_{p^f} has f distinct conjugates, and the coefficients of the factors of $\phi(x)$ modulo p will be the symmetric polynomials in these conjugates. It follows that, modulo p , $\phi(x)$ factors into g distinct factors, each of degree f .

Example. If $\ell = 3$, then $\zeta = \frac{-1+\sqrt{-3}}{2}$ so that $k = \mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$. By our work above, we know that $3A = P^2$. If $p \equiv 1 \pmod{3}$, then $pA = P_1 P_2$. If $p \equiv -1 \pmod{3}$, then $f = 2$ and $g = 1$ so that $pA = P$.

Example. If $\ell = 5$, then $\mathbb{F}_5^\times \cong \mathbb{Z}/4\mathbb{Z}$. As before, $5A = P^4$. If $p \equiv 1 \pmod{5}$, then pA splits completely as $pA = P_1 P_2 P_3 P_4$. If $p \equiv -1 \pmod{5}$, then $f = 2$ and $g = 2$ so that $pA = P_1 P_2$. If $p \equiv 2, 3 \pmod{5}$, then $f = 4$ and $g = 1$ so that $pA = P$.

We observe that a cyclotomic field k is always Galois over \mathbb{Q} . The extension is separable because $\text{char}(\mathbb{Q}) = 0$, and it is normal since the conjugates of ζ are simply $\zeta^i \in k$. Furthermore, the Galois group $G = \text{Gal}(K/\mathbb{Q}) = (\mathbb{F}_\ell)^\times$. The homomorphism $\psi : G \rightarrow (\mathbb{F}_\ell)^\times$ is given by $\sigma \mapsto a \pmod{\ell}$ where $\sigma(\zeta) = \zeta^a$. The map ψ is always an injection, and the irreducibility of $\phi(x)$ implies that ψ is also a surjection.

Back in the case $\ell = 5$, $G = \mathbb{Z}/4\mathbb{Z}$ has a unique subgroup of index 2. The Galois correspondence implies that there is a unique quadratic subfield L of k . If $\alpha = \zeta + \zeta^{-1}$, then $\mathbb{Q}(\alpha) \subsetneq k$ since α is real and $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha)$ since α is irrational. Thus, $\mathbb{Q}(\alpha)$ must be the unique quadratic subfield of k . It will follow from the following theorem that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$.

Theorem 38. (Gauss) Assume that ℓ is a prime number, $\ell > 2$, and $\zeta = \zeta_\ell \in \mathbb{C}$ is a primitive ℓ th root of unity. Let $k = \mathbb{Q}(\zeta)$. Then there is a unique quadratic subfield L of k , and $L = \mathbb{Q}(\sqrt{(-1)^{\frac{\ell-1}{2}}\ell})$.

Compare this to the theorem which states that every quadratic field is contained in a cyclotomic field (cf. Lang, *Algebra*, Theorem VI.3.3).

Proof. As we noted before, k is Galois over \mathbb{Q} with Galois group $G = \mathbb{F}_\ell^\times = \mathbb{Z}/(\ell-1)\mathbb{Z}$. Since ℓ is odd, G has a unique subgroup of index 2, which implies that k has a unique quadratic subfield. Let

$$D = (-1)^{\frac{\ell-1}{2}}\ell \quad \text{and} \quad g = \sum_{a=1}^{\ell-1} \left(\frac{a}{\ell}\right) \zeta^a$$

It is not difficult to show that $g^2 = D$ (cf. Lang, *Algebra*, Theorem VI.3.3). Thus, $L = \mathbb{Q}(g) = \mathbb{Q}(\sqrt{D})$ is the desired subfield. \square

Of course, the fields we have studied in depth thus far have all been Galois and cyclic over \mathbb{Q} . This has made our computations relatively easy. The following example involves an extension with Galois group S_3 , and we omit proofs of many of the facts.

