6. Algebraic Number Fields

We can look at the factorisation problem as the study of the group of non-zero rationals; writing every element in terms of the generators (the prime numbers and -1) and taking into account the relation $(-1)^2 = 1$. The study of the unit group in $\mathbb{Z}/N\mathbb{Z}$ can be identified with the study of a suitable quotient of a suitable subgroup (elements prime to N) of this group. We now ask how this group can be generalised. One natural idea is to use algebraic number fields. An algebraic number is an "object" (we will be more specific later) that satisfies a polynomial equation with rational (equivalently integer) coefficients (we should actually insist on irreducibility of the equation). We can represent such objects as we will see below. However, it turns out that studying groups of algebraic numbers is not quite the same as studying the generalised factorisation problem; that involves the study of *divisors* or *ideals* and their groups.

6.1. **Algebraic Numbers.** How concisely can we specify an algebraic number? Since every equation in one variable with complex coefficients can be solved completely with complex numbers as solutions (Gauss's Fundamental theorem of algebra), one way to specify an algebraic number is to specify it as a complex number. However, a real (or complex) number is (in general) only specified by its *entire* decimal expansion which cannot be stored in a finite space. On the other hand it is enough to specify an algorithm that produces, on sufficient iteration, an arbitrarily close approximation to the complex number that represents it.

Thus, one way to specify an algebraic number α is as follows. First we give $P(t)$ which is the non-zero polynomial (with rational or integer coefficients) of least degree such that $P(\alpha) = 0$ (by Euclidean division applied to polynomials it follows that P divides any other Q for which $Q(\alpha) = 0$). Further, we need to specify a number x_0 of the form $r + s \cdot \sqrt{-1}$ with r and s rational so that successive iterations of Newton's method

$$x_{k+1} = x_k - \frac{P(x_k)}{P'(x_k)}$$

(where $P'(T)$ denotes the (entirely formal) derivative of $P(T)$ with respect to T) converge to the complex number representing α. There is some (minor) ambiguity in this due the to the "choice" of $\sqrt{-1}$ (which we cannot "specify" by this method). To quote Abhyankar "which is i and which $-i$, perhaps only a physicist can tell!"

Another way is to make use of Hensel's lemma. We will define below the discriminant D_P for a polynomial P. For now it suffices that if a prime p does not divide D_P then for any n so that p divides $P(n)$, we have that p does not divide $P'(n)$. In other words D_P is the least common multiple of $\gcd(P(n), P'(n))$ as n varies over all integers. Now, for n sufficiently large it is clear that there is such a prime p (i. e. not dividing D_P) so that p divides $P(n)$. We can now specify α by saying that is should be *congruent to* n modulo p. Because of Hensel's lemma (which is Newton's iteration done modulo powers of p!) we can then produce n_k so that $\alpha - n_k$ is divisible by p^k for every k. In modern language, we are replacing the approximation by complex numbers given above by a p-adic approximation. We can actually, find a suitable p so that this can be done for *all* roots of the polynomial P. (This is a particular case of Chebychev's density theorem).

An entirely less obvious problem is how we can perform common arithmetic operations on algebraic numbers when they are represented in this fashion. For

that reason, and for the reason mentioned at the beginning of this section we now turn to the matrix representation of algebraic numbers.

6.2. **Algebraic Number Fields as Matrix Algebras.** Let n be any positive integer and consider a sub-algebra K of the algebra of $n \times n$ matrices with rational entries; by this we mean that K contains scalar multiples of the identity matrix and is closed under matrix addition, subtraction and multiplication. To handle division we also insist that non-zero matrices in K are invertible (this actually implies that the inverses are also in K but it is not entirely trivial to prove this). Finally, one knows that the algebra of matrices is not commutative for $n \geq 2$. So we put in an additional hypothesis that matrix multiplication between elements of K is commutative.

Now, consider the map $\alpha \mapsto \alpha \cdot v$ where v is any (fixed) non-zero column vector such as the transpose of $(1, 0 \ldots, 0)$. When α and β are an elements of K with $\alpha \cdot v = \beta \cdot v$, we obtain $(\alpha - \beta) \cdot v = 0$. But we have assumed that every non-zero element of K is invertible so we must have $\alpha - \beta = 0$. In other words this map is *one-to-one* on K. Thus K is actually isomorphic to a vector space of rank at most n over the rationals. By a suitable change of basis (and restricting to a submatrix) we may as well assume that the space $K \cdot v$ contains *all* column vectors or equivalently that K has rank n. Then $K \cdot w$ is the space of all column vectors for *any* non-zero vector w. We will henceforth make this additional assumption as well.

