Introduction to Number Fields

B.SURY

1. Integral extensions

Definition. An element x of a ring B is *integral* over a subring A if it satisfies a monic polynomial with coefficients from A. One says B *is integral over* A if all elements of B are so.

Examples. For any n, the n-th roots of unity are integral elements of $\mathbf{C}$ over $\mathbf{Z}$. The two square roots of $1/2$ are *not* integral over $\mathbf{Z}$.

Proposition. *For rings $A \subset B$, the following are equivalent for an element x of B:*
(a) x is integral over A.
(b) The subring $A[x]$ of B generated by A and x is finitely generated as an A-module.
(c) There exists a subring C of B such that $A[x] \subset C$ and C is finitely generated as an A-module.

Proof. The assertions $(a) \Rightarrow (b)$ and $(b) \Rightarrow (c)$ are obvious. To prove the assertion $(c) \Rightarrow (a)$, start with A-module generators $y_1, \cdots, y_n$ for C. As $x \in C$, we can write $xy_i = \sum_j a_{ij} y_j$ for certain $a_{ij} \in A$.
This can be rewritten as a matrix equation $My = 0$ where y is the column made up of the y_i's and $m_{ij} = \delta_{ij} x - a_{ij}$. Multiplying on the left by the adjoint of M, we get $dy_i = 0$ where $d = \det(M)$. As y_i's generate C, we have $dC = 0$. In particular, as C is a ring, $1 \in C$, we have $d.1 = d = 0$.

But, $d = \det(\delta_{ij} x - a_{ij})$ is a monic polynomial in x over A. This proves the proposition.

Corollary. *$A \subset B$ rings. Let $x_1, \cdots, x_n \in B$. Suppose x_1 is integral over A and x_i is integral over $A[x_1, \cdots, x_{i-1}]$ for $2 \leq i \leq n$. Then, $A[x_1, \cdots, x_n]$ is finitely generated as an A-module.*

Subcorollary. *For rings $A \subset B$, the set C of elements of B integral over A is a subring of B which is integral over A.*

Definition. In the notation above, C is referred to as the *integral closure* of A in B. If A is an integral domain, it is said to be integrally closed if it equals its integral closure in its quotient field.

Examples/Exercises. *(a) Any UFD is integrally closed.*
(b) For what d is the ring $\mathbf{Z}[\sqrt{d}]$ integrally closed?

(c) If C is integral over B and B is integral over A, then C is integral over A.
(d) If C is the integral closure of A in B, then C is integrally closed in B.
(e) If $A \subset B$ and $B \setminus A$ is closed under multiplication then A is integrally closed in B.
(f) If B is integral over A and I is a non-zero ideal, then $I \cap A$ is a non-zero ideal of A and B/I is integral over $A/(I \cap A)$.

Proposition. *(a) If B is integral over A and $S \subset A$ is a multiplicative subset, then $S^{-1}B$ is integral over $S^{-1}A$.*
(b) If C is the integral closure of A in B, and $S \subset A$ is a multiplicative subset, then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

Proof. (a) is clear. For (b), start with any $b/s \in S^{-1}B$ which is integral over $S^{-1}A$. Write

$$\frac{b^n}{s^n} + \frac{a_1}{s_1}\frac{b^{n-1}}{s^{n-1}} + \cdots + \frac{a_n}{s_n} = 0 \text{ in } S^{-1}B.$$

This means that there exists $t \in S$ such that
$t((s_1 \cdots s_n b)^n + a_1(s_1 \cdots s_n b)^{n-1} s s_2 \cdots s_n + \cdots + a_n s^n s_1^n \cdots s_{n-1}^n s_n^{n-1}) = 0$ in B. Multiply by t^{n-1} to conclude that $ts_1 \cdots s_n b \in C$. This proves the proposition.

Proposition. *Let A be an integral domain. Then, the following are equivalent:*
(a) A is integrally closed.
(b) For each prime ideal P, the local ring A_P is integrally closed.
(c) For each maximal ideal M, A_M is integrally closed.

Proof. $(b) \Rightarrow (c)$ is evident. The implication $(a) \Rightarrow (b)$ is immediate from the above proposition. Finally, we prove $(c) \Rightarrow (a)$. Since all the A_M's are contained in the quotient field of A, it suffices to show that $A = \cap_M A_M$. To prove this latter statement, let us call $B = \cap_M A_M$. As $A \subset B$ is a subring with the property that $A_M \subset S^{-1}B \subset A_M$ where $S = A \setminus M$, we get $A_M = S^{-1}B$. Therefore, viewing B/A as an A-module, we have $S^{-1}(B/A) = 0$. Now, if $0 \neq b \in B/A$, then look at the ideal $I = Ann(b) := \{a \in A : ab = 0 \in B/A\}$. As $b \neq 0$, $1 \notin I$. Let $M \supset I$ be a maximal ideal of A. As $S_M^{-1}(B/A) = 0$, the image of b is zero; in other words, there exists $s \in S_M$ with $sb = 0$ in B/A. But, then $s \in I$ by the very definition of I. This is a contradiction to the assumption that $M \supset I$. The proof is complete.

Lemma. *Let $A \subset B$ be integral domains such that B is integral over A. Then, B is a field if, and only if, A is a field.*

Proof. If A is a field, consider any $0 \neq b \in B$. Writing $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ with $a_n \neq 0$, we have $-a_n^{-1}(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) = b^{-1}$. Conversely, let B be a field. Let $0 \neq a \in A$. As $a^{-1} \in B$, we may write $a^{-n} + a_1 a^{-(n-1)} + \cdots + a_n = 0$ for some $a_i \in A$. Multiplying by a^{n-1}, we get $a^{-1} \in A$.

Corollary. *Let B be integral over A. Suppose that $Q \subset B$ is a prime ideal. Then, $Q \cap A$ is a prime ideal of A which is maximal if, and only if, Q is maximal. Moreover, if $Q_0 \supset Q$ is a prime ideal of B such that $Q_0 \cap A = Q \cap A$, then $Q = Q_0$.*

Proof. The first statement is a restatement of the lemma modulo the exercise (f) above. To prove the final assertion, write $P = Q \cap A$ and $S = A \setminus P$. Then, $S^{-1}B$ is integral over $S^{-1}A$. Now, $N := S^{-1}Q \subset N_0 := S^{-1}Q_0$ are prime ideals such that $M \subset N \cap S^{-1}A \subset N_0 \cap S^{-1}A \subset S^{-1}A$. As $S \cap Q_0$ is empty, $N_0 = S^{-1}Q_0 \neq S^{-1}B$ and so $N_0 \cap S^{-1}A = S^{-1}A$. As the ring $S^{-1}A$ is a local ring with the unique maximal ideal $S^{-1}P$, we must have $M = N \cap S^{-1}A = N_0 \cap S^{-1}A$. As $S^{-1}B$ is integral over $S^{-1}A$, the prime ideals N and N_0 must be maximal as M is. But, $N \subset N_0$ so that $N = N_0$ and we get $Q = Q_0$. The proof is complete.

Going-up theorem. *Let B be integral over A. Then,*
(a) for each prime ideal P of A, there exists a prime ideal Q of B lying over P (i.e. such that $Q \cap A = P$),
(b) If $P_1 \subset P_2$ are prime ideals of A and Q_1 is a prime ideal of B lying over P_1, then there exists a prime ideal $Q_2 \supset Q_1$ of B lying over P_2.

Proof. (a) Let us localize at P i.e. let $S = A \setminus P$. Then $S^{-1}B$ is integral over $S^{-1}A$. Start with *any* maximal ideal $N \subset S^{-1}B$. Then, $N \cap S^{-1}A$ is a maximal ideal of $S^{-1}A$. Therefore, it is the unique maximal ideal $S^{-1}P$ of the local ring $S^{-1}A$. If Q is the inverse image of N in B, it is a prime ideal and must lie over P (as the composites $A \to S^{-1}A \subset S^{-1}B$ and $A \subset B \to S^{-1}B$ are equal).
(b) Write $\bar{A} = A/P_1, \bar{B} = B/Q_1$. Then, $\bar{B}$ is integral over $\bar{A}$. If $\bar{P}_2$ denotes the image of P_2 in $\bar{A}$, there is (by (a)) a prime ideal $\bar{Q}_2$ of $\bar{B}$ lying over $\bar{P}_2$. If Q_2 is the inverse image of $\bar{Q}_2$ in B, it is a prime ideal of B lying over P_2 (as the composites $A \to \bar{A} \subset \bar{B}$ and $A \subset B \to \bar{B}$ are equal).

Definition. The *dimension* of a ring A is the largest integer d for which there is a strictly increasing chain of prime ideals $P_0 \subset P_1 \subset \cdots \subset P_d$.

Examples/exercises.
(a) Any field is of dimension 0.
(b) $\mathbf{Z}$ *has dimension* 1. *In fact, the integral closure of* $\mathbf{Z}$ *in any finite field*

extension of $\mathbf{Q}$ *is of dimension* 1*; this follows from the next corollary.*
(c) The polynomial ring $K[X_1, \cdots, X_n]$ *over a field* K *has dimension* n*.*

Corollary. *If* B *is integral over* A*, then their dimensions are equal.*

2. Dedekind domains

Definition. A *Dedekind domain* is a Noetherian, integrally closed domain of dimension 1.