Example. Let $f(x) = x^3 - x - 1$ and $\alpha \in \mathbb{C}$ a zero of $f(x)$. Any rational zero of $f(x)$ would necessarily be ± 1 , so $f(x)$ is irreducible. Let $k = \mathbb{Q}(\alpha)$ and let K be a splitting field of $f(x)$ over \mathbb{Q} . The discriminant of $f(x)$ is -23 and therefore not a square, so that k is not Galois over \mathbb{Q} and the Galois group of $f(x)$ is $G = \text{Gal}(K/\mathbb{Q}) = S_3$. The ring of algebraic integers in k is $A = \mathbb{Z}[\alpha]$ and $d = \text{disc}(A) = -23$. Modulo 23, $f(x)$ factors as $(x-3)(x-10)^2$. Thus, by Corollary 32, $23A = P_1P_2^2$ where the residue degrees are $f_1 = f_2 = 1$. In fact, $P_2 = \mathcal{D}$ has index 23 in A . If $p \neq 23$ then there is no ramification. When $\left(\frac{p}{23}\right) = -1$, i.e. p is not a square modulo 23, $pA = P_1P_2$ where $f_1 = 1$ and $f_2 = 2$. When $\left(\frac{p}{23}\right) = 1$, either $pA = P_1P_2P_3$ with the $f_i = 1$ or $pA = P$ with $f = 3$. These different possibilities mirror the different quadratic forms $x^2 + xy + 6y^2$ and $2x^2 + xy + 3y^2$ with discriminant -23 as in Lecture 3: pA splits completely when $p = x^2 + xy + 6y^2$ for integers x, y , and pA is inert when $p = 2x^2 + xy + 3y^2$ for integers x, y .

We note that prime factorization is known explicitly in relatively few cases. For example, if k has degree 5 over \mathbb{Q} and has nonsolvable Galois closure, then a simple recipe for prime factorization is not known.

Now, we are ready to build the machinery to finish the proof of Theorem 30. We state the result in more generality, as a separate theorem.

Theorem 39. (Unit Theorem) Assume that k is a number field and that B is an order in k . Then the group of units B^\times is a finitely generated abelian group. Furthermore, the torsion subgroup of B^\times is cyclic of finite order, and the rank of B^\times is $r = r_1 + r_2 - 1$. Finally, if $r_1 \neq 0$, then $B_{\text{tor}}^\times = \{\pm 1\}$.

It should be noted that the torsion subgroup of B^\times is exactly the set of roots of unity in B , since an element $\alpha \in B$ is torsion iff $\alpha^s = 1$ for some integer s .

Example. If $k = \mathbb{Q}$, then $r_1 = 1$ and $r_2 = 0$ so that $A^\times = \{\pm 1\}$, not that this is a surprise.

If $k = \mathbb{Q}(\sqrt{-D})$ for a positive, square-free integer D , then $r_1 = 0$ and $r_2 = 1$. Thus, A^\times is torsion. If $D = 1$, then A^\times is cyclic of order 4, generated by $\sqrt{-1}$. If $D = 3$, then A^\times is cyclic of order 3, generated by $\frac{-1+\sqrt{-3}}{2}$. In all other cases, $A^\times = \{\pm 1\}$.

If $k = \mathbb{Q}(\sqrt{D})$ for a positive, square-free integer D , then $r_1 = 2$ and $r_2 = 0$. Thus, A^\times has rank 1, and since $k \subset \mathbb{R}$, the torsion subgroup is $\{\pm 1\}$. If $B = \mathbb{Z}[\sqrt{D}]$ and $\epsilon = a + b\sqrt{D}$ is a unit in B , then $a^2 - Db^2 = \mathbb{N}(\epsilon) = \pm 1$. The equation $a^2 - Db^2 = \pm 1$ is Pell's equation, which was studied in depth by Fermat, Wallis and Brounker, using continued fractions to find \sqrt{D} .

Lemma 40. *Assume that k is a number field and that B is an order in k . Then $\epsilon \in B$ is a unit in B iff $\mathbb{N}(\epsilon) = \pm 1$.*

Proof. If ϵ is a unit, then $1 = \mathbb{N}(1) = \mathbb{N}(\epsilon)\mathbb{N}(\epsilon^{-1})$, and since $\mathbb{N}(\epsilon)$ and $\mathbb{N}(\epsilon^{-1})$ are integers, $\mathbb{N}(\epsilon) = \pm 1$. Conversely, assume that $\mathbb{N}(\epsilon) = \pm 1$. The minimal polynomial of ϵ over \mathbb{Q} is $x^m - \text{Tr}(\epsilon)x^{m-1} + \dots + \pm \mathbb{N}(\epsilon)$. Thus, $\epsilon(\epsilon^{m-1} - \text{Tr}(\epsilon)\epsilon^{m-2} + \dots) = \pm \mathbb{N}(\epsilon) = \pm 1$. Since the element $\epsilon^{m-1} - \text{Tr}(\epsilon)\epsilon^{m-2} + \dots$ is in B , we see that ϵ is a unit in B . \square