For any $n \times n$ matrix α we have (the Cayley-Hamilton theorem) that *characteristic* polynomial $\mathrm{ch}_\alpha(T)$ of degree n and $\mathrm{ch}_\alpha(\alpha) = 0$. (In the words of one mathematician *khudh kaa nahi satisfy karega to kiska satisfy karega?*(Hindi); if it doesn't satisfy its' own then whose will it satisfy?). On the other hand, we have the minimal polynomial $\min_\alpha(T)$, which is the polynomial of least degree with rational coefficients that is satisfied by α. If $\min_\alpha(T) = P(T)Q(T)$, then $P(\alpha)Q(\alpha) = 0$. Since, $P(\alpha)$ and $Q(\alpha)$ are in K at least one of them must be zero thus one of them must be a constant; in other words the minimal polynomial is *irreducible*. It also follows as before that it divides the characteristic polynomial. One can show that, under the hypothesis of the previous paragraph (and the fact the we are working over rationals; a *perfect* field), there is an element α in K whose characteristic polynomial is *irreducible*, i. e. its characteristic polynomial equals its minimal polynomial. In particular, the field K has a basis over the field $\mathbb{Q}$ of rationals of the form $1, \alpha, \ldots, \alpha^{n-1}$.

(Sketch of Proof). Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a basis of K over the field $\mathbb{Q}$. Consider the characteristic polynomial of $T_1\alpha_1 + \cdots + T_n\alpha_n$ as a function of the *variables* $T_1, \ldots, T_n$. The condition that this is reducible will impose certain non-trivial polynomial relations between the T_k's. Thus all we need to do is to find rational numbers r_k that do not satisfy these relations. Then the characteristic polynomial of $\alpha = r_1\alpha_1 + \cdots + r_n\alpha_n$ will be irreducible (and of degree n. It follows that, the elements $1, \alpha, \ldots, \alpha^{n-1}$ will be independent over $\mathbb{Q}$. □

To summarise, we will henceforth think of an algebraic number field as a sub-algebra of the ring of $n \times n$ matrices which is commutative, with all non-zero elements being invertible. Moreover, this algebra contains an element α whose characteristic polynomial $P_(T)$ is equal to its minimal polynomial. An further extension of the above argument then shows that *any* invertible matrix g that

commutes with every element of K is contained in K; we will use this in later sections.

As an example, let us consider the "construction" of the field associated with an irreducible polynomial $P(T) = T^n + a_1 T^{n-1} + \cdots + a_n$. We consider the matrix

$$\alpha_P = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -a_n & -a_{n-1} & \cdots & -a_1 \end{pmatrix}$$

This has minimal polynomial and characteristic polynomial equal to $P(T)$. The sub-algebra of matrices generated by α_P is the required field $\mathbb{Q}(\alpha_p)$, sometimes also denoted by $\mathbb{Q}[T]/(P(T))$ (one uses Euclid's algorithm for polynomials to show that every non-zero element of this is invertible). The above discussion says that any field under consideration is *isomorphic* to a field of this form for some irreducible polynomial $P(T)$.

6.3. **Orders and Maximal orders.** We now look a the subring R of K consisting of matrices with *integer* entries; R is called an *order* in K. Now, for any invertible $n \times n$ matrix g it is clear that gKg^{-1} is isomorphic to K; *but* g or g^{-1} may have entries with denominators. So the ring R_g consisting of matrices in gKg^{-1} with integer entries need not be that same as R. Thus, one can look for a *maximal* order. We will see below that one such exists and is unique. It is usually called the ring of integers in K and is denoted by $\mathcal{O}_K$.

There is a natural symmetric pairing on $n \times n$ matrices given by

$$\langle A, B \rangle = \text{Trace}(A \cdot B)$$

We study the restriction of this to K. This pairing is *non-degenerate*; i. e. for any non-zero A there is a B so that $< A, B > \neq 0$. For example, if α in K, then $\langle \alpha, \alpha^{-1} \rangle = \text{Trace}(1) = n$ which is non-zero! (Clearly, a different argument is required when the base field is not $\mathbb{Q}$ but a finite field). From the non-degeneracy it also follows that for *any* additive map from K to the rationals $\mathbb{Q}$ there is an α in K so that the map is precisely $\beta \mapsto \langle \alpha, \beta \rangle$.