Remark. Sometimes one regards fields also as Dedekind domains; in that case the above definition must be refined to include dimension zero also. Note that a ring A has dimension 1 if, and only if, it is not a field and all non-zero prime ideals are maximal.

Examples/exercises.
(a) Any PID is a Dedekind domain (we shall write DD for short).
(b) $\mathbf{Z}[X]$ *is not a DD (Why?).*

Scholium. *If* L *is a finite separable extension of fields, then the 'trace form'* $Tr : L \times L \to K; (x, y) \mapsto Tr_K^L(xy)$ *is non-degenerate.*

Proposition. *Let* A *be a DD and let* L *be a finite, separable extension of the quotient field* K *of* A*. Then,* B *is a DD.*

Proof. We already know that B must have dimension 1 and must be integrally closed. To show that B is Noetherian, we prove the stronger statement that B is an A-submodule of a free A-module of rank $n = [L : K]$. If this is proved, it would follow that B is a Noetherian A-module. Any ideal of B is, in particular, an A-submodule of B and, therefore, finitely generated as an A-module (and therefore as a B-module). Thus, it suffices to show that B is an A-submodule of a free A- module of rank n. To see this, let $e_1, \cdots, e_n$ be any K-basis of L lying in B (Why is it possible to choose such a basis?). Then, if $e_1^*, \cdots, e_n^*$ is its dual basis with respect to the trace form i.e., if $Tr_K^L(e_i e_j^*) = \delta_{ij}$, then any $x \in L$ is of the form $\sum_i Tr(xe_i)e_i^*$. If $x \in B$, then all the coefficients $Tr(xe_i) \in A$ as they are integral over A. Therefore, $B \subset \sum_i Ae_i$ which is a free A-module of rank n (as e_i's are linearly independent over K). Thus, the proof is complete.

Remarks. The hypothesis of separability is not needed for the conclusion above and can be proved in this generality using the so-called Krull-Akizuki theorem. However, in the proof above, we had the intermediary assertion that B is a finitely generated A-module and this may not be true in general.

Definition. If A is an integral domain and if K denotes its quotient field,

one defines a *fractional ideal* to be a non-zero A-submodule I of K such that $I \subset d^{-1}A$ for some $d \neq 0$ in A.

Examples/exercises.
(a) Each finitely generated A-submodule of K is a fractional ideal.
(b) If A is Noetherian, each fractional ideal is finitely generated as an A-module.
(c) If I, J are fractional ideals, then so are $I \cap J, I+J, IJ$. Moreover, $IJ = JI$ and $I(JK) = (IJ)K$.

Lemma. *Let A be a Noetherian, integrally closed domain, $I \neq 0$ an ideal. If $x \in K \setminus A$, then $xI \not\subset I$.*

Proof. If $x \in K$ is so that $xI \subset I$, then $x^n I \subset I$ for all n. So, $A[x]$ is an A-submodule of K which satisfies $A[x] \subset d^{-1}A$ for some $d \neq 0$ in A (in fact, any $d \neq 0$ in I). As A is Noetherian, so is $d^{-1}A$ and thus $A[x]$ is a finitely generated A-module. This means that x is integral over A i.e. $x \in A$.

Proposition. *Let A be a DD and let P be a non-zero prime (= maximal) ideal. If K denotes the quotient field of A, then the set*

$$P' := \{x \in K : xP \subset A\}$$

is a fractional ideal of A and properly contains A. Further, P' is the unique fractional ideal such that $PP' = P'P = A$.

Proof. It is trivial to see that P' is an A-module. Moreover, evidently $P' \subset d^{-1}A$ for any $d \neq 0$ in P. Thus, P' is a fractional ideal and clearly contains A. We shall show now that $A \neq P'$. For this, we make use of the following:
Claim: Every non-zero ideal of A contains a finite product of non-zero prime ideals.
The claim is proved as follows. If there are exceptions to the claim made above, consider the family of ideals which fail to contain a product as claimed. As A is Noetherian, there exists a maximal such ideal M. So, M itself cannot be prime. If $ab \in M$ with neither a nor b in M, then the ideals $M + (a)$ and $M + (b)$ contain products of prime ideals. As M is contained in their product, M contains a product of prime ideals, which contradicts our assumption. Therefore, the claim is indeed true. Now, let $a \neq 0$ be in P. Then, the ideal $(a) \supset P_1 P_2 \cdots P_n$ with n minimal possible and P_i's non-zero primes. So, $P \supset P_1 \cdots P_n$. As P is prime, we have $P \supset P_i$ for some i, say $P \supset P_1$. As P_i are maximal, we obtain $P = P_1$. Writing $I = P_2 \cdots P_n$ or A according as $n > 1$ or $n = 1$, we get $I \not\subset (a)$ by the minimality of n. Choose any $b \in I \setminus (a)$. Then, $ba^{-1} \notin A$. Now, $PI \subset (a) \Rightarrow Pb \subset (a)$ i.e., $ba^{-1} \in P'$.

Hence, we have shown that $A \neq P'$. Further, we have $P = PA \subset PP' \subset A$ so that PP' is an (actual) ideal of A containing P. It must, therefore, be either equal to P or to the unit ideal A. If $x \in P' \setminus A$, we must have (by the above lemma) $xP \not\subset P$. This means that $xP \subset P'P \setminus P$. Thus, $PP' = A$. Finally, if P_0 is any fractional ideal such that $PP_0 = P_0P = A$, then $P' = AP' = (P_0P)P' = P_0(PP') = P_0A = P_0$ which proves uniqueness also.

Notation. One uses the notation P^{-n} instead of P'^n for any n. Then, (like ideals) one has $AP^{-n} = P^{-n}$.

Theorem. *Let A be a DD. Then, any fractional ideal $I \neq A$ can be uniquely written as $I = P_1^{n_1} \cdots P_k^{n_k}$ where n_i are non-zero integers and P_i are distinct prime ideals.*

Proof. The uniqueness is easy to prove as follows.

If $P_1^{n_1} \cdots P_k^{n_k} = Q_1^{m_1} \cdots Q_r^{m_r}$, then one can shift all the negative powers on each side to the other side to obtain an equality where all powers are positive. Then, a simple induction on the sum of the exponents yields uniqueness.

We prove the existence of the prime ideal decomposition by contradiction. First, we assume that there is an (actual) ideal I which is not expressible as a product of prime ideals. By using the fact that A is Noetherien, we obtain an ideal I which is maximal with respect to this property. Of course, I is not a prime ideal. If $I \subset P$ with P maximal, then $I = AI \subset P^{-1}I \subset P^{-1}P = A$. Now, if $x \in P^{-1} \setminus A$, then $xI \not\subset I$ and so $xI \subset P^{-1}I \setminus I$. Hence $P^{-1}I$ is an (actual) ideal which contains I properly. By the choice of I, we obtain that $P^{-1}I$ must be a product of prime ideals. Therefore, clearly I itself is such a product, which manifestly contradicts the choice of I. Therefore, every ideal in A is, indeed, a product of prime ideals.

Finally, if J is any fractional ideal, there is some $d \neq 0$ in A such that dJ is an ideal of A. So, if $(d) = P_1^{a_1} \cdots P_r^{a_r}$ and $dJ = Q_1^{b_1} \cdots Q_s^{b_s}$, then $J = P_1^{-a_1} \cdots P_r^{-a_r} Q_1^{b_1} \cdots Q_s^{b_s}$. This proves the theorem.

Examples/Exercises. (a) In any DD, $P \supset P^2 \supset P^3 \cdots$ is a strictly decreasing chain.

(b) Every fractional ideal in a DD can be generated by two elements one of which can be taken to be any arbitrary element.

Hint: Enough to prove this for ideals I; in this case if $a \in I$ and if $(a) = P_1^{a_1} \cdots P_r^{a_r}$ and $I = P_1^{b_1} \cdots P_r^{b_r}$, then $a_i \geq b_i \geq 0$. Use the Chinese remainder theorem to choose an appropriate element b in I so that $I = (a, b)$.

(c) A DD which has only finitely many prime ideals is a PID.

Hint : If $P_1, \cdots P_n$ are all the prime ideals, use the Chinese remainder theorem to choose $x_i \in P_i$, $x_i \notin P_i^2$ and $x_i \equiv 1 \bmod P_j$ for $i \neq j$. Then, $P_i = (x_i)$. (d) Use the fact that $\mathbf{Z}[\sqrt{-5}]$ is not a PID and (c) above to prove that there are infinitely many prime numbers (!)

3. Prime decomposition in extension fields

Let A be a DD with quotient field K and let L be a finite, separable extension of K. Then, we have seen that the integral closure B of A in L is again a DD. If $A = \mathbf{Z}$, then L is called an *algebraic number field* and B is called the *ring of integers of* L.

Exercises. *(a) Show that if $K \subset L$ are algebraic number fields, then the ring of integers of L is the integral closure of the ring of integers of K in L. (b) Find the ring of integers of the field $\mathbf{Q}(\sqrt{d})$ for any square-free integer d.*

Definition. For a field extension L/K of degree n, and an n-tuple of elements $v_1, \cdots, v_n$ of L, one defines *the discriminant of the n-tuple $v_1, \cdots, v_n$* to be the element $D_K^L(v_1, \cdots, v_n) = \det(M)$ of K where $M_{ij} = Tr_K^L(v_i v_j)$. This is an important concept, and let us start with a few easy exercises to see its use.