Given a number field k , there are r_1 distinct embeddings of k in \mathbb{R} , and there are $2r_2$ distinct embeddings of k in \mathbb{C} whose images are not contained in \mathbb{R} . We construct $r_1 + r_2$ valuations $v : k^\times \rightarrow \mathbb{R}^\times$ corresponding to the embeddings. Recall that a valuation on k is a homomorphism of multiplicative groups $|\cdot| : k^\times \rightarrow \mathbb{R}^\times$ such that $|\alpha + \beta| \leq |\alpha| + |\beta|$. We shall use the notation $|\alpha|_v$ in place of $v(\alpha)$ to remind us that v is a valuation. If $\sigma : k \rightarrow \mathbb{R}$, then define $|\alpha|_v = |\sigma(\alpha)|$ where $|\cdot|$ represents the usual absolute value on \mathbb{R} . If $\sigma : k \rightarrow \mathbb{C}$ is a strictly complex embedding, then let $|\alpha|_v = |\sigma(\alpha)|^2$ where $|\cdot|$ is the usual absolute value on \mathbb{C} . If $\bar{\sigma} : k \rightarrow \mathbb{C}$ is the conjugate embedding, then it follows that $|\alpha|_v = \sigma(\alpha)\bar{\sigma}(\alpha)$, so this does not depend on the choice of representative of conjugacy class. We refer to the valuations constructed in this manner as the *infinite* valuations, and we say that the valuation *divides* ∞ . Also, an *infinite place* is one of the following: a real embedding of k or a conjugate pair of complex embeddings.

Claim: For any nonzero $\alpha \in A$, $\prod_{r_1+r_2} |\alpha|_v = |\mathbb{N}(\alpha)| \in \mathbb{Q}_+^\times$, where the product is taken over the distinct infinite valuations of k . To see this, we compute

$$|\mathbb{N}(\alpha)| = \prod_{i=1}^n |\sigma(\alpha)| = \prod_{\mathbb{R} \text{ plc.}} |\sigma(\alpha)| \cdot \prod_{\mathbb{C} \text{ plc.}} \sigma(\alpha)\bar{\sigma}(\alpha) = \prod_{r_1+r_2} |\alpha|_v$$

as claimed.

Corollary 41. *A nonzero element $\alpha \in A$ is a unit iff $\prod_{r_1+r_2} |\alpha|_v = 1$.*

Example. If $k = \mathbb{Q}(\sqrt{D})$ for a positive, square-free integer D , then $r_1 = 2$ and $r_2 = 0$. If $\epsilon = a + b\sqrt{D} \neq \pm 1$ is a unit in A , then $|\epsilon|_1 > 1$ and $|\epsilon|_2 < 1$ so that either $|a + b\sqrt{D}| > 1$ and $|a - b\sqrt{D}| < 1$ or vice versa. We shall generalize this example in the next lecture.

We can also find valuations corresponding to nonzero prime ideals P of A . For $\alpha \in k^\times$, let $\text{ord}_P(\alpha) = \text{ord}_P(\alpha A)$ as in Lecture 4, and define $|\alpha|_P = \mathbb{N}(P)^{-\text{ord}_P(\alpha)} = q^{\text{ord}_P(\alpha)}$ where $q = \mathbb{N}(P) = p^f$. The image of $|\cdot|_P$ in $\mathbb{R}_+^\times \cong \mathbb{R}$ is exactly $q^{\mathbb{Z}}$. In this case, we have $|\alpha + \beta|_P \leq \max\{|\alpha|, |\beta|\}$. A valuation which satisfies this property is called *non-archimedean*. The valuations constructed in this manner are the *finite* valuations on k .

Theorem 42. (*Product Formula*) If $\alpha \in k^\times$, then $|\alpha|_v = 1$ for almost all valuations defined thus far, and $\prod_{\text{all } v} |\alpha|_v = 1$.