Now, R is a subgroup of the finitely-generated free abelian group of $n \times n$ matrices with integer coefficients; thus R is a finitely-generated free abelian group as well. If α is any element of K we can clear denominators to find an integer d so that $d\alpha$ is a matrix with integer entries. It follows that R contains a basis of K as a vector space over $\mathbb{Q}$. Thus R is of the form $\mathbb{Z} \cdot w_1 + \cdots + \mathbb{Z} \cdot w_n$; moreover, $K = \mathbb{Q} \cdot w_1 + \cdots + \mathbb{Q} \cdot w_n$. Let $\check{R}$ denote the collection of all elements α in K so that $< \alpha, \beta >$ is an *integer* for all β in R. Finding such an α is clearly equivalent to solving the system of equations

$$\begin{array}{ccccccc} r_1 \cdot \langle w_1, w_1 \rangle & + & \cdots & + & r_n \cdot \langle w_n, w_1 \rangle & = & p_1 \\ \vdots & & & & \vdots & & \vdots \\ r_1 \cdot \langle w_1, w_n \rangle & + & \cdots & + & r_n \cdot \langle w_n, w_n \rangle & = & p_n \end{array}$$

By Cramer's rule, this requires the inversion of the matrix $(\langle w_i, w_j \rangle)_{i=1,j=1}^{n,n}$. The determinant of this matrix is called the *discriminant* of the order R and is denoted by D_R. Note that if $v_1, \ldots, v_n$ is another basis for R and A is the matrix that gives the "change of co-ordinates", then the determinant of $(\langle v_i, v_j \rangle)_{i=1,j=1}^{n,n}$ differs from the earlier determinant by $\det(A)^2$. Since A and A^{-1} have integer entries,

$\det(A) = \pm 1$. Hence D_R is independent of the choice of basis. Clearly, $R \subset \check{R}$ and $\check{R}/R$ is a finite group with $|D_R|$ elements.

Now suppose $R \subset S$, where S is another order (i. e. an R_g for some g). We clearly have the sequence of inclusions $R \subset S \subset \check{S} \subset \check{R}$. It follows that D_S *divides* D_R; by decreasing induction we see that there is a maximal order. We also note that by duality, S/R and $\check{R}/\check{S}$ have the same order, so that D_R is the multiple of D_S by the *square* of an integer. Let $\mathcal{O}_K$ be the collection of all elements of K whose characteristic polynomials have integer coefficients; one can show that this is closed under addition and multiplication. It is clear that $\mathcal{O}_K$ contains R since very matrix with integer entries has a characteristic polynomial with integer coefficients. By the above, we see that $\mathcal{O}_K$ is contained in $\check{R}$, hence it is finitely generated; let $\mathcal{O}_k = \mathbb{Z} \cdot u_1 + \cdots + \mathbb{Z} \cdot u_n$. Let v be any non-zero column vector and consider the basis $u_i \cdot v$ of the space of column vectors. With this change of basis, each each element of $\mathcal{O}_K$ is represented by a matrix with integer entries. Thus $\mathcal{O}_K$ is an order and the *unique* maximal order.

An extension of the example we looked at for fields is to associate an order with an irreducible polynomial $P(T) = T^n + a_1 T^{n-1} + \cdots + a_n$ where the a_i are all integers. We continue the notation of the previous subsection. It follows that α_P is a matrix with integer coefficients; with a little effort one can also show that the natural order R_P in $\mathbb{Q}(\alpha_P)$ is precisely the collection of all integer linear combinations of the powers $1, \alpha_P, \ldots, \alpha_P^{n-1}$. The discriminant of this order is also the discriminant of the polynomial $P(T)$ and is denoted as D_P. Unlike the case of fields, however, it is *not* true that every order has the form R_P for some polynomial $P(T)$.

