October 5:

Math 432 Class Lecture Notes

- Does $\mathbf{Z}_F$ have a basis over $\mathbf{Z}$?
- Free abelian groups

0.1 Does $\mathbf{Z}_F$ have a basis over Z?

Let $\mathbf{F}$ be a number field of degree n over $\mathbf{Q}$. Let $\alpha_1, \ldots, \alpha_n$ be a basis of $\mathbf{F}$ over $\mathbf{Q}$. By multiplying each α_i by an integer, if necessary, we can assume that each α_i is in $\mathbf{Z}_F$, i.e., that each α_i is an algebraic integer.

The set

$$\mathrm{span}_{\mathbf{Z}}(\alpha_1, \cdots, \alpha_n) = \left\{ \sum_{i=1}^{n} a_i \alpha_i : a_i \in \mathbf{Z} \text{ for all } i \right\}$$

of all integral linear combinations of the α_i is a subgroup of (the additive group of) $\mathbf{Z}_F$. In fact we can bound the distance between $\mathrm{span}_{\mathbf{Z}}(\alpha_i)$ and $\mathbf{Z}_F$ in terms of the discriminant of the basis.

Theorem 1. Let $\alpha_1, \ldots, \alpha_n$ be a basis of $\mathbf{F}$ over $\mathbf{Q}$, where each $\alpha_i \in \mathbf{Z}_F$, and let $d = \mathrm{disc}(\alpha_1, \cdots, \alpha_n)$. Then for every $\alpha \in \mathbf{Z}_F$

$$d\alpha = \sum_{i=i}^{n} a_i \alpha_i, \quad a_i \in \mathbf{Z},$$

i.e., when α is expressed as a linear combination of the basis elements the rational numbers that occur as coefficients have denominators that are divisors of d.

Proof. Let α be an element of $\mathbf{Z}_F$. Then we have

$$\alpha = \sum_{i=i}^{n} b_i \alpha_i \qquad \text{where } b_1, \ldots, b_n \in \mathbf{Q}.$$

For each j, $1 \leq j \leq n$, we have

$$\alpha^{(j)} = \sum_{i=i}^{n} b_i \alpha_i^{(j)}$$

where the superscripts denote the images under the various embeddings. This system of equalities can be written in matrix form as $v = Mb$, where

$$v = \begin{bmatrix} \alpha^{(1)} \\ \alpha^{(2)} \\ \vdots \\ \alpha^{(n)} \end{bmatrix}, \quad M = \begin{bmatrix} \ldots\ldots\ldots\ldots\ldots \\ \alpha_1^{(i)} \quad \cdots \quad \alpha_n^{(i)} \\ \ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots \end{bmatrix}, \quad \text{and} \quad b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}.$$

Now we have $M^T v = M^T M b$, thus $(M^T M)^{-1} M^T v = b$. Now we see that $M^T M = [TrF/\mathbf{Q}(\alpha_i \alpha_j)]$, and $M^T v = [Tr_{F/\mathbf{Q}}(\alpha \alpha_i)]$. However,,

$$(M^T M)^{-1} = \frac{1}{d}[(-1)^{i+j}(M^T M)_{ij}]$$

where $(M^T M)_{ij}$ is the ij^{th} cofactor, and $d = \det(M^T M) = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$. Thus db is a matrix of integers, so

$$\alpha = \sum_{i=i}^{n} \frac{a_i}{d} \alpha_i \qquad \text{where } a_1, \ldots, a_n \in \mathbf{Z}.$$

□

Thus we see that $\mathbf{Z}_F \subset \operatorname{span}_{\mathbf{Z}} (\alpha_1/d, \cdots, \alpha_n/d)$.

0.2 Free abelian groups

Definition 2. A finitely generated free abelian group, or **fab** for short, is a finitely generated free $\mathbf{Z}$-module. Equivalently, a fab is a finitely generated torsion-free abelian group. The **rank** of a fab is its number of generators (from results below, it follows immediately that any two generating sets have the same number of elements).

Example 3. The lattice $\{(0,0)\}$ inside $\mathbf{Z}^2$ has rank 0, and $\mathbf{Z}^2$ itself has rank 2. The set $\{nv : n \in \mathbf{Z}\}$ of all multiples of a given nonzero vector $v \in \mathbf{Z}^2$ forms a line of lattice points, and is a fab of rank 1.

Example 4. Any fab G of rank 2 in $\mathbf{Z}^2$ is of finite index, where the index is the number of cosets, i.e., the order of the quotient group $\mathbf{Z}^2/G$.

- The fab consisting of vectors (x, y) where $x + y$ is even has index 2.

- The fab consisting of vectors (x, y) where both x and y are even has index 4, and is sometimes denoted $2\mathbf{Z}^2$.