Exercises. *Let L, K, v_i be as above.*
(a) Show that $D_K^L(v_1, \cdots, v_n) \neq 0$ if, and only if, $v_1, \cdots, v_n$ form a K-basis of L.
(b) If $K = \mathbf{Q}$ and v_i form a $\mathbf{Z}$-basis of the ring of integers (this always exists as we observed), then $D_K^L(v_1, \cdots, v_n)$ is an integer which is independent of the choice of the $\mathbf{Z}$-basis.
(c) If $\sigma_1, \cdots, \sigma_n$ are the K-embeddings of L in $\mathbf{C}$, then $D_K^L(v_1, \cdots, v_n) = \det(N)^2$ where $N_{ij} = \sigma_i(v_j)$.

Definition. The *discriminant D_K of an algebraic number field K* is the discriminant of any $\mathbf{Z}$-basis of its ring of integers. By the exercise (b) above, it is well-defined. Moreover, it is clear that if $\{v_1, \cdots, v_n\}$ are in $\mathcal{O}_K$ and satisfy $D_K = D_{\mathbf{Q}}^K(v_1, \cdots, v_n)$, then $\{v_i\}$ form an integral basis (Why?).

Exercise. *(a) For a square-free integer d, show that the discriminant of $\mathbf{Q}(\sqrt{d})$ is d or $4d$ according as whether $d \equiv 2, 3$ mod 4 or $d \equiv 1$ mod 4.*
(b) Let $K = \mathbf{Q}(\alpha)$ be an algebraic number field. Suppose the minimal

(monic) polynomial of α is $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$. Then, prove that

$$D_{\mathbf{Q}}^{K}(1, \alpha, \cdots, \alpha^{n-1}) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2} N_{\mathbf{Q}}^{K} f'(\alpha)$$

where N denotes the norm map.
(c) Use (b) to show that for any n, and $K = \mathbf{Q}(\zeta_n)$ with ζ_n a primitive n-th root of unity, one has $D_{\mathbf{Q}}^{K}(1, \zeta, \cdots, \zeta^{\phi(n)-1})$ divides $n^{\phi(n)}$.
(d) Let K be an algebraic number field and let $\alpha_1, \cdots, \alpha_n$ be a $\mathbf{Q}$-basis of K contained in $\mathcal{O}_K$, the ring of integers of K. Then,

$$\mathcal{O}_K \subset \{\sum m_i \alpha_i / d : m_i \in \mathbf{Z}, d | m_i^2\}$$

Here d stands for $D_{\mathbf{Q}}^{K}(\alpha_1, \cdots, \alpha_n)$.
Hint: Write any $\alpha \in \mathcal{O}_K$ as $\sum_i t_i \alpha_i$ with $t_i \in \mathbf{Q}$. Apply the various embeddings of K to this equation and solve the system of linear equations by Cramer's rule.
(e) If K, L have degrees m, n over $\mathbf{Q}$ and if KL has degree mn, then $\mathcal{O}_{KL} \subset \frac{1}{d}\mathcal{O}_K \mathcal{O}_L$ where d is the GCD of D_K and D_L.
Hint: Use the fact (implied by the hypothesis $[KL : \mathbf{Q}] = mn$) that each embedding of K in $\mathbf{C}$ has a unique extension as an embedding of KL which restricts to the identity on L. Then, use the same idea as for (d).

Lemma. *For any positive integer n, consider the field $K = \mathbf{Q}(\zeta)$ where $\zeta = e^{2i\pi/n}$. Then, $\mathcal{O}_K = \mathbf{Z}[\zeta]$.*

Proof. By the exercises (c) and (e) above, and the fact that Euler's phi-function is multiplicative, it suffices to prove the lemma when n is a power of a prime.

Let us use the notation $\mathrm{disc}(\alpha)$ when we talk about $D_{\mathbf{Q}}^{K}(1, \alpha, \cdots, \alpha^{m-1})$ for some number field $K = \mathbf{Q}(\alpha)$ of degree m. Let $n = p^r$ and ζ be a primitive n-th root of unity. From an earlier exercise, we have $\mathrm{disc}(\zeta) = \mathrm{disc}(1 - \zeta)$. Moreover, $p = \prod_{(k,p)=1}(1 - \zeta^k)$ as seen by evaluating the corresponding cyclotomic polynomial at 1. Evidently, $1 - \zeta^k$ is an associate of $1 - \zeta$ for any k coprime to p. Therefore, p divides $(1 - \zeta)^{\phi(p^r)}$ in $\mathbf{Z}[\zeta]$. Now, by an exercise above, every element of $\mathcal{O}_K$ is of the form

$$\sum_{i<\phi(p^r)} m_i (1 - \zeta)^{i-1} / d,$$

where $d = \mathrm{disc}(\zeta)$. Note that d is a power of p. If $\mathcal{O}_K \neq \mathbf{Z}[1 - \zeta]$, then there exists an element $x \in \mathcal{O}_K$ for which not all m_i are divisible by d. If all the

m_i's are divisible by p, we can divide them all by p and proceeding this way we finally arrive at an element in $\mathcal{O}_K$ of the form $x = \sum_{i \geq j} m_i(1-\zeta)^{i-1}/p$ with $j \geq 1$ and m_j not a multiple of p. Now, we noted in the beginning of the proof that p is an associate of $(1-\zeta)^{\phi(p^r)}$ in $\mathbf{Z}[\zeta]$. This means, in particular, that $p/(1-\zeta)^j \in \mathbf{Z}[\zeta] \subset \mathcal{O}_K$. Hence, we have $xp/(1-\zeta)^j \in \mathcal{O}_K$. Hence, we get from the expression for x that $m_j/(1-\zeta) \in \mathcal{O}_K$. So, $N_{\mathbf{Q}}^K(1-\zeta)$ divides $N_{\mathbf{Q}}^K(m_j) = m_j^{\phi(p^r)}$ i.e., $p|m_j$, which is a contradiction. This proves the lemma.

Definition. Let A be a DD, K its quotient field and L a finite, separable extension. Let B denote the integral closure of A in L. For any non-zero prime ideal P of A, as B is a DD, one can write $PB = P_1^{e_1} \cdots P_g^{e_g}$ where all $e_i > 0$. The integer e_i is called the *ramification index of* P_i and sometimes denoted by $e(P_i/P)$ to make its dependence clear. P is said to be *unramified in* B if each $e_i = 1$; otherwise it is said to be ramified. P is said to be *totally ramified* if $g = 1$ and $e_i > 1$. The primes P_i lie over P and these are all the primes lying over P (*Why*?). The degree f_i (denoted by $f(P_i/P)$) of the field extension $B/P_i \supset A/P$ is evidently (*why?*) at the most equal to the degree of L over K. The finite field A/P (*why is it finite?*) is called the residue field of K at P. The field extension $B/P_i \supset A/P$ is called the residue field extension at P_i and f_i is called the *residue field degree of* P_i.

Exercises. *Answer the three why's in the above definition.*

Proposition. *Let A be a DD, K its quotient field and L a finite separable extension. Let B denote the integral closure of A in L. For a non-zero prime ideal P of A, writing $PB = P_1^{e_1} \cdots P_g^{e_g}$ we have $\sum_{i=1}^g e_i f_i$ where $f_i = [B/P_i : A/P]$.*

Proof. The trick is to localize at P i.e. consider $S^{-1}A$ and $S^{-1}B$ where $S = A \setminus P$. Now $S^{-1}B$ is the integral closure of $S^{-1}A$ in L, and $S^{-1}A/S^{-1}P \cong A/P$. Note also that $PS^{-1}B = Q_1^{e_1} \cdots Q_g^{e_g}$ where $Q_i = P_i S^{-1}B$ and that $S^{-1}B/Q_i \cong B/P_i$ Thus, to prove the proposition we may replace A, B by $S^{-1}A, S^{-1}B$. In this case, A, B are PIDs as they are DDs with only finitely many primes! Therefore, B which is a submodule of a free A-module is, itself, free of rank n (the rank is n as B contains a K-basis of L). Let $v_1, \cdots, v_n$ be an A-basis of B. If $\bar{v_i}$ denotes the image of v_i modulo PB, we have $B/PB = \sum_{i=1}^n (A/P)\bar{v_i}$. Moreover, if $\sum_{i=1}^n \bar{a_i}\bar{v_i} = 0$ in B/PB, then $\sum_{i=1}^n a_i v_i \in PB$. This forces each a_i to be in P since v_i's form a basis of B. Thus, $\bar{v_1}, \cdots, \bar{v_n}$ is a basis of the A/P-vector space B/PB. Thus, $\dim_{A/P} B/PB = n$. Let us count this same dimension in another way. By

the Chinese remainder theorem, one has $B/PB = B/\prod P_i^{e_i} \cong \oplus B/P_i^{e_i}$ as rings as well as as A/P-vector spaces. We need to count the dimension of each $B/P_i^{e_i}$. Now, since $P \subset P_i$, we have $PP_i^r \subset P_i^{r+1}$ for all $r \geq 1$. Hence, P_i^r/P_i^{r+1} is an A/P-vector space. Thus, as A/P-vector spaces, we have

$$B/P_i^{e_i} \cong B/P_i \oplus P_i/P_i^2 \oplus \cdots \oplus P_i^{e_i-1}/P_i^{e_i}$$

Further, as B is a PID, one can write $P_i = (\pi_i)$. Then, for each r, the multiplication by π_i^r gives an A/P-isomorphism from B/P_i onto P_i^r/P_i^{r+1}. Hence, we have $\dim_{A/P} B/P_i^{e_i} = e_i f_i$ which gives that $n = \sum e_i f_i$.

