September 24:

Math 432 Class Lecture Notes

- Primes
- Pell's equation
- Embeddings
- Primitive Element Theorem
- Traces and Norms

0.1 Primes

Recall, that to find primes in $\mathbf{Z}[i]$ it suffices to factor (rational) prime numbers $p \in \mathbf{Z}$.

Indeed, if P is a prime in $\mathbf{Z}[i]$ then $N(P)$ is an integer. Since P is irreducible it must divide one of the primes that divides $N(P)$.

If the ring of integers $\mathbf{Z}_F$ is a PID the same story holds. If $\mathbf{Z}_F$ isn't a PID, then in turns out that the same story holds if we consider *ideals* P: Every ideal factors uniquely into a produce of prime ideals, and these ideals can be determined by factoring the ideals $(p) := p\mathbf{Z}_F$ generated by rational primes p.

0.2 Pell's equation

The existence of nontrivial solutions to Pell's equation $x^2 - dy^2 = \pm 1$ can be proved in several ways. One is to explicitly give an algorithm using continued fractions. Another is to apply a special case of a result that will be proved later in the course for arbitrary number fields. Another is to use an argument about approximation of algebraic numbers by rational numbers; specially one shows that for all irrational α and all positive integers n there are y, z such that

$$\left|\alpha - \frac{y}{z}\right| < \frac{1}{zn}.$$

This can be used to show that there are infinitely many approximations

$$|\alpha - (x/y)| < \frac{1}{yz},$$

which in turn implies that there exist x, y such that $|x^2 - dy^2| < 2\sqrt{d}$, which finally implies that there exist x, y such that $|x^2 - dy^2| = 1$.

It's not clear which of these arguments Neukirch had in mind in the exercise earlyl on in his text, or whether there is a different and better argument.

0.3 Embeddings

Our investigations into galois theory culminated in being able to count embeddings of separable field extensions into splitting fields. This did *not* require any of the results of galois theory that we didn't prove (e.g., the fundamental theorem of galois theory or its immediate precursors, such as the independence of characters).

We'll need the following result in several contexts.

Theorem 1. (Embedding Theorem) Let E be a separable extension of degree n of a field F. Let K be an extension of E that is the splitting field over F of a separable polynomial (with coefficients in F). Then there are n embeddings of E into K, i.e.,

$$|\mathrm{Hom}_F(E, K)| = n.$$

Remark 2. The theorem was proved by generalizing to a "relative" version that involved extending a given automorphism of ground fields, and then proving the generalized theorem with an easy proof by induction.

Remark 3. On several occasions we will number the embeddings $\sigma_1, \cdots, \sigma_n$; it is customary to let σ_1 be the identity map.

We will also be interested in the set $\mathrm{Hom}_{\mathbf{Q}}(F, \mathbf{C})$ of field embeddings of F into the complex numbers. We can, without loss of generality, assume that F is contained in the complex numbers, and that a splitting field K that contains it is also contained in the complex numbers. Then all of the $n = [F : \mathbf{Q}]$ embeddings given in the above theorem take their image in K.

An embedding of a number field F into $\mathbf{C}$ is said to be **real** (resp. **complex**) if its image is contained (resp., not contained) in the real numbers $\mathbf{R} \subset \mathbf{C}$. Complex embeddings come in pairs (if σ is an embedding so is its complex conjugate $x \mapsto \overline{\sigma(x)}$). So if r_1 is the number of real embeddings and r_2 is the number of complex conjugate pairs of embeddings then

$$r_1 + 2r_2 = n.$$

Example 4. Suppose $F = \mathbf{Q}(\alpha)$. (We will soon see that any number field is of this form.) Any embedding takes α to a root of $\mathrm{m}_{\alpha,\mathbf{Q}}$. Indeed, we apply σ to

$$0 = \mathrm{m}_{\alpha,\mathbf{Q}}(\alpha) = \alpha^n + a_1\alpha^{n-1} + \cdots, \qquad a_i \in \mathbf{Q}$$

we see that $\sigma(\alpha)$ is a root of the same polynomial. So r_1 is the number of real roots of m_α and r_2 is the number of pairs of complex conjugate roots. Therefore

- The field $F = \mathbf{Q}(\sqrt[3]{2})$ has $r_1 = 1$, $r_2 = 1$ since $x^3 - 2 = 0$ has one real root and a pair of complex conjugate roots.
- The polynomial

  $$(x - \cos 2\pi/7)(x - \cos 4\pi/7)(x - \cos 6\pi/7) = x^3 + \frac{1}{2}x^2 - \frac{1}{2}x - \frac{1}{8}$$

  has three real roots, so its root field has $r_1 = 3, r_2 = 0$.

0.4 Primitive Element Theorem

In several circumstances it can be useful to know that in any number field F there is an element α that generates the field, i.e., $F = \mathbf{Q}(\alpha)$. This turns out to be any easy application of the emedding theorem.

Theorem 5. Primitive Element Theorem. If E is a finite separable extension of a field F then there is an element α of E such that $E = F(\alpha)$.

Proof. If E is finite, then it suffices to take α to be a generator of the cyclic group E^*. So from now on we can assume that E is infinite.

By induction on the number of generators, it suffices to find a single generator for a field $E = F(\alpha, \beta)$. Let $n := [E : F]$, and let $\sigma_1, \cdots, \sigma_n$ be the embeddings of E into a normal extension K of F that contains E. For λ in F, let

$$g(x) := \prod_{i<j} \sigma_i(\alpha) + x\sigma_i(\beta) - \sigma_j(\alpha) - x\sigma_j(\beta).$$

Note that all factors are nonzero, since the embeddings are distinct, and are determined by what they do to α and β. In addition, the coefficients are all in F, since they are symmetric functions of the conjugates of α and β.

Thus the polynomial g is a nonzero polynomial with coefficients in F, and there is a $\lambda \in F$ such that $g(\lambda) \neq 0$. (Over a finite field it is in fact possible for a nonzero polynomial to have all of its values equal to 0.)

Let $\gamma = \alpha + \lambda\beta$. Then each $\sigma_i(\gamma)$ is a root of g, and they are all distinct, so the degree of $F(\gamma)$ over F is at least n. Since $F(\gamma)$ is contained in the field $F(\alpha, \beta)$ of degree n, it follows that the degree of γ is exactly n, and

$$F(\alpha, \beta) = F(\gamma)$$

which finishes the proof. □

0.5 Traces and Norms

If E/F is a finite extension of fields, then for every element $x \in E$ we get a "multiplication by x" mapping from E to E that is an endomorphism of an F-vector space of dimension $n := [E : F]$.

We define the norm and trace of the element x, from E down to F, to be the determinant and trace of this endomorphism; let mul_x denote the multiplication by x map, so that

$$N_{E/F}(x) := \det(mul_x), \qquad Tr_{E/F}(x) := Tr(mul_x).$$

We will run into the trace and norm again and again, and will need the following basic results (to be proved next time).

Theorem 6. Let x and y range over elements of F. Then:

- $N_{E/F}(x) \in F, \quad Tr_{E/F}(x) \in F$
- $N_{E/F}(xy) = N_{E/F}(x)N_{E/F}(y), \quad Tr_{E/F}(x+y) = Tr_{E/F}(x)Tr_{E/F}(y)$.
- $$N_{E/F}(x) = \prod_{\sigma} \sigma(x), \qquad Tr_{E/F}(x) = \sum_{\sigma} \sigma(x)$$

  where the sum and product range over all embeddings of E into a splitting field K of E over F.