- The fab G generated by $(2, 1)$ and $(0, 3)$ has coset representatives (i, j) where $0 \leq i < 2$, $0 \leq j < 3$, as can be checked by showing that every element of $\mathbf{Z}^2$ is congruent to one of them modulo G, and no two of them are congruent modulo G‘

The key results that we will need about fab's are that any subgroup H of a fab G of rank n is itself a fab of rank $m \leq n$, and if $m = n$ then H has finite index in G, and the index can be obtained by taking the absolute value of the determinant of the change of basis matrix.

In class these proofs were done in the case $n = 2$; the arguments in the general case are similar.

Theorem 5. If G is a fab with basis $e_1, \cdots, e_n$ and H is a subgroup of G, then H is a fab, and it has a basis f_j, $1 \leq j \leq m$ such that the change of basis matrix is upper triangular, i.e.,

$$f_i = \sum_{j \geq i} a_{ij} e_j, \qquad a_{ij} \in \mathbf{Z}.$$

In particular, the rank of H is less than or equal to the rank of G.

Proof. Without loss of generality we can take $G = \mathbf{Z}^n$, and the basis e_i to be the standard basis vectors. (This is exactly the picture we get by writing elements g of G as linear combinations of the basis vectors, and mapping g to the vector of coefficients.)

We prove the result by induction on n. The case n is trivial: any subgroup of $\mathbf{Z}$ is an ideal and is therefore principal. So either H is $\{0\}$ or else there is a vector f_1 such that $H = \mathbf{Z} f_1$ consists of all multiples of f_1.

Let $n > 1$, assume that the result is true for all ranks smaller than n. Consider the projection π of $\mathbf{Z}^n$ onto its first $n-1$ components. The kernel consists of all multiples $\mathbf{Z}e_n$ of the last basis vector (i.e., all vectors whose first $n-1$ coefficients are 0). Let $H' = \pi(H)$ be the image of H under this map, and $K = \ker(\pi) \cap H$. This information is summarized by a diagram

By our induction assumption, H' is a fab with rank at most $n-1$ and the change of basis matrix is upper triangular. Let $f_1, \cdots, f_k$ be elements of H whose images under π are a basis of H'. If $K = \{0\}$ then $H = \mathrm{span}_{\mathbf{Z}}(f_1, \cdots, f_k)$ and we are done. Otherwise, K is an ideal in $\mathbf{Z}$, and we let f_{k+1} be a generator. One checks that $f_1, \cdots, f_{k+1}$ is the desired basis of H. □

Remark 6. The matrix interpretation of this result is that any matrix of integers can be converted to upper triangular form by row operations over the integers (i.e., division by an integer is not allowed).

Corollary 7. The ring $\mathbf{Z}_F$ of algebraic integers in a number field F is a fab of rank n.

Proof. If α_i is an arbitrary basis of algebraic integers with discriminant d then

$$\mathrm{span}_{\mathbf{Z}}(\alpha_i) \subset \mathbf{Z}_F \subset \mathrm{span}_{\mathbf{Z}}(\alpha_i/d)$$

and the corollary follows immediately, using the theorem. □

If the rank of the subgroup H is equal to the rank n of G then one checks that the set of vectors

$$\sum_{i=1}^{n} c_i e_i, \quad 0 \le c_i < |a_{ii}|$$

is a set of coset representatives for H in G. Thus H is of finite index in G, and the index is equal to the product of the $|a_{ii}|$, i.e., the absolute value of the determinant of the (upper triangular) change of basis matrix.

Theorem 8. If $e_1, \cdots, e_n$ and $e'_1, \cdots, e'_n$ are two different basis of the fab G, then the change of basis matrix A has the property that $\det(A) = \pm$.

Proof. Writing

$$e'_i = \sum_{j=1}^{n} a_{ij} e_j, \qquad e_i = \sum_{j=1}^{n} b_{ij} e'_j$$

one finds by substitution of one set of equations into the other that $AB = BA = I_n$. Thus $\det(A)\det(B) = 1$, and since the matrix entries, and the determinants of the matrices, are integers it follows that both determinants are equal to ± 1. □

Corollary 9. If G is a fab of rank n, and H is a subgroup of rank n then the index of H in G is the absolute value of the determinant of a change of basis matrix.

Proof. The earlier theorem said that this was true for a specific change of basis matrix A. Changing the basis for H changes the change-of-basis matrix A my multiplying it on the left by a matrix M that is the change-of-basis matrix between the two bases of H. By the preceding theorem, $\det(M) = \pm 1$ and therefore

$$|\det(MA)| = |\det(A)| = [G : H]$$

as claimed. □