Definition. With A, B as before, a maximal ideal P of A is said to *split completely in* B if $e_i = 1 = f_i$; so PB is a product of n distinct primes.

Examples/Exercises. *(a) Show that the e's and the f's multiply in towers. (b) Let p be a prime, $\zeta = e^{2i\pi/p}$ and $K = \mathbf{Q}(\zeta)$. Then, p is totally ramified in K.*
Hint: Show that $p = \prod_{i=1}^{p-1}(1-\zeta^i)$ and that each $1-\zeta^i$ is a unit times $1-\zeta$.

Corollary. *Let the notations be as in the above proposition. Assume, in addition, that L/K is a Galois extension. Then, all the e_i's are equal and all the f_i's are equal. Hence $n = efg$ for some positive integers e, f, g.*

Proof. We shall show that the Galois group $\mathrm{Gal}(L/K)$ acts transitively on the set $\{P_1, \cdots, P_g\}$. If it does not, then there exist $i \neq j$ such that $gP_i \neq P_j$ for all $g \in \mathrm{Gal}(L/K)$. Then, choosing by the Chinese remainder theorem, an element $b \in P_j, b \equiv 1 \bmod gP_i$ for each $g \in G$. But then the element $a = N_K^L(b) = \prod_g g(b)$ is in A on the one hand, and is in P_j on the other. As $A \cap P_j = P$, this means that $\prod_g g(b) \in P \subset P_i$ i.e. some $g(b) \in P_i$, which contradicts the choice of b. Hence, it follows that the Galois group acts transitively. Then, if $gP_i = P_j$, the observation $PB = g(PB)$ along with the uniqueness of decomposition into prime ideals in B yields $e_i = e_j$. Therefore, all the e_i's are equal. Finally, if $g(P_i) = P_j$, then g induces an A/P-isomorphism from B/P_i to B/P_j and so $f_i = f_j$. The corollary is proved.

Definitions. With notations as above, the *decomposition group* of P_i is the subgroup $D_{P_i} := \{g \in \mathrm{Gal}(L/K) : g(P_i) = P_i\}$. The Galois group induces a natural homomorphism θ_{P_i} from D_{P_i} to $\mathrm{Gal}((B/P_i)/(A/P))$. The kernel T_{P_i} is called the *inertia group of* P_i. If the inertia group T_{P_i} is trivial, one defines the *Frobenius element* Fr_{P_i} at P_i as the inverse image under the isomorphism θ_{P_i} of the Frobenius automorphism $t \mapsto t^{\#(A/P)}$ which generates $\mathrm{Gal}((B/P_i)/(A/P))$.

Exercises.
(a) Show that the above homomorphism from D_{P_i} to $Gal((B/P_i)/(A/P))$ is surjective.
Hint: Use the Chinese remainder theorem.
(b) Show that the D_{P_i}'s are mutually conjugate and that $\#D_{P_i} = ef$, $\#T_{P_i} = e$ for all i.
Hint: D_{P_i} is the stabiliser at P_i for the action of $Gal(L/K)$ on the set $\{P_1, \cdots, P_g\}$.

Definition. For any algebraic number field K and a non-zero ideal I, the *norm $N(I)$ of I* is defined to be the cardinality of the finite ring $\mathcal{O}_K/I$.

Corollary. *Let K be an algebraic number field. Then,*
(a) if I, J are non-zero ideals, $N(IJ) = N(I)N(J)$.
(b) if P is a maximal ideal, $N(P) = p^f$ where p is the prime number lying below P and $f = f(P/p)$.
(c) if L/K is an extension of degree n, then for any non-zero ideal I of $\mathcal{O}_K$, $N(I\mathcal{O}_K) = N(I)^n$.
(d) if $a \neq 0$ is in $\mathcal{O}_K$, $N((a)) = \mid N_{\mathbf{Q}}^K(a) \mid$.

Examples/exercises. *Let $K = \mathbf{Q}(\sqrt{d})$ where d is a square-free integer. For any odd prime p, denote by (a/p) the Legendre symbol. Then,*
(a) if $p|d$, p is (totally) ramified i.e. $p\mathcal{O}_K = P^2$ where the prime ideal $P = (p, \sqrt{d})$,
(b) if p is odd and coprime to d, it is unramified and splits completely or remains a prime according as whether $(d/p) = 1$ or not,
(b)$'$ if $d = q$ is a prime $\equiv 1$ mod 4, and p is an odd prime, prove that $(q/p) = 1 \Leftrightarrow$ the polynomial $X^2 - X + \frac{1-q}{4}$ has a solution mod $p \Leftrightarrow \mathbf{Q}(\sqrt{q})$ is fixed by the Frobenius $Fr_p \Leftrightarrow (p/q) = 1$.
(c) if d is odd, 2 is ramified if $d \equiv 3$ mod 4, splits completely if $d \equiv 1$ mod 8 and remains a prime if $d \equiv 5$ mod 8.
(d) Prove the whole of quadratic reciprocity law by proving a corresponding version of (b)$'$ for primes $\equiv 3$ mod 4.

Remarks. The exercise above provides a nice criterion to decide when a prime splits completely in a quadratic extension. The criterion is in terms of some congruences. One of the principal aims of ramification theory (in fact, of algebraic number theory itself!) is to give a 'nice' criterion for a prime to split completely in a given extension; one often calls such a criterion to be a reciprocity law. The reason that one is interested in a criterion to decide which primes split completely is that given K, the set of primes of K which split in L determine L uniquely. The last fact mentioned is deep and the

proof requires the so-called class field theory.

An interesting exercise - Why is Fermat's last theorem not trivial to prove?
(a) Let p be an odd prime and $\zeta = e^{2i\pi/p}$. Show that the element $S = \sum_{i=1}^{p-1}(i/p)\zeta^i$ of $K = \mathbf{Q}(\zeta)$ satisfies $S^2 = (-1/p)p$. Hence conclude that every quadratic extension of $\mathbf{Q}$ is contained in a cyclotomic extension.
(b) Let $K = \mathbf{Q}(\sqrt{-23}), L = \mathbf{Q}(\zeta)$ where $\zeta = e^{2i\pi/23}$. Show that $\mathcal{O}_L$ is not a PID.
Hint : $K \subset L$ by (a). Also, $2\mathcal{O}_K = P\bar{P}$ where $P = (2, \frac{1+\sqrt{-23}}{2})$ and $\bar{P} = (2, \frac{1-\sqrt{-23}}{2})$. If a prime Q in L lying over P is principal, then P^f is principal where $f = f(Q/P)$. As P is not principal and $P^3 = (\frac{-3+\sqrt{-23}}{2})$, P^f cannot be principal as f divides $[L : K]$.

Theorem (A Cyclotomic reciprocity law). *Let n be a positive integer and p be a prime not dividing n. Denote by ζ a primitive n-th root of unity. Then, p is unramified in $K = \mathbf{Q}(\zeta)$ and splits into $\phi(n)/f$ primes where f is the order of p in the unit group of $\mathbf{Z}/n$ and ϕ is Euler's phi function. In particular, p splits completely in K if, and only if, $p \equiv 1$ mod n.*

Proof. We already know that p is unramified as the minimal polynomial of ζ (indeed, its multiple $X^n - 1$ itself) has distinct roots mod p. Let P be a prime in K which lies over p. First, we observe that the powers $\zeta^i, 0 \leq i \leq n-1$ are distinct modulo P. This is a consequence of the identity $n = \prod_{i=1}^{n-1}(1-\zeta^i)$ and the observation that $n \notin P$; these imply that $1 - \zeta^i \notin P$. Now, the Frobenius element Fr_p of $\mathrm{Gal}(K/\mathbf{Q})$ satisfies $\mathrm{Fr}_p(x) \equiv x^p$ mod P for all $x \in \mathcal{O}_K$. But, $\mathrm{Fr}_p(\zeta)$ is obviously again an n-th root of unity. In view of the observation made above, it follows that $\mathrm{Fr}_p(\zeta) = \zeta^p$. ¿From this, it follows easily that the order $f(P/p)$ of Fr_p is just the order f of p in $(\mathbf{Z}/n)^*$.

Remarks. When K is the quotient field of a DD A, and L is a finite, separable extension of K and B the integral closure of A in L, the following theorem of Kummer provides a way to read off the decomposition of a prime ideal in terms of the decomposition of the minimal polynomial of α modulo P. Here $L = K(\alpha)$ and $\alpha \in B$ and the theorem is valid under a mild assumption.

Theorem (Kummer). *Let $A, K, L = K(\alpha), B, P, f$ be as above. Assume, in addition, that $B = A[\alpha]$. Write $\bar{f} = \bar{p}_1^{e_1} \cdots \bar{p}_g^{e_g}$ where $\bar{p}_i$ are irreducible polynomials in $(A/P)[X]$ and $\bar{f}$ denotes the image of f mod P. Then,*

$$PB = P_1^{e_1} \cdots P_g^{e_g}$$

where P_i's are prime ideals and $f(P_i/P) = deg(\bar{p}_i)$. Indeed, $P_i = PB + (p_i(\alpha))$ where p_i's are arbitrary lifts of $\bar{p}_i$'s.

