September 17:

Math 432 Class Lecture Notes

- Number Fields
- Examples
- Algebraic integers

0.1 Number Fields

The simplest field of characteristic 0 is of course the field $\mathbf{Q}$ of rational numbers. Perhaps the next object of study should be finite extensions of this field; in fact this turns out to be an extraordinarily fertile area of study, full of many open problems. The rest of the course will be concerned with such fields.

Definition 1. A **number field** is a finite extension of $\mathbf{Q}$.

A later exercise will show that every number field is generated by a single element, i.e., is a root field of an irreducible polynomial. If $F = \mathbf{Q}(\alpha)$ is a number field then the minimal polynomial $\mathrm{m}_\alpha(x)$ factors as a product of distinct linear factors in its splitting field. If one desires, one can take the roots to be complex roots, so that the splitting field, and the number field, lie inside the complex numbers. We then let

- r be the number of real roots of m_α, and
- s be the number of pairs of complex conjugate roots.

Thus

$$r + 2s = n := \deg(f).$$

The number of embeddings of F into $\mathbf{C}$ is clearly n, i.e., there is an embedding for each choice of root.

It is largely a matter of taste as to whether one thinks of number fields as lying explicitly inside the complex numbers, but there is no loss of generality in doing this, and we will do so when it is convenient.

0.2 Examples

The simplest number field is of course the field of rational numbers.

The fields

$$\mathbf{Q}(i), \quad \mathbf{Q}(\sqrt{-3}) = \mathbf{Q}(\omega), \quad \mathbf{Q}(\sqrt{5})$$

are all examples of quadratic number fields, and by earlier remarks we know that any such field is of the form $\mathbf{Q}(\sqrt{d})$ where d is a rational number that is not a perfect square.

A quadratic field $\mathbf{Q}(\sqrt{d})$ is said to be **real** if $d > 0$ and **imaginary** if $d < 0$. These correspond to $r = 2, s = 0$ and $r = 0, s = 1$ respectively. Any quadratic field is a galois extension, and we will denote the nontrivial automorphism, which takes $\sqrt{d}$ to $-\sqrt{d}$ by $x \mapsto x'$.

The fields

$$\mathbf{Q}(\sqrt[3]{2}), \quad \mathbf{Q}[x]/(x^3 + x^2 - 2x - 1$$

are "cubic" number fields of degree 3 over $\mathbf{Q}$. In this case $r = s = 1$ or $r = 3, s = 1$ according to whether a defining polynomial has 1 or 3 real roots. A cubic field might or might not be galois.

A "cyclotomic" field $\mathbf{Q}(e^{2\pi i/n})$ obtained by adjoining a primitive n-th root of unity. Cyclotomic fields turn out to be galois extensions, since $\mathbf{Q}(e^{2\pi i/n})$ is the splitting field of $x^n - 1$. Later we will learn that the "cyclotomic" polynomial

$$f_n(x) := \prod_{\gcd(k,n)=1} (x - e^{2\pi ik/n})$$

is irreducible and is therefore the minimal polynomial of $\zeta_n := e^{2\pi i/n}$. Thus the $[\mathbf{Q}(e^{2\pi i/n} : \mathbf{Q}] = \phi(n)$, where $\phi(n)$ is the Euler-phi function, i.e., the number of positive integers less than n that are relatively prime to n. By the

basic lifting result, this means that for every such integer k there is a unique automorphism σ_k such that

$$\sigma_k(\zeta_n) = \zeta_n^k.$$

From the obvious fact that $\sigma_k\sigma_l = \sigma_{kl}$ we see that the galois group $G(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ is isomorphic to the group multiplicative group $(\mathbf{Z}/n\mathbf{Z})^*$.

A deep theorem due to Kronecker and Weber asserts that any galois extension of $\mathbf{Q}$ whose galois group is abelian is contained in a cyclotomic extension; this is one of the important theorems of "class field theory."

0.3 Algebraic integers

To actually do algebraic number theory in a number field we need to go beyond field theory and have "integers" $\mathbf{Z}_F$ in a number field F, just as to do usual number theory one works in the integers $\mathbf{Z}$ inside $\mathbf{Q}$.

Definition 2. Let F be a number field. Define

$$\mathbf{Z}_F = \{\alpha \in F \ : \ \mathrm{m}_\alpha(x) \in \mathbf{Z}[x]\}.$$

We call $\mathbf{Z}_F$ the ring of **algebraic integers** in F.

One of our first tasks is to show that $\mathbf{Z}_F$ is in fact a ring, i.e., that the sum and product of algebraic integers are algebraic integers. It is convenient to first develop a useful criterion for integrality.

Theorem 3. Let F be a number field and $\alpha \in F$. Then the following are equivalent.

1. α is an algebraic integer, i.e., $\mathrm{m}_\alpha(x) \in \mathbf{Z}_F$.
2. The ring $\mathbf{Z}[\alpha]$ has a finitely generated additive group.
3. α is contained in a subring with a finitely generated additive group.
4. There exists a finitely generated additive group L inside F such that $\alpha L \subset L$.

Proof. If α is an algebraic integer then α^n can be expressed, using the minimal polynomial, as an integral linear combination of $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$. By a simple induction argument, all higher powers of α are in the span of those n elements, and the additive group of $\mathbf{Z}[\alpha$ is generated by those elements. This proves that (1) implies (2).

(2) $\Rightarrow$ (3) and (3) $\Rightarrow$ (4) are obvious. Suppose that L is a finitely generated group inside F with the property that $\alpha L \subset L$. Choose a basis (generating set) $\beta_1, \ldots, \beta_n$ for L. We have:

$$\alpha\beta_i = \sum_j a_{ij}\beta_j.$$

We can write this in matrix notation as

$$\alpha \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}.$$

Let $A = (a_{ij})$. It is now clear that α is an eigenvalue of this matrix, i.e. $\det(\alpha I - A) = 0$. This implies that the minimal polynomial for α divides the characteristic polynomial of A. Since the latter is a monic polynomial over $\mathbf{Z}$, Gauss' lemma implies that $\mathrm{m}_\alpha(x) \in \mathbf{Z}[x]$, and α is an algebraic integer. $\square$

Example 4. We determine the algebraic integers in an arbitrary quadratic field. Let $F = \mathbf{Q}(\sqrt{d})$, where we may assume that d is a squarefree integer. An arbitrary element of F can be written $z = a + b\sqrt{d}$. Its minimal polynomial is then

$$\mathrm{m}_z(x) = x^2 - 2ax + (a^2 - db^2).$$

The integrality of the linear term implies that a has the form $a = \frac{A}{2}$, where $A \in \mathbf{Z}$. The squarefreeness of d implies that b also has at worst a 2 in the denominator, i.e., $b = \frac{B}{2}$, for $B \in \mathbf{Z}$. In order for $a^2 - db^2$ to be an integer it follows that A and B have the same parity. We summarize these observations as follows.

Theorem 5. Let $d \in \mathbf{Z}$ be a squarefree integer, and $F = \mathbf{Q}(\sqrt{d})$. Then if $d \equiv 2, 3 \pmod 4$,

$$\mathbf{Z}_F = \mathbf{Z}[d].$$

If, on the other hand, $d \equiv 1, 4 \pmod 4$,

$$\mathbf{Z}_F = \mathbf{Z}[\frac{1+\sqrt{d}}{2}] = \{\frac{A + B\sqrt{d}}{2} : A \equiv B \bmod 2\}.$$