October 8:

Math 432 Class Lecture Notes

- The discriminant of a field
- Power bases
- Ideals

0.1 The discriminant of a field

Last time we saw that a subgroup H of a fab G of finite rank n is itself a fab of rank at most n. Moreover, if a basis of G is given, then there is a basis of H such that the "change of basis matrix" is upper triangular. If the rank of H is the same as the rank of G, then H is of finite index, and it can be checked directly that the index is the (absolute value of the) product of the diagonal entries.

Since any two bases of a fab of rank n are related by change of bases matrices of determinant ± 1, it follows that the index of H in G is the absolute value of the determinant of *any* change of basis matrix.

Theorem 1. If F is a number field of rank n over $\mathbf{Q}$ then the ring of integers $\mathbf{Z}_F$ is a fab of rank n.

Proof. Choose a basis $\alpha_1, \cdots, \alpha_n$ of F over Q (i.e., a basis as a $\mathbf{Q}$-vector space). Without loss of generality, by multiplying by integers if necessary, we can assume that each α_i is an algebraic integer. If $d = \mathrm{disc}(\alpha_1, \cdots, \alpha_n)$

then by earlier work we know that $\mathbf{Z}_F$ is sandwiched in between two fabs of rank n:

$$\mathrm{span}_{\mathbf{Z}}(\alpha_1, \cdots, \alpha_n) \subset \mathbf{Z}_F \subset \mathrm{span}_{\mathbf{Z}}(\alpha_1/d, \cdots, \alpha_n/d).$$

The result follows from our general results, recalled above, on fabs. □

Definition 2. The discriminant of a number field F is defined to be the discriminant of some (and hence any) basis of $\mathbf{Z}_F$.

(Recall that the discriminant of two bases of F over $\mathbf{Q}$ are related by the square of the determinant of the change of basis matrix; since two basis of $\mathbf{Z}_F$ are related by a matrix of determinant ± 1 it follows that the discriminant as defined above is indeed well-defined.)

The problem of finding $\mathbf{Z}_F$ is usually fairly easy in the case of textbook examples that are intended to be done by hand. However, as an algorithmic problem for "general number fields" it is difficult. It is known that this problem is equivalent (in "polynomial time") to the problem of finding the largest square factor of an integer m.

Remark 3. Although the latter problem might be easier than the more general problem of factoring integers, no one knows any way to find the largest square factor that is any easier than factoring.

Remark 4. It is easy to see that the problem of finding an "integral basis" is at least as hard as the problem of finding the largest square factor: If d is an arbitrary integer, the problem of finding an integral basis in $\mathbf{Q}(\sqrt{d})$ is essentially the same as the problem of finding the largest square factor of d. So the nontrivial direction is the other one: showing that *if* one can find solve the largest square factor efficiently (i.e., in polynomial time) then the integral basis can be found efficiently.

0.2 Power bases

One special case of some importance is when a "number ring" $\mathbf{Z}_F$ has a basis of the form

$$1, \alpha, \alpha^2, \cdots, \alpha^{n-1}.$$

Such bases are called "power bases," and, as we will see, are particularly easy to work with. In this case the discriminant of the field, i.e., the discriminant of the above basis, is just the discriminant of the polynomial m_α.

Whether or not an algebraic integer α generates a power basis, the span of the powers of α is denoted $\mathbf{Z}[\alpha]$, and this set is a subring of $\mathbf{Z}_F$. Subrings of the ring of integers are sometimes called **orders** in $\mathbf{Z}_F$.

Note that any quadratic field has a power bases. In a future homework assignment we will see that there are cubic fields with no power basis. The cyclotomic fields $\mathbf{Q}(\zeta_n)$, $\zeta_n := e^{2\pi i/n}$ are very important, and it is convenient that they have a power basis, and that in fact the ring of integers $\mathbf{Z}[\zeta_n]$. Unfortunately, it seems to be the case that large "random" number fields do not have power bases.

By our earlier work on fabs, we know that for any algebraic integer α we have

$$\operatorname{disc}(\mathrm{m}_\alpha) = \operatorname{disc}(1, \alpha, \cdots, \alpha^{n-1}) = [\mathbf{Z}_F : \mathbf{Z}[\alpha]]^2 \operatorname{disc}(\mathbf{Z}_F).$$

Thus we can compute the discriminant on the left explicitly as a polynomial discriminant. To find the discriminant of the field we have to allocate factors of the polynomial discriminant either to the square of the index or to the discriminant of the field.

One crucial special case is:

Theorem 5. If $\operatorname{disc}(\mathrm{m}_\alpha)$ is squarefree then $\mathbf{Z}_F = \mathbf{Z}[\alpha]$.

Perhaps later we will return to the problem of actually finding $\mathbf{Z}_F$.

0.3 Ideals

As hinted earlier, factorization of ideals in $\mathbf{Z}_F$ is unique. In fact, this is true in much more general circumstances.

Definition 6. A ring R (commutative, with identity) is a **Dedekind domain** if

- Every ideal is finitely generated (i.e., R is Noetherian).
- Every prime ideal is maximal (i.e., R is "one-dimensional").
- Every element of the fraction field F of R that satisfies a monic polynomial with coefficients in R lies in R (i.e., R is integrally closed in F, i.e., R is "smooth").

Since the important theorems about ideals can be proved for Dedekind domains, and number rings $\mathbf{Z}_F$ are Dedekind domains, we will find it convenient to work in that context (though there are one or two points where it is slightly more convenient to work in the special case $\mathbf{Z}_F$). To finish today, we show that number rings are in fact Dedekind domains.

Theorem 7. If F is a number field, then its ring of integers $\mathbf{Z}_F$ is a Dedekind domain.

Proof. An ideal I is contained in $\mathbf{Z}_F$ and is therefore a fab of finite rank, and is hence finitely generated. So $\mathbf{Z}_F$ satisfies the first condition for being a Dedekind domain.

If I is an ideal then it contains n linearly independent elements over $\mathbf{Q}$. (Take a basis of $\mathbf{Z}_F$ and multiply each element by a fixed nonzero element of I.) Thus I is a fab of rank n and the quotient $\mathbf{Z}_F/I$ is finite. If I is a prime ideal then $\mathbf{Z}_F$ is a finite integral domain.

Lemma 8. Any finite integral domain is a field.

Proof. (of lemma) The set of powers of a given nonzero element form a finite set, so $x^{m+n} = x^m$ for a nonnegative integer m and positive integer n. This implies that $x^m(x^n - 1) = 0$ and by the integral domain property we conclude that $x^n = 1$, i.e., that x is of finite multiplicative order and hence has an inverse. □

Thus if I is a prime ideal then $\mathbf{Z}_F/I$ is a field, which is to say that I is a maximal ideal. This proves the second condition for $\mathbf{Z}_F$ to be a Dedekind domain.

Finally, if an element x of F satisfies a monic polynomial with coefficients in $\mathbf{Z}_F$ then, as we saw earlier, x lies in a ring that is finitely generated over $\mathbf{Z}$ and x is an algebraic integer. I.e., $x \in \mathbf{Z}_F$. So $\mathbf{Z}_F$ is indeed integrally closed in its fraction field, as claimed. □