Before proving the theorem, let us look at its applications to see really how powerful it is.

Applications of Kummer's theorem

I. Prime decomposition in quadratic fields

As we saw earlier, if $K = \mathbf{Q}(\sqrt{d})$ with d square-free, then $\mathcal{O}_K = \mathbf{Z}[\alpha]$ where $\alpha = \sqrt{d}$ or $\frac{1+\sqrt{d}}{2}$ according as $d \equiv 2, 3 \bmod 4$ or $d \equiv 1 \bmod 4$. The minimal polynomial f is $X^2 - d$ in the first case and $X^2 - X + \frac{1-d}{4}$ in the second. If $d \equiv 2$ or $3 \bmod 4$, $f(X) = X^2 - d$ is a square modulo any prime p dividing d and also modulo 2. Thus, 2 and primes dividing d are (totally) ramified. If an odd prime p does not divide d, then f modulo p is reducible or irreducible according as whether d is a square modulo p or not. Thus, these primes, respectively, split completely and remain inert. Similarly, one can argue for the case $X^2 - X + \frac{1-d}{4}$ corresponding to $d \equiv 1 \bmod 4$.

II. Discriminant criterion for ramification

Theorem. *Suppose $K = \mathbf{Q}(\alpha)$ is an algebraic number field and assume that $\mathcal{O}_K = \mathbf{Z}[\alpha]$ for some α. Then, a prime p ramifies in K if, and only if, p divides $Disc(K)$.*

Proof. Let $f(X) = \prod_i (X - \alpha_i)$ be the minimal polynomial of α. We have seen that $\mathrm{disc}(K) = \mathrm{disc}(f) = \pm\prod_{i \neq j}(\alpha_i - \alpha_j)$. By Kummer's theorem, a prime ramifies in K if, and only if, f has a multiple root modulo p. This is so if, and only if, $\mathrm{disc}(\bar{f}) \equiv 0 \bmod p$ i.e. if, and only if, p divides $\mathrm{disc}(f)$. Here $\bar{f}$ denotes the reduction of f modulo p.

Proof of Kummer's theorem. Consider the ring homomorphisms

$$A[X] \to (A/P)[X] \to (A/P)[X]/(\bar{p}_i(X))$$

Call the composite map ϕ_i. Note that $(A/P)[X]/(\bar{p}_i(X)) \cong (A/P)[\alpha_i]$ for any root α_i of $\bar{p}_i$. Therefore, $\mathrm{Ker}(\phi_i)$ is a maximal ideal as ϕ_i is evidently surjective. Moreover, it is clear that $P \subset \mathrm{Ker}(\phi_i)$ and $p_i(X) \in \mathrm{Ker}(\phi_i)$ for any arbitrary $p_i \in A[X]$ which maps to $\bar{p}_i$. Further, it is clear from the definition of ϕ_i that $\mathrm{Ker}(\phi_i)$ is the ideal generated by P and p_i in $A[X]$. Now, by the hypothesis, $\bar{f} = \bar{p}_1^{e_1} \cdots \bar{p}_g^{e_g}$ which implies that $f \in (P, p_i) = \mathrm{Ker}(\phi_i)$. Therefore, ϕ_i factors through (f) to give a surjective homomorphism $\theta_i : A[X]/(f) \to (A/P)[X]/(\bar{p}_i(X))$. Note that we have assumed that $B = A[\alpha]$ which gives that $A[X]/(f) \cong B$ where X maps to α. So, we have obtained $\theta_i : B \to (A/P)[X]/(\bar{p}_i(X))$ which is surjective and has kernel $\mathrm{Ker}(\theta_i) = PB + p_i(\alpha)B$. Thus, $P_i :== PB + p_i(\alpha)B = \mathrm{Ker}(\theta_i)$ are maximal ideals in

B. As they contain P, they lie over P. Note that $f(P_i/P) = [B/P_i : A/P] = \dim_{A/P}(A/P)[X]/(\bar{p}_i(X)) = \deg \bar{p}_i$. We shall prove now that P_i exhaust all the maximal ideals of B lying over P and have ramification indices equal to e_i.
Note first that the assumption $\bar{f} = \bar{p}_1^{e_1} \cdots \bar{p}_g^{e_g}$ gives, on comparing degrees that $\sum_i e_i f_i = \deg(f) = [L : K]$. The same thing also gives for arbitrary lifts p_i that $f - p_1^{e_1} \cdots p_g^{e_g} \in P[X]$ which, in turn gives, on evaluation at α, that $p_1(\alpha)^{e_1} \cdots p_g(\alpha)^{e_g} \in PA[\alpha] = PB$. So, if Q is any prime ideal of B lying over P, we have $p_1(\alpha)^{e_1} \cdots p_g(\alpha)^{e_g} \in PB \subset Q$. Then, $p_i(\alpha) \in Q$ for some i. But then, $P_i = PB + p_i(\alpha) \subset Q$ and, as both are maximal ideals, they must be equal.
Finally, let $PB = P_1^{d_1} \cdots P_g^{d_g}$. Then,

$$\begin{aligned} P_1^{e_1} \cdots P_g^{e_g} &= (P, p_1(\alpha))^{e_1} \cdots (P, p_g(\alpha))^{e_g} \\ &\subset PB + (p_1(\alpha)^{e_1} \cdots p_g(\alpha)^{e_g}) = PB = P_1^{d_1} \cdots P_g^{d_g}. \end{aligned}$$

Thus, $e_i \geq d_i$. As $\sum e_i f_i = [L : K] = \sum d_i f_i$, this forces $d_i = e_i$. The proof is complete.

The last application was generalised by Dedekind to the situation when the base field is the quotient field K of any DD A and when the integral closure B of A in a finite, separable extension L may not satisfy the condition $B = A[\alpha]$ for any α.

The following example shows that the condition $B = A[\alpha]$ may not hold for any α.

Example. *Let K denote the unique subfield K of $L = \mathbf{Q}(\zeta_{31})$ of degree 6 over $\mathbf{Q}$. Then, $\mathcal{O}_K \neq \mathbf{Z}[\alpha]$ for any α.*

Reason: In general, if E/F is a finite Galois extension, and D is the decomposition group at some prime Q of E, then, $P = Q \cap \mathcal{O}_F$ splits completely in E^D (Why?).
Returning to our situation, look at the prime 2 which is unramified. As the order of 2 modulo 31 is 5, 2 splits in $\mathcal{O}_L$ into $\phi(31)/5 = 6$ primes. Therefore, the decomposition group D at any prime of L lying over 2 has order 5. As $\mathrm{Gal}(L/\mathbf{Q})$ is cyclic, it has a unique subgroup of order 5 (indeed, of order any divisor of 30). Thus the fixed field L^D is of degree 6 over $\mathbf{Q}$ and must be K. By the observation made in the beginning, it follows that 2 splits completely (into 6 primes) in K. Hence, if $\mathcal{O}_K$ were of the form $\mathbf{Z}[\alpha]$, it would follow by Kummer's theorem that the minimal polynomial of α would split modulo $Q \cap \mathbf{Z}$ into six distinct linear factors. However, over $\mathbf{Z}/2$, there

are only two linear polynomials! This contradiction establishes the validity of the example.

Before stating and proving Dedekind's theorem, we introduce the concept of the discriminant ideal.

Definition. Let A be a DD with quotient field K, L be a finite, separable extension and B be the integral closure of A in L. The *discriminant ideal* $D_{B/A}$ is defined to be the ideal of A generated by the elements $\mathrm{disc}(v_1, \cdots, v_n)$ as $\{v_1, \cdots, v_n\}$ runs through K-bases of L which are contained in L.

Exercise. *If B is free over A, then $D_{B/A}$ is the principal ideal generated by the discriminant of any A-basis of B.*
Hint: For any A-basis $\{e_1, \cdots, e_n\}$ of B and any K-basis $\{v_1, \cdots, v_n\}$ of L which is contained in A, write $v_j = \sum_i a_{ij} e_i$ with $a_{ij} \in A$. Then, $\mathrm{disc}(v_1, \cdots, v_n) = \det(a_{ij})^2 \mathrm{disc}(e_1, \cdots, e_n)$.

Exercise. *For any n, let Φ_n denote the nth cyclotomic polynomial (i.e. minimal polynomial of $e^{2i\pi/n}$ over $\mathbf{Q}$). Note that $X^n - 1 = \prod_{d|n} \Phi_d(X)$. Let p be a prime not dividing n and $a \in \mathbf{Z}$. Show that p divides $\Phi_n(a)$ if, and only if, a has order n in $(\mathbf{Z}/p)^*$. Moreover, this happens for some p, a if, and only if, $p \equiv 1$ mod n. Hence, show that there are infinitely many primes $p \equiv 1$ mod n.*

Exercise. *For any n, and any prime $p \equiv 1$ mod n, show that p splits completely in the cyclotomic field $\mathbf{Q}(\zeta_n)$ into the prime ideals $P_i = (p, \zeta_n - i)$, where i has order n in $(\mathbf{Z}/p)^*$.*

Exercise. *Let K be the quotient field of a DD A, and suppose that L is a finite, Galois extension of K. Let B denote the integral closure of A in L and let $P \subset A$ be a maximal ideal. If $PB = (P_1 \cdots P_g)^e$ in B, then show that there are fields E, F such that $K \subset F \subset E \subset L$ with $[L : E] = e$, $[E : F] = f$, $[F : K] = g$. Further, prove that such E, F exist with the properties: (i) P splits completely in F into the product of the primes of F lying below $P_1, \cdots, P_g$,*
(ii) each prime of F lying above P remains a prime in E,
and (iii) each prime of F lying above P totally ramifies in L.