6.4. **Lattices and ideals.** To generalise one step further, we can consider any finitely-generated subgroup M of K which contains a basis of K over $\mathbb{Q}$; such an M is called a *lattice*. Standard arguments then show that M is of the form $\mathbb{Z} \cdot m_1 + \cdots + \mathbb{Z} \cdot m_n$ for some basis m_i of K. For any fixed column vector v, let g be the invertible matrix that makes $m_i \cdot v$ the standard basis of the space of column vectors. Then after applying g, we see that $M \cdot v$ becomes the standard lattice of column vectors with integer entries. The collection $R(M)$ of all matrices in K that take M to itself, is thus identified with the ring which we denoted as R_g above. In the following paragraphs we assume that we have made this change of co-ordinates (i. e. that g is the identity matrix). In that case $R = R(M)$ is precisely the order consisting of integer matrices. Moreover, there is a non-zero vector v so that M is precisely the collection of all α so that $\alpha \cdot v$ is a vector with integer entries.

By collecting the denominators of the generators of M we can find a non-zero integer d so that $d \cdot M$ is contained in R. Since this is a subgroup of R that is closed under multiplication by R, it is an *ideal* I in R. Thus $M = d^{-1} I$ is a *fractional ideal* for R. It is clear that $R(d \cdot M) = R(M) = R$. More generally, for any non-zero α in K, we have $R(\alpha \cdot M) = R$. Moreover, $\alpha \cdot M$ is obtained by replacing the v in the previous paragraph by $\alpha^{-1} v$, which is just another non-zero vector.

Conversely, let I be a non-zero ideal in the ring R. Let α be a non-zero element of I. Then α^{-1} is in K and by collecting the denominators we find a non-zero integer d so that $d \cdot \alpha^{-1}$ has integer coefficients so is in R. But then $d = d\alpha^{-1} \cdot \alpha$ is in I; thus I contains $d \cdot R$. In particular, I contains a basis of K and is a free group of rank n; in other words I is a lattice. Clearly R is contained in $R(I)$ but in general the latter could be bigger.

Now, for any non-zero ideal in R we have the *restriction* $I \cap \mathbb{Z} = a\mathbb{Z}$. By the above discussion this is a non-zero ideal in $\mathbb{Z}$. We also see that R/I is a quotient of the finite group R/aR; the latter group has order a^n. The order of R/I is called the *norm* of the ideal and denoted as $\mathrm{Nm}(I)$. The norm of an element α is $\det(\alpha)$; these two definitions are related since $\mathrm{Nm}(\alpha \cdot R) = |\det(\alpha)|$ (Exercise).

Now, we noted above that $\mathrm{Nm}(d \cdot R) = d^n$ for any positive integer d so we can extend the above definition by defining for $M = d^{-1}I$, $\mathrm{Nm}(M) = d^{-n}\,\mathrm{Nm}(I)$. Similarly, the restriction of $d \cdot R$ is clearly d, so we define the restriction of M to be $d^{-1}(I \cap \mathbb{Z})$. When M is contained in (i. e. M is an ideal) R, the two definitions are consistent.

6.5. **Groups of invertible fractional ideals.** The above definitions depended on a choice of ring $R \subset R(M)$, but the following definition does not. As before, let $\check{M}$ denote the collection of all α in K for which $\langle \alpha, \beta \rangle$ is an integer for every β in M. Now, the non-degeneracy of the pairing $\langle , \rangle$ means that for every additive map from K to $\mathbb{Q}$ there is an α in K so that the additive map is given by $\beta \mapsto \langle \alpha, \beta \rangle$. It follows that $\check{M}$ can also be identified with the collection of *all* additive maps from M to $\mathbb{Z}$. By the usual double-duality result it follows that $M = (\check{M})\check{}$. In particular, we see that $\check{M}$ is also a lattice and $R(\check{M}) = R(M)$.

Let $[M : R]$ denote the collection of all α in K so that $\alpha \cdot M$ is contained in R. Clearly, $d \cdot R$ is contained in $[M : R]$. On the other hand $\check{M} = [M : \check{R}]$ was shown above to contain all α that send M into $\check{R}$. The latter contains R so we see that $[M : R]$ is contained in $\check{M}$. Thus $[M : R]$ is also a lattice. Specifically, we define C_R as $[\check{R} : R]$.

Definition 3. Let M be a lattice in K and $R \subset R(M)$. Then we say that M is projective over R if $M \cdot [M : R] = R$. When $R = R(M)$ and we have $[M : R] = C_R \cdot \check{M}$ then we say that M is a *Gorenstein* R module. Here the product of lattices $L_1 \cdot L_2$ is the collection of all linear combinations of products $\alpha\beta$ with α in L_1 and β in L_2.