Proof. For any such α there exist an integer N and nonzero $\beta \in A$ such that $\alpha = \frac{\beta}{N}$, so we may assume without loss of generality that $\alpha \in A$. Then $\alpha A = \prod_i P_i^{m_i}$, so the only possible valuations v with $|\alpha|_v \neq 1$ are the infinite valuations (a finite number) and those from the product with $m_i \geq 1$. Furthermore,

$$\begin{aligned} \prod_{\text{all } v} |\alpha|_v &= \prod_{v|\infty} |\alpha|_v \cdot \prod_P |\alpha|_P = |\mathbb{N}(\alpha)| \cdot \prod_i \mathbb{N}(P_i)^{-m_i} \\ &= |\mathbb{N}(\alpha)| \cdot (A : \alpha A)^{-1} = |\mathbb{N}(\alpha)| \cdot |\mathbb{N}(\alpha)|^{-1} = 1 \end{aligned}$$

as claimed. \square

It follows from the proof that $\alpha \in A$ iff $|\alpha|_P \leq 1$ for all prime ideals P , and $\alpha \in A^\times$ iff $|\alpha|_P = 1$ for all prime ideals P .

Corollary 43. For all $\alpha \in A^\times$, $\prod_{v|\infty} |\alpha|_v = 1$.

Lecture 8

We continue with the notation from last lecture.

Proposition 44. Assume that $r_1 + r_2 \geq 2$, and fix an infinite valuation v . Let B be an order in k . Then there exists a unit $\epsilon \in B^\times$ such that $|\epsilon|_v < 1$ and for all infinite valuations $w \neq v$, $|\epsilon|_w < 1$.

Proof. For any $t = (t_1, \dots, t_{r_1+r_2}) \in \mathbb{R}_+^{r_1+r_2}$ let $P_t \subset k \otimes \mathbb{R} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ be the region

$$P_t = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : |x|_v < t_v \text{ for all } v\}$$

The numbers t_1, \dots, t_{r_1} are radii of intervals. The $t_{r_1+1}, \dots, t_{r_1+r_2}$ are square roots of radii of circles, as $z\bar{z} < t_v \Rightarrow |z| < \sqrt{t_v}$, which implies that the area of the circle is πt_v . Then \overline{P}_t is a closed, bounded, convex, centrally symmetric subset of Euclidean space. Also, $\text{Vol}(P_t) = 2^{r_1} \pi^{r_2} \prod_{r_1+r_2} t_v$. Let $M = \prod_{r_1+r_2} t_v$ and choose t and t' so that $\overline{P}_{t'} \subset P_t$ and $M' = (\frac{2}{\pi})^{r_2} |d_B|^{1/2} = M + 1$. Then $\text{Vol}(P_{t'}) = 2^{r_1+r_2} |d_B|^{1/2} = 2^n \text{Vol}(D)$ where D is the fundamental domain of B acting on $k \otimes \mathbb{R}$. It follows from Theorem 16 that $\overline{P}_{t'}$ contains a nonzero element α of B , and by our choices $\alpha \in P_t \cap B$. Since α is an algebraic integer, $|\mathbb{N}(\alpha)| \geq 1$. By construction $|\mathbb{N}(\alpha)| < M + 1$. So, α is an element of small norm. There is no reason *a priori* why we should expect α to satisfy the properties we desire from ϵ . However, we apply the following strategy to generate ϵ . (We say “generate” instead of “construct” because this method is *not* an efficient way to calculate ϵ in practice.) We shall construct elements α_i of B with small norm, and it will follow that $\alpha_i B = \alpha_j B$ for some $i \neq j$. Then $\alpha_i = \alpha_j \epsilon$ for some unit ϵ .

For $\delta > 0$, let $t_w = \delta$ for $w \neq v$ and $t_v = M/\delta^{(r_1+r_2-1)}$, and let $P(\delta)$ denote the corresponding P_t . (Here, we are taking “small” values of δ .) These choices for t give us a nonzero

$\alpha \in P(\delta) \cap B$. By construction, if $w \neq v$, then $0 < |\alpha|_w < \delta$. We claim that $|\alpha|_w \geq \frac{\delta}{M}$, so that these values are bounded away from zero. Fix some $w_0 \neq v$, and suppose that $|\alpha|_{w_0} < \frac{\delta}{M}$. Then

$$1 \leq |\mathbb{N}(\alpha)| = |\alpha|_{w_0} \cdot |\alpha|_v \cdot \prod_{w \neq v, w_0} |\alpha|_w < \frac{\delta}{M} \left(\frac{M}{\delta^{(r_1+r_2-1)}} \right) \delta^{(r_1+r_2-2)} = 1$$

a contradiction.