Hint: Look at the fixed fields under the decomposition group and the inertia group of any P_i.

Lemma. *Let $S \subset A$ be a multiplicative subset. Then, $D_{S^{-1}B/S^{-1}A} = S^{-1}(D_{B/A})$. In particular, for a prime P of A and $S = A \setminus P$, one has*

$P \supset D_{B/A} \Leftrightarrow S^{-1}(P) \supset D_{S^{-1}(B)/S^{-1}(A)}$.

Proof. If $\{v_i\}$ is a K-basis contained in B, then v_i's are also in $S^{-1}(B)$. So, $D_{B/A} \subset D_{S^{-1}B/S^{-1}A}$. Therefore, $S^{-1}(D_{B/A}) \subset D_{S^{-1}B/S^{-1}A}$. Conversely, if $\{w_i\}$ is a K-basis contained in $S^{-1}B$, then there exists $s \in S$ such that $sw_i \in B$ for all i. Therefore, $\mathrm{disc}(sw_1, \cdots, sw_n) = s^{2n}\mathrm{disc}(w_1, \cdots, w_n)$. As the left hand side is in $D_{B/A}$, it follows that $\mathrm{disc}(w_1, \cdots, w_n) \in S^{-1}(D_{B/A})$ which proves the other part of the equality asserted.

Theorem (Dedekind). *Let A, K, L, B be as before. Assume that every finite extension of A/P (for any maximal ideal P) is separable - this is true when K is an algebraic number field, for then, A/P is a finite field. Then P ramifies in L if, and only if, $P \supset D_{B/A}$.*

Proof. By the lemma, one can, without loss of generality, localise at P. Then, A, B etc. get replaced by $S^{-1}A, S^{-1}B$ which are PID's (Why?). Then, B is A-free with a basis $\{v_1, \cdots, v_n\}$ say. As observed earlier, this means that the images $\bar{v_i}$ of v_i give a basis of the A/P-vector space B/PB. *Claim:* If $b \in B$, then $\overline{Tr_{L/K}(b)} = tr(\bar{b})$ where $\bar{b}$ is regarded as an A/P-endomorphism of B/PB.
To see why this is so, let us look at the endomorphism $\rho_b : B \to B; x \mapsto xb$. Write M for the matrix of ρ_b with respect to the basis $\{v_i\}$. Then, $v_i b = \sum_j m_{ij} v_j$. Reading this modulo PB, we get the fact that $\bar{M}$ is the matrix of $\bar{b}$. This gives $tr(\bar{b}) = \sum_i \bar{m_{ii}} = \overline{tr(\rho_b)} = \overline{Tr_{L/K}(b)}$ which was claimed above. Hence, $D_{B/A} = (\mathrm{disc}(v_1, \cdots, v_n)) \subset P$ if, and only if, $\mathrm{disc}(\bar{v_1}, \cdots, \bar{v_n}) = 0$. Let us write $PB = P_1^{e_1} \cdots P_g^{e_g}$; then $B/PB \cong B/P_1^{e_1} \oplus \cdots \oplus B/P_g^{e_g}$. To prove the theorem, let us first assume that P is unramified in B; then all the e_i are 1. Thus, B/PB is a direct sum of fields B/P_i which are separable by our hypothesis. Choose a new A/P-basis $\{\bar{b_1}, \cdots, \bar{b_n}\}$ of B/PB which is compatible with the direct sum decomposition (What does that mean?). Then, for each $\bar{b} = b^{(1)} + \cdots + b^{(g)} \in B/PB$, the matrix of $\rho_{\bar{b}}$ consists of diagonal blocks $M_1, \cdots, M_g$ where $M_i = \rho_{b^{(i)}}$. Therefore, $tr(\bar{b}) = \sum_i tr^{(i)}(b^{(i)}$ where $tr^{(i)}$ denotes the trace from B/P_i to A/P. Consequently, $\mathrm{disc}_{A/P}^{B/PB}(\bar{b_1}, \cdots, \bar{b_n}) = \prod_i \mathrm{disc}_{A/P}^{B/P_i}(b_1^{(i)}, \cdots, b_n^{(i)}) \neq 0$. Hence, for the original A/P-basis $\{\bar{v_i}\}$, one has $\mathrm{disc}(\bar{v_1}, \cdots, \bar{v_n}) = d^2\mathrm{disc}(\bar{b_1}, \cdots, \bar{b_n}) \neq 0$ in A/P, where d is the determinant of the change of basis. This proves that $P \not\supset D_{B/A}$ as observed earlier.
Conversely, suppose that some $e_i > 1$. Then, $B/P_i^{e_i}$ (and so B/PB itself) has a nilpotent element, say u_1. Extend it to a basis $\{u_1, \cdots, u_n\}$ of B/PB. As $u_1 u_i$ is nilpotent, one has $tr(u_1 u_i) = 0$ for all i. Therefore, $\mathrm{disc}(u_1, \cdots, u_n) = 0$ and so for the other basis too, one has $disc(\bar{v_1}, \cdots, \bar{v_n})$

$= 0$. In other words, $P \supset D_{B/A}$. This completes the proof.

4. Finiteness of class number and Minkowski's bound

In this section, we shall show that the class group of an algebraic number field is finite. Its order, called the *class number*, gives a measure of the deviation from the unique factorisation property. Although the finiteness is easy to establish, the easy proof gives a somewhat large bound. A much better bound was obtained by Minkowski using a geometric method. We shall discuss Minkowski's method and in the next section, we shall apply it to prove a theorem of Dirichlet on the structure of units of a number field.

Theorem. *For an algebraic number field K, the class group is finite.*

Proof. Fix an integral basis $\{v_1, \cdots, v_n\}$ of $\mathcal{O}_K$. Let $I \neq 0$ be any ideal and consider the subset S of $\mathcal{O}_K$ consisting of all $\sum_{i=1}^{n} m_i v_i$ with $0 \leq m_i \leq N(I)^{1/n}$. Evidently, $\#\ S > N(I) = \#\ (\mathcal{O}_K/I)$. Therefore, there exist $a \neq b \in S$ such that $a - b \in I$. Notice that $a - b = \sum_i m_i v_i$ for some integers m_i which satisfy $\mid m_i \mid \leq N(I)^{1/n}$. Let us compute its norm over $\mathbf{Q}$. We have $N_{K/\mathbf{Q}}(a-b) = \prod_i \sigma_i(\sum_j m_j v_j)$ where σ_i's are the embeddings of K in $\mathbf{C}$. Therefore,

$$\mid N_{K/\mathbf{Q}}(a-b) \mid \ = \prod_i \mid \sum_j m_j \sigma_i(v_j) \mid \ \leq \prod_i \sum_j \mid m_j \mid \ \mid \sigma_i(v_j) \mid \ \leq N(I)C,$$

where $C = \prod_i \sum_j \mid \sigma_i(v_j) \mid$ is a constant independent of the ideal I; it depends only on K. Now $a - b \in I \Rightarrow (a-b) = IJ$ for some non-zero ideal J. Thus $N_{K/\mathbf{Q}}(a-b) = N(I)N(J) \leq N(I)C$ and we get $N(J) \leq C$. As J is just the inverse of I in the class group, it runs through the class group when I does. Therefore, we have shown that any element of the class group has a representative ideal whose norm is at the most the constant C. As there are only finitely many ideals with the norm bounded by an absolute constant, the theorem follows.

Example. Let $K = \mathbf{Q}(\sqrt{2})$. Then, $\mathcal{O}_K = \mathbf{Z}[\sqrt{2}]$ has $\{1, \sqrt{2}\}$ as a $\mathbf{Z}$-basis. The constant C above is $C = (1 + \sqrt{2})^2 = 5.8....$ So, every ideal has a representative I with norm at the most 5. Thus, the prime ideals dividing I must have norm ≤ 5 which means that they are among those lying over $2, 3$ and 5. Now, $3, 5$ are unramified and must, therefore, be either inert or split. As 2 is not a square mod 3, 3 remains prime. So is the case with 5 also. Finally, 2 is the square of the prime ideal $(\sqrt{2})$. Thus, we have shown that every ideal class contains a representative ideal which is principal. Thus, the class group is trivial, i.e. $\mathcal{O}_K$ is a PID.

The bound given above is somewhat large. One can do somewhat better; proceeding as in the proof of the theorem, one can write out the matrix M of $a-b$ with respect to the basis $\{v_1,\cdots,v_n\}$. $M=\sum_i m_iM_i$ where M_i is the matrix of v_i with respect to the same ordered basis. Note that all the entries of M_i are integers whose absolute values are bounded by a constant depending only on the basis $\{v_i\}$ and not on the ideal I. Then, by definition, $\mid N_{K/\mathbf{Q}}(a-b)\mid \;=\; \mid \det(M)\mid \;\leq C_0N(I)$. This constant C_0 is better than the constant C in the proof of the theorem. For example, when $K=\mathbf{Q}(\sqrt{-5})$, we have $C=10,\ C_0=6$. But, in fact, the method we shall discuss below, due to Minkowski, gives a much better bound. In this example, it will give a constant less than 3 which will enable us to conclude quite easily that the class number is 2.