Armed with this result, we now consider the collection of all lattices M with the property that $R(M) = R$ for a fixed *Gorenstein* order R. This collection of lattices includes R, $\check{R}$ and C_R. For any such M, the above lemma says that $M \cdot [M : R] = R$. If we define the product of M and N as $M \cdot N$, then this shows that we have a group with R playing the role of identity. It is further clear that M and $\alpha \cdot M$ are naturally isomorphic for any non-zero α in K. We may further consider lattices modulo such isomorphisms. This gives us the *class group* of invertible fractional ideals modulo isomorphism which is denoted by $\mathrm{Cl}(R)$. We noted above that there could be ideals (and fractional ideals) M for R such that R is a proper subring of $R(M)$. In this case we do not necessarily have $M[M : R] = R$; we do not include such M in the class group. However, since $R(M)$ is an order as well, this situation cannot arise if R is the maximal order $\mathcal{O}_K$. The corresponding class group is sometimes loosely referred to as the class group of K and denoted $\mathrm{Cl}(K)$.

6.6. **Minkowski's Geometry of Numbers.** In order to decide whether or not a lattice M is of the form $\alpha \cdot R$ (and hence trivial in the class group) we need to find elements α in M whose norm is as close as possible to that of M. This is achieved in the following section.

We now want to give a "measure" associated with an order R. The space of $n \times n$ matrices with rational entries is naturally contained in the space of $n \times n$ matrices with real entries. Thus we can consider the ring $\mathbb{R} \cdot K$ of real linear combinations of elements of K. This is an n-dimensional vector space over $\mathbb{R}$. Thus, for any lattice M, the space $T_M = \mathbb{R} \cdot K/M$ is an n-dimensional torus. Taking some translation invariant measure on $\mathbb{R} \cdot K$ gives us a notion of volume for the tori T_M with the property that $\mathrm{vol}(T_M) = \mathrm{vol}(T_R)\,\mathrm{Nm}(M)$. Now, if A is any (compact measurable) subset of $\mathbb{R} \cdot K$ with the property that $\mathrm{vol}(A) > \mathrm{vol}(T_M)$ then the map $A \to T_M$ cannot be one-to-one (with a little thought it is clear that this is actually also true if $\mathrm{vol}(A) \geq \mathrm{vol}(T_M)$). The difference between two points with the same inverse image will give a non-zero element of M.

Now, one natural way to identify $\mathbb{R} \cdot K$ with $\mathbb{R}^n$ (and thus put a measure on it) is to use "simultaneous diagonalisation". As seen above K is generated by a single $n \times n$ matrix α whose characteristic polynomial $P(T)$ is irreducible over rationals. This means that this has distinct roots and so over real numbers can be brought into a "diagonal" form as below by a suitable change of co-ordinates.

$$\begin{pmatrix}
\alpha^{(1)} & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\
0 & \alpha^{(2)} & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots & \vdots \\
0 & 0 & \dots & \alpha^{(r_1)} & 0 & 0 & \dots & 0 & 0 \\
0 & 0 & \dots & 0 & \mathrm{Re}\,\tilde{\alpha}^{(1)} & \mathrm{Im}\,\tilde{\alpha}^{(1)} & \dots & 0 & 0 \\
0 & 0 & \dots & 0 & -\mathrm{Im}\,\tilde{\alpha}^{(1)} & \mathrm{Re}\,\tilde{\alpha}^{(1)} & \dots & 0 & 0 \\
\vdots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \dots & 0 & 0 & 0 & \dots & \mathrm{Re}\,\tilde{\alpha}^{(r_2)} & \mathrm{Im}\,\tilde{\alpha}^{(r_2)} \\
0 & 0 & \dots & 0 & 0 & 0 & \dots & -\mathrm{Im}\,\tilde{\alpha}^{(r_2)} & \mathrm{Re}\,\tilde{\alpha}^{(r_2)}
\end{pmatrix}$$