Let c be the number of ideals I of B such that $\mathbb{N}(I) \leq M+1$. (As noted before, c is finite.) For $i = 0, 1, 2, \dots, c$ fix nonzero $\alpha_i \in P(\frac{\delta}{M^i}) \cap B$. Since the set $\{\alpha_i B\}$ consists of $c+1$ ideals of norm $\mathbb{N}(\alpha_i B) = |\mathbb{N}(\alpha)| < M+1$, it follows that some $\alpha_i B = \alpha_j B$ for $0 \leq i < j \leq c$. Let $\epsilon = \alpha_i / \alpha_j$, which is an element of B^\times . Then, for $w \neq v$, $|\alpha_i|_w \geq \frac{\delta}{M^{i+1}}$ and $|\alpha_j|_w < \frac{\delta}{M^j}$, which implies that

$$|\epsilon|_w = \frac{|\alpha_i|_w}{|\alpha_j|_w} > \frac{(\delta/M^{i+1})}{(\delta/M^j)} = \frac{M^j}{M^{i+1}} \geq 1$$

Furthermore, by Corollary 43, $1 = |\alpha|_v \cdot \prod_{w \neq v} |\alpha|_w < |\alpha|_v$, as desired. \square

If B is an order in a number field k , define a group homomorphism

$$\lambda : B^\times \rightarrow \bigoplus_{v|\infty} \mathbb{R}v = \mathbb{R}^{(r_1+r_2)} \quad \text{as} \quad \lambda(\epsilon) = \sum_v \log |\epsilon|_v \cdot v.$$

Since $\mathbb{R}^{(r_1+r_2)}$ is torsion-free, it is clear that the torsion subgroup of B^\times is in the kernel of λ . Also, the fact that $\prod_{v|\infty} |\epsilon|_v = 1$ implies that the image of λ is contained in the hyperplane $H = \{\sum_v a_v v : \sum_v a_v = 0\}$, since $\sum_v \log |\epsilon|_v = 0$. We can now formulate the Unit Theorem in terms of λ .

Theorem 45. (*Unit Theorem*) *Assume that k is a number field and that B is an order in k . Then the group of units B^\times is a finitely generated abelian group. In fact,*

1. *The torsion subgroup of B^\times is cyclic of finite order and equal to $\ker(\lambda)$.*
2. *The image of λ is a lattice in H , that is, a discrete, co-compact subgroup. Therefore, the rank of B^\times is $r = r_1 + r_2 - 1$.*
3. *If $r_1 \neq 0$, then $B_{\text{tor}}^\times = \{\pm 1\}$.*

Proof. First, we note that, if we can prove that B_{tor}^\times is finite, then the fact that it consists exactly of the roots of unity in B implies that it is cyclic. Second, if $r_1 \neq 0$, then there is a real embedding of k . Since roots of unity map to roots of unity, this implies that the only roots of unity in k are ± 1 .

Let S be a compact subset of H . Then $\lambda^{-1}(S)$ is contained in the intersection of B with a bounded subset of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = k \otimes \mathbb{R}$. Since B is discrete in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, it follows that $\lambda^{-1}(S)$ is finite. Let $S = \{0\}$ to see that $\ker(\lambda) \supseteq B_{\text{tor}}^\times$ is finite. The fact that $\ker(\lambda)$ is finite implies that it is torsion, so that it is contained in (and therefore equal to) the set of roots of unity in B . This implies 1.

The argument of the preceding paragraph implies that $\text{Im}(\lambda)$ is discrete in H . To show that $\text{Im}(\lambda)$ is co-compact in H , we must show that the \mathbb{R} -span of $\text{Im}(\lambda)$ is H . It suffices to show that if a linear form $\ell = \sum_v a_v x_v$ vanishes on $\text{Im}(\lambda)$, then it vanishes on H , i.e., all a_v are equal since $H = \{(x_v) : \sum_v x_v = 0\}$. If $r_1 + r_2 < 2$ then there are two cases. Case 1: $r_1 = 1$ and $r_2 = 0$. In this case $k = \mathbb{Q}$ and the result is trivial. Case 2: $r_1 = 0$ and $r_2 = 1$. In this case, k is a purely imaginary quadratic field, which we checked explicitly in the previous lecture. Thus, we assume without loss of generality that k has at least two places.