Definitions. A *lattice* Λ in the Euclidean space $\mathbf{R}^n$ is the $\mathbf{Z}$-span of an $\mathbf{R}$-basis of $\mathbf{R}^n$. Clearly, the group $GL_n(\mathbf{R})$ of invertible $n\times n$ matrices acts transitively on the set of all lattices. Thus, any lattice can be identified with $g\mathbf{Z}^n$ for some $g\in GL_n(\mathbf{R})$. Given a lattice Λ, *a fundamental parallelotope* for it is the set of vectors $\{\sum_i t_ie_i\ :\ 0\leq t_i<1\}$ for any basis $\{e_i\}$ of Λ. As any two $\mathbf{Z}$-bases are transforms of each other under a matrix in $GL_n(\mathbf{Z})=\{\gamma\in M_n(\mathbf{Z}):det(\gamma)=\pm1\}$, the *volume of the lattice* $\Lambda=g\mathbf{Z}^n$ is the well-defined non-zero real number $\mid det(g)\mid$. We write $\mathrm{Vol}(\mathbf{R}^n/\Lambda)$ for the volume of Λ.

Lemma. *Let K be an algebraic number field. Let $\sigma_1,\cdots,\sigma_r,\tau_1,\cdots,\tau_s$, $\bar\tau_1,\cdots,\bar\tau_s$ be the embeddings of K in $\mathbf{C}$. Here, the σ_i's take real values and the τ_j's take nonreal values. Then, the map $\theta: t\mapsto$*

$$(\sigma_1(t),\cdots,\sigma_r(t),Re(\tau_1(t)),\cdots,Re(\tau_s(t)),Im(\tau_1(t)),\cdots,Im(\tau_s(t)))$$

from K to $\mathbf{R}^n$ embeds $\mathcal{O}_K$ as a lattice. Its volume is $\sqrt{\mid \mathrm{disc}(K)\mid}/2^s$. In particular, K embeds densely in $\mathbf{R}^n$.

Proof. Let $v_1,\cdots,v_n$ be a $\mathbf{Z}$-basis of $\mathcal{O}_K$. We show that $\theta(v_1),\cdots,\theta(v_n)$ are linearly independent. If we write $\theta=(\theta_1,\cdots,\theta_n)$ to mean the obvious, look at the matrix M with $m_{ij}=\theta_i(v_j)$. Elementary column operations transform M to the matrix whose i-th row is

$$(1/2i)^s(\sigma_1(v_i),\cdots,\sigma_r(v_i),\tau_1(v_1),\bar\tau_1(v_i),\cdots,\tau_s(v_i),\bar\tau_s(v_i))$$

This gives the result that the determinant of M is $(1/2i)^s\sqrt{\mathrm{disc}(K)}$; so $\mathrm{Vol}(\mathbf{R}^n/\theta(\mathcal{O}_K))=\sqrt{\mid \mathrm{disc}(K)\mid}/2^s$.

Definition and Remarks. Given a positive integer n and non-negative integers r,s such that $r+2s=n$, define a *norm on* $\mathbf{R}^n$ by $N_{r,s}(x)=$

$x_1 \cdots x_r(x_{r+1}^2 + x_{r+2}^2) \cdots (x_{n-1}^2 + x_n^2)$. Thus, in the situation of a number field K of degree n over $\mathbf{Q}$ and r, s, θ as above, we have $N_{r,s}(\theta(t)) = N_{K/\mathbf{Q}}(t)$ for all $t \in \mathcal{O}_K$.

Theorem (Minkowski). *Every lattice Λ in $\mathbf{R}^n$ contains $x \neq 0$ with $N_{r,s}(x) \leq \frac{n!}{n^n}(\frac{8}{\pi})^s \mathrm{Vol}(\mathbf{R}^n/\Lambda)$.*

We shall give the proof of this important theorem after pointing out some very useful consequences of it.

Corollary. *Let $[K : \mathbf{Q}] = n$ and r, s have the usual meaning. Then,*
(a) Every non-zero ideal I contains $x \neq 0$ with

$$| N(x) | \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{| \operatorname{disc}(K) |}\, N(I).$$

(b) Every ideal class contains an ideal I with

$$| N(I) | \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{| \operatorname{disc}(K) |}.$$

(c) $\operatorname{disc}(K) > 1$ *if $K \neq \mathbf{Q}$.*
(d) If $K \neq \mathbf{Q}$, then some prime number p ramifies in K.

Proof. Using the lemma above, $\mathcal{O}_K$ can be viewed as a lattice in $\mathbf{R}^n$ whose volume has also been computed. Therefore, both (a) and (b) are direct consequences of Minkowski's theorem. To prove (c), just observe that the number $\frac{n^n}{n!}(\frac{\pi}{4})^s > \frac{1}{n!}(\frac{n\pi}{4})^n > 1$ for $n > 1$. Finally, (d) follows from Dedekind's theorem which showed that prime numbers which divide the discriminant of K must ramify in K.

Example/Exercise. Let $K = \mathbf{Q}(\sqrt{-5})$. Then, the above constant (called Minkowski's constant) on the right hand side of (b) shows that each ideal class contains a representative ideal I of norm $N(I) \leq \frac{4\sqrt{5}}{\pi} < 3$. So, one need only consider the ideals lying above 2 viz., $(2, 1 \pm \sqrt{-5})$. It is easy to see that these are not principal and thus it follows that K has class number 2.
Using this fact, show that the equation $x^2 + 5 = y^3$ has no integral solutions.

For the proof of Minkowski's theorem, one needs the following beautiful lemma on convex bodies which is of independent interest:

Minkowski's lemma. *Let Λ be a lattice in $\mathbf{R}^n$, E a convex, measurable, centrally symmetric subset of $\mathbf{R}^n$ such that $\mathrm{Vol}(E) > 2^n \mathrm{Vol}(\mathbf{R}^n/\Lambda)$. Then, E contains some non-zero point of Λ. Further, if E is also compact, then the strict inequality in the hypothesis can be weakened to $\geq$.*

Proof. Let F be a fundamental parallelotope for Λ. Then, we have $\mathbf{R}^n = \bigsqcup_{x\in\Lambda}(x+F)$. Now, $\frac{1}{2}E = \bigsqcup_{x\in\Lambda}(\frac{1}{2}E \cap (x+F))$. By the hypothesis,

$$\begin{aligned}\mathrm{Vol}(F) < \mathrm{Vol}(E)/2^n = \mathrm{Vol}(E/2) &= \sum_{x\in\Lambda} \mathrm{Vol}(\frac{1}{2}E \cap (x+F)) \\ &= \sum_{x\in\Lambda} \mathrm{Vol}((\frac{1}{2}E - x) \cap F)\end{aligned}$$

Therefore, as x runs over Λ, the sets $(\frac{1}{2}E - x)\cap F$ are not all disjoint. Thus, we get $x \neq y$ in Λ so that $\frac{1}{2}a - x = f = \frac{1}{2}b - y$ for some $a, b \in E, f \in F$. Clearly, then we get $0 \neq x - y = \frac{1}{2}a + \frac{1}{2}(-b) \in E \cap \Lambda$. This proves the main assertion. For the case when E is also compact, one may consider the sets $(1+\frac{1}{n})E$ and obtain lattice points $x_n \neq 0$ as above. Evidently, then all the $x_n \in 2E \cap \Lambda$ which is a finite set. Thus, for some n_0, $x_{n_0} \in (1+\frac{1}{n})E$ for infinitely many n i.e. $x_{n_0} \in \bar{E} = E$. The proof is complete.

Corollary. *Suppose that Ω is a compact, convex, centrally symmetric subset of $\mathbf{R}^n$ such that $Vol(\Omega) > 0$ and such that $\mid N_{r,s}(a) \mid \leq 1 \ \ \forall\ a \in \Omega$. Then, every lattice Λ contains a non-zero vector x with*

$$\mid N_{r,s}(x) \mid \leq 2^n \frac{Vol(\mathbf{R}^n/\Lambda)}{Vol(\Omega)}.$$

The proof is immediate from Minkowski's lemma applied to the set $E = t\Omega$ where $t^n = 2^n \frac{Vol(\mathbf{R}^n/\Lambda)}{Vol(\Omega)}$.

Proof of Minkowski's theorem. Let Ω be the subset of $\mathbf{R}^n$ defined by the inequality $\sum_{i=1}^{r} \mid x_i \mid + 2\sqrt{(x_{r+1}^2 + x_{r+2}^2)} + \cdots + 2\sqrt{(x_{n-1}^2 + x_n^2)} \leq n$. We shall prove that Ω is convex, and that $\mid N_{r,s}(a) \mid \leq 1\ \forall\ a \in \Omega$. Then, we shall compute its volume and apply the above corollary.