Here $\alpha^{(i)}$ denote the real roots of $P(T)$, while $(\tilde{\alpha}^{(j)}, \overline{\tilde{\alpha}^{(j)}})$ are the pairs of conjugate complex roots of $P(T)$. Now, every element of K is a linear combination of powers of α so that it too is brought into the above form by the *same* change of co-ordinates. For simplicity of notation we write the matrix associated with an element β of K as $[\beta^{(1)}, \dots, \beta^{(r_1)}, \tilde{\beta}^{(1)}, \dots, \tilde{\beta}^{(r_2)}]$. More generally, for any element x in $\mathbb{R} \cdot K$ we have a representation $[x^{(1)}, \dots, x^{(r_1)}, \tilde{x}^{(1)}, \dots, \tilde{x}^{(r_2)}]$. This representation gives us an identification of $\mathbb{R} \cdot K$ with $\mathbb{R}^n$. If $R = \mathbb{Z} \cdot w_1 + \cdots + \mathbb{Z} w_n$, then the volume of T_R, with respect to this identification is the determinant of the $n \times n$ matrix Ω given by

$$\Omega = \left(w_i^{(1)}, \dots, w_i^{(r_1)}, \mathrm{Re}\,\tilde{w_i}^{(1)}, \mathrm{Im}\,\tilde{w_i}^{(1)}, \dots, \mathrm{Re}\,\tilde{w_i}^{(r_2)}, \mathrm{Im}\,\tilde{w_i}^{(r_2)} \right)_{i=1}^{n}$$

Let the matrix $\tilde{\Omega}$ (complex entries) be given by

$$\tilde{\Omega} = \left(w_i^{(1)}, \dots, w_i^{(r_1)}, \tilde{w}_i^{(1)}, \overline{\tilde{w}_i^{(1)}}, \dots, \tilde{w}_i^{(r_2)}, \overline{\tilde{w}_i^{(r_2)}} \right)_{i=1}^{n}$$

Standard rules for column operations on determinants show that the determinant of $\tilde{\Omega}$ is 2^{r_2} times the determinant of Ω. On the other hand the (i,j)-th entry of the matrix $\tilde{\Omega} \cdot \tilde{\Omega}^t$ is

$$\sum_{p=1}^{r_1} w_i^{(p)} w_j^{(p)} + \sum_{q=1}^{r_2} \tilde{w}_i^{(q)} \tilde{w}_j^{(q)} + \sum_{q=1}^{r_2} \overline{\tilde{w}_i^{(q)}}\, \overline{\tilde{w}_j^{(q)}}$$

which we immediately recognise as $\mathrm{Trace}(w_i \cdot w_j)$ when it is expressed in the form given above. Combining these observations we obtain the identity $\mathrm{vol}(T_R) = (1/2^{r_2})\sqrt{|D_R|}$.

Now consider the region A consisting of all x in $\mathbb{R} \cdot K$ so that $|x^{(i)}| \leq a_i$ and $|\tilde{x}^j| \leq b_i$ for some positive constants a_i and b_j. We have

$$\mathrm{vol}(A) = 2^{r_1}\pi^{r_2} \prod_{i=1}^{r_1} a_i \prod_{j=1}^{r_2} b_j^2$$

Thus, in order to obtain a pair (v_1, v_2) in A so that $v = v_1 - v_2$ is a non-zero element of M we need the condition

$$2^{r_1}\pi^{r_2} \prod_{i=1}^{r_1} a_i \prod_{j=1}^{r_2} b_j^2 = (1/2^{r_2})\sqrt{|D_R|}\,\mathrm{Nm}(M)$$

Now the norm of the element v is the product

$$\mathrm{Nm}(v) = \prod_{i=1}^{r_1} |v_1^{(i)} - v_2^{(i)}| \cdot \prod_{j=1}^{r_2} |\tilde{v}_1^{(j)} - \tilde{v}_2^{(j)}|^2 \leq 2^{r_1} \prod_{i=1}^{r_1} a_i \times 2^{2r_2} \prod_{j=1}^{r_2} b_j^2$$

Hence, we have the following

Lemma 14. *For any ideal I of an order R in K there is a non-zero element v in I so that*

$$\mathrm{Nm}(v) \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|D_R|} \cdot |R/I|$$

Here we have written $|R/I|$ instead of $\mathrm{Nm}(I)$ in order to make the dependence on R clear.

Proof. We just combine the inequality above with the condition that needs to be satisfied in order to obtain such a v. □

In particular, if I is an invertible ideal, then $vR = I \cdot J$ where $J = vR \cdot I^{-1}$ and $\mathrm{Nm}(J) \leq (2/\pi)^{r_2}\sqrt{|D_R|}$. Now, for any element of the class group $\mathrm{Cl}(R)$, let I represent the inverse of this class. The above argument produces a representative J of the class which has norm no more than $(2/\pi)^{r_2}\sqrt{|D_R|}$. In particular, we have shown than the class group is finite (an ideal J of norm n is a quotient of cardinality n the group R/nR; there are at most finitely many such quotient groups).