If the form ℓ vanishes on $\text{Im}(\lambda)$, then $\sum_v a_v \log |\epsilon|_v = 0$ for all $\epsilon \in B^\times$. Let v_0 be a place such that $a_{v_0} \leq a_v$ for all v , and let $\ell' = \ell - a_{v_0} \sum_v x_v$. Then all the coefficients of ℓ' are nonnegative, and the coefficient of x_{v_0} is 0. Furthermore, ℓ' vanishes on $\text{Im}(\lambda)$ because ℓ vanishes on $\text{Im}(\lambda)$ and $a_{v_0} \sum_v x_v$ vanishes on H . It suffices to show that $\ell' = 0$. By Proposition 44, there is an element $\epsilon \in B^\times$ such that $|\epsilon|_{v_0} < 1$ and for $w \neq v_0$, $|\epsilon|_w > 1$. If some $a'_w > 0$, then

$$0 = \ell'(\lambda(\epsilon)) = \sum_v a'_v \log |\epsilon|_v = \sum_{w \neq v_0} a'_w \log |\epsilon|_w > 0$$

a contradiction. □

We sketch a generalization of the ideas behind the Unit Theorem. Recall that

$$A = \{\alpha \in k : |\alpha|_P \leq 1 \text{ for all } P\}$$

and

$$A^\times = \{\alpha \in k : |\alpha|_P = 1 \text{ for all } P\} = \{\alpha \in k : |\alpha|_v = 1 \text{ for all finite valuations } v\}.$$

Let S be a finite set of valuations of k which contains the infinite valuations. That is, S consists of all $r_1 + r_2$ infinite valuations and a finite number of the finite valuations. Let A_S denote the set $A_S = \{\alpha \in k : |\alpha|_v \leq 1 \text{ for all } v \notin S\}$. In other words, A_S consists of the elements α of k such that the only primes with negative ramification index in the prime decomposition of αA must be in S . A_S is a ring containing A , and we sometimes denote A_S by $A[1/P]_{P \in S}$. The Generalized Unit Theorem states that the group of units of A_S is exactly $A^\times = \{\alpha \in k : |\alpha|_v = 1 \text{ for all } v \notin S\}$. The proof is similar to that of the Unit Theorem. The main tool is the homomorphism of groups

$$\lambda_S : A_S^\times \rightarrow \bigoplus_{v \in S} \mathbb{R}v \quad \text{given by} \quad \lambda_S(\epsilon) = \sum_{v \in S} \log |\epsilon|_v v.$$

The kernel of λ_S is $(A_S^\times)_{\text{tor}}$, which is finite and consists of roots of unity. The image of λ_S is a lattice in the hyperplane $H_S = \{(x_v)_{v \in S} : \sum_{v \in S} x_v = 0\}$ and therefore the rank of A_S^\times is $\dim(H) = \#(S) - 1$. The details are left to the interested reader. We will, however, consider a few examples.

Example. Let $k = \mathbb{Q}$ so that $A = \mathbb{Z}$, and let $S = \{\infty, p\}$ for some prime number p . (By saying that $\infty \in S$, we mean that the unique (real) embedding of \mathbb{Q} is in S .) Then $A_S = \mathbb{Z}[1/p] = \{\frac{a}{p^r} : r \in \mathbb{Z}\}$. A contains the units ± 1 as well as the new unit p . It follows that $A_S^\times = \{\pm 1\} \times p^{\mathbb{Z}}$.

Example. Assume that A is the ring of algebraic integers in an arbitrary number field k , and S consists of the infinite valuations and a single finite valuation, say at the prime ideal P . Fix an element $\epsilon \in A_S^\times \setminus A^\times$. Then for $Q \neq P$, $\text{ord}_Q(\epsilon) = 0$ and $\text{ord}_P(\epsilon) < 0$. It follows from the finiteness of the class group of A that $P^n = \epsilon A$ for some $n \geq 1$.