Step I: Ω is convex

¿From the definition of Ω, it is easy to see that if midpoints of any two points of Ω are in Ω, then Ω is convex. Let $(x_1, \cdots, x_n), (y_1, \cdots, y_n) \in \Omega$. Then, we have

$$\sum_{i=1}^{r} \mid x_i \mid + 2\sqrt{(x_{r+1}^2 + x_{r+2}^2)} + \cdots + 2\sqrt{(x_{n-1}^2 + x_n^2)} \leq n,$$

$$\sum_{i=1}^{r} \mid y_i \mid + 2\sqrt{(y_{r+1}^2 + y_{r+2}^2)} + \cdots + 2\sqrt{(y_{n-1}^2 + y_n^2)} \leq n.$$

Adding and using the triangle inequality

$$\sqrt{(a^2+b^2)} + \sqrt{(c^2+d^2)} \geq \sqrt{((a+c)^2 + (b+d)^2)}$$

one concludes that $(\frac{x_1+y_1}{2}, \cdots, \frac{x_n+y_n}{2}) \in \Omega$.
Step II: $\mid N_{r,s}(a) \mid \leq 1 \ \forall \ a$.
This is clear from the usual inequality $A.M \geq G.M$.
Step III: $Vol(\Omega) = \frac{(2n)^n}{n!}(\frac{\pi}{8})^s$.
Let $V_{r,s}(t)$ denote the volume of the set Ω_t defined in a similar fashion to Ω but with n replaced by the real number $t > 0$. It is easy to see from the definition that $V_{r,s}(t) = V_{r,s}(1)t^{r+2s}$. Now, if $r > 0$, then

$$\begin{aligned} V_{r,s}(1) &= 2\int_0^1 V_{r-1,s}(1-x)dx \\ &= 2V_{r-1,s}(1)\int_0^1 (1-x)^{r-1+2s}dx = \frac{2}{r+2s}V_{r-1,s}(1). \end{aligned}$$

Proceeding inductively, one obtains finally that $V_{r,s}(1) = \frac{2^r}{(r+2s)\cdots(2s+1)}$.
Similarly, if $s > 0$, then

$$\begin{aligned} V_{0,s}(1) &= \int\int_{x^2+y^2\leq 1/4} V_{0,s-1}\left(1-2\sqrt{(x^2+y^2)}\right)dxdy \\ &= \int_0^{2\pi}\int_0^{1/2} V_{0,s-1}(1-2\rho)\rho d\rho d\theta. \end{aligned}$$

Once again, iterating inductively, one finally obtains $V_{0,s}(1) = (\frac{\pi}{2})^s\frac{1}{(2s)!}$. Then, $Vol(\Omega_t) = t^n V_{r,s}(1) = t^n 2^{r-s}\pi^s\frac{1}{n!}$ which gives that $Vol(\Omega = \Omega_n) = n^n\frac{2^n}{2^{3s}}\pi^s\frac{1}{n!} = \frac{(2n)^n}{n!}(\frac{\pi}{8})^s$. The proof of Step III and, along with it, that of Minkowski's theorem, is complete.

5. Dirichlet's unit theorem

In this section, we use Minkowski's method to find the structure of the units in any algebraic number field K.

Recall that we embedded $\mathcal{O}_K$ as a lattice Λ_0 in $\mathbf{R}^n$ by means of $\theta : a \mapsto (\sigma_1(a), \cdots, \sigma_r(a), Re\tau_1(a), Im\tau_1(a), \cdots, Re\tau_s(a), Im\tau_s(a))$. Here $n = [K : \mathbf{Q}]$ and $\sigma_1, \cdots, \sigma_r, \tau_1, \bar{\tau}_1, \cdots, \tau_s, \bar{\tau}_s$ are the distinct embeddings of K in $\mathbf{C}$. Clearly, if a is a unit in $\mathcal{O}_K$, then both u and u^{-1} map to vectors which are linearly dependent. Thus, one needs to go to a subspace of $\mathbf{R}^n$ to be sensitive to the units.

Lemma. *Consider the composite map L in*

$$\mathcal{O}_K^* \subset \mathcal{O}_K \setminus 0 \stackrel{\theta}{\to} \Lambda_0 \setminus 0 \to \mathbf{R}^{r+s}$$

where the last map is $(x_1, \cdots, x_n) \mapsto$
$(log(\mid x_1 \mid), \cdots, log(\mid x_r \mid), log(x_{r+1}^2 + x_{r+2}^2), \cdots, log(x_{n-1}^2 + x_n^2)\ )$. *Then,*

(i) the image of $L : \mathcal{O}_K^* \to \mathbf{R}^{r+s}$ *is contained in the hyperplane* H *of vectors* $(x_1, \cdots, x_{r+s})$ *such that* $\sum_{i=1}^{r+s} x_i = 0$.
(ii) L *is a homomorphism.*
(iii) $Im(L) \cong \mathbf{Z}^d$ *for some* $d \leq r + s - 1$.
(iv) $\mathrm{Ker}(L) \cong \mu(K)$, *the group of roots of unity in* K *and* $\mathcal{O}_K^* \cong \mu(K) \times \mathbf{Z}^d$ *for some* $d \leq r + s - 1$.

Proof. (i) follows since units must have norm ± 1. (ii) is obvious. To see that (iii) holds, let R be any bounded region in $H \subset \mathbf{R}^{r+s}$ and let $L(u) \in R$. Then, all the conjugates of u have absolute values bounded by a constant depending on R. As the coefficients of the minimal polynomial of u are symmetric functions of the various conjugates of u, this means that there are only finitely many polynomials satisfied by units whose images under L lie in the bounded region R. In other words, $R \cap \mathrm{Im}(L)$ is finite i.e. $\mathrm{Im}(L)$ is discrete in H. Now, (iii) follows by the easy exercise below. The first assertion of (iv) is trivial and the second one follows because one can check easily that units $u_1, \cdots, u_d$ mapping under L to a basis of $\mathrm{Im}(L)$ have to generate a free abelian group.

Exercise. *Show by induction on* n *that a discrete subgroup of* $\mathbf{R}^m$ *is isomorphic to* $\mathbf{Z}^d$ *for some* $d \leq m$.

Dirichlet's unit theorem. $\mathcal{O}_K^* = \mu(K) \times V$ *where* $V \cong \mathbf{Z}^{r+s-1}$.

In other words, the image of $\mathcal{O}_K^*$ under L is actually a lattice in H. This will be seen by actually showing the existence of $r+s-1$ units whose images under L are linearly independent.

Lemma. *Fix any* $k \leq r + s$. *Then,* $\forall\ \alpha \neq 0$ *in* $\mathcal{O}_K$, *there exists* $\beta \in \mathcal{O}_K$ *with* $\mid N(\beta) \mid \leq (\frac{2}{\pi})^s \sqrt{\mid \mathrm{disc}(K) \mid}$ *and satisfies* $\beta_i < \alpha_i\ \forall\ i \neq k$. *Here* α_i, β_i *denote the co-ordinates of their images under* L.

Proof. Let c_i be constants such that $0 < c_i < e^{\alpha_i}\ \forall\ i \neq k$ and $c_k = (\frac{2}{\pi})^s \sqrt{\mid \mathrm{disc}(K) \mid} / \prod_{i \neq k} c_i$. Then, consider the set $\Omega \subset \mathbf{R}^n$ defined by $\mid x_i \mid \leq c_i$, $\forall\ i \leq r$ and $x_{r+1}^2 + x_{r+2}^2 \leq c_{r+1}, \cdots, x_{n-1}^2 + x_n^2 \leq c_{r+s}$. $\mathrm{Vol}(\Omega) = (2c_1) \cdots (2c_r)(\pi c_{r+1}) \cdots (\pi c_{r+s}) = 2^n \mathrm{Vol}(\mathbf{R}^n / \Lambda_0)$. Applying Minkowski's lemma, one gets some $t \neq 0$ in $\Omega \cap \Lambda_0$. Then, choose $\beta \in \mathcal{O}_K$ corresponding to t.

Lemma. *Fix any* $k \leq r+s$. *Then,* $\exists\ u \in \mathcal{O}_K^*$ *such that* $L(u) = (u_1, \cdots, u_{r+s})$ *satisfies* $u_i < 0\ \forall\ i \neq k$.

Proof. Start with any $\alpha_1 \neq 0$ in $\mathcal{O}_K$ and apply the previous lemma to get some β as above; call that α_2. Repetitively, one gets a sequence $\{\alpha_n\}$ in $\mathcal{O}_K$ such that for all $i \neq k$, the i-th co-ordinate of $L(\alpha_{n+1})$ is less than that of

$L(\alpha_n)$. By the lemma, $\mid N(\alpha_n) \mid$ are bounded above as $n \to \infty$. Therefore, the principal ideals (α_n) are only finitely many. Taking any $n < m$ so that $(\alpha_n) = (\alpha_m)$, we have $\alpha_m = \alpha_n u$ for some unit u. Evidently, u does the job.

The proof of Dirichlet's unit theorem is completed as follows. Observe that the units $u_k, k \leq r + s$, obtained by the previous lemma have the property that the $(r+s) \times (r+s)$ matrix $A = (a_{ij})$ whose k-th row is $L(u_k)$ satisfies $a_{ij} < 0$ for all $i \neq j$ and each row sums to 0. It is an easy elementary exercise to see that the rank of A must be $r + s - 1$.

REFERENCES

1. Gerald J. Janusz, *Algebraic Number Fields*, Graduate Studies in Mathematics, Vol. 7, Second Edition, American Mathematical Society, (1996).

2. Daniel A. Marcus, *Number Fields*, Springer-Verlag (1977).

3. Raghavan Narasimhan, S. Raghavan, S.S. Rangachari and Sundar Lal, *Algebraic Number Theory*, TIFR pamphlet (1966).

B. Sury
Indian Statistical Institute
Bangalore
e-mail: bsury@isibang.ac.in