While it is not too difficult to use this procedure to write all the ideals J satisfying the above condition, it is much harder to write the "multiplication table" for the group $\mathrm{Cl}(R)$ on the basis of what has gone so far. If J_1 and J_2 are two ideals as above and the product no longer satisfies the above condition, then we need to find the element v in $(J_1 \cdot J_2)$ that the lemma guarantees. But the proof of the lemma gives us no way to find such elements!

6.7. **Prime ideals.** Another way to write generators of groups of ideals is to use prime ideals. An ideal P of R is prime if for every a and b in R so that ab lies in P at least one of a and b lies in P; an equivalent assertion is that R/P is a domain—non-zero elements give non-zero products. It is clear that the restriction $P \cap \mathbb{Z}$ satisfies the same conditions for integers a and b. In other words $P \cap \mathbb{Z}$ is generated by a prime number p. Thus P determined by the ideal P/pR in R/pR. Now, if $R = \mathbb{Z} \cdot w_1 + \cdots + \mathbb{Z} \cdot w_n$, then R/pR is a vector space of rank n over the finite field $\mathbb{Z}/p\mathbb{Z}$. Instead of solving this specific problem, we can ask for a structure theorem

for commutative rings with identity with underlying additive group a vector space of rank n over $\mathbb{Z}/p\mathbb{Z}$.

Lemma 15. *Any ring with underlying additive group a finite dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$ is a direct sum of rings of the form $(\mathbb{Z}/p\mathbb{Z})[T]/(P(T)^m)$, where $P(T)$ is an irreducible polynomial over the field $\mathbb{Z}/p\mathbb{Z}$.*

This result follows from the Chinese Remainder theorem and Euclidean division applied to the polynomial ring in one variable $(\mathbb{Z}/p\mathbb{Z})[T]$. If we use the symbol $\mathbb{F}_q$ to denote the field with q elements (where q is a prime power), then this result can be refined further as follows

Lemma 16. *The ring $(\mathbb{Z}/p\mathbb{Z})[T]/(P(T)^m)$, where $P(T)$ is an irreducible polynomial of degree d, is isomorphic to the ring $\mathbb{F}_{p^d}[h]/(h^n)$.*

This result follows by constructing (using Newton's method of successive approximations) a polynomial $\tilde{T}$ of the form $T + P(T)Q_1(T) + \cdots + P(T)^{n-1}Q_{n-1}(T)$ so that $P(\tilde{T})$ is divisible by $P(T)^n$. Then $h = \tilde{T} - T$. Combining these results, we see that R/pR has the form

$$\frac{\mathbb{F}_{p^{f_1}}[h_1]}{(h_1^{e_1})} \oplus \cdots \oplus \frac{\mathbb{F}_{p^{f_g}}[h_g]}{(h_g^{e_g})}$$

Corresponding to each factor we get a surjective ring homomorphism $R/pR \to \mathbb{F}_{p^{f_i}}$. The kernel of this has the form P_i/pR for a prime ideal P_i whose restriction is p. The number f_i is called the residual degree (or more simply the degree) of P_i over p, while the number e_i is called the ramification degree (or order of ramification) of P_i over p.

Now, let I be any ideal. Suppose first that the restriction i of I is of the form $i_1 i_2$, with i_1 and i_2 co-prime. We can apply the Chinese Remainder theorem to write R/I as a direct sum of R/I_1 and R/I_2, where $I_1 = I + i_1 R$ and $I_2 = I + i_2 R$. Thus $I = I_1 \cap I_2$; if I is invertible one easily shows that $I = I_1 \cdot I_2$. Thus we can reduce our study of groups of ideals to the study of ideals Q so that the restriction q is the power of a prime p. Now, $R/(Q + pR)$ is a quotient of the ring studied above and is not zero. Thus there is a prime P_i as above so that Q is contained in P_i. By successively removing such P_i (if Q is invertible) we can write Q as a product of various powers of the P_i considered above. Thus we have written any invertible ideal as a product of (invertible) prime ideals. It is not difficult to show that any such product expression is unique. Thus, we obtain the unique factorisation of ideals in terms of prime ideals.