ALGEBRAIC NUMBER THEORY

LECTURE 2 SUPPLEMENTARY NOTES

Material covered: Sections 1.4 through 1.7 of textbook.

For the proof of Theorem 1 of Section 1.5, a motivating example to keep in mind is that of a lattice in $\mathbb{Z}^n$. The proof using linear forms basically starts off with the observation that any lattice is cut out by linear congruences modulo some integers.

1. Section 1.7

If K is a field, its characteristic is the smallest positive integer n such that $1 + \cdots + 1$ (n terms) is 0, or if no such positive integer exists, we say the characteristic of K is zero. Now if K is a finite field, its characteristic must be finite and also a prime (because K is an integral domain). So K is a vector space over $\mathbb{F}_p$. So $|K| = p^e$ for some positive integer e. In fact, we will see that there is a unique finite field of size p^e.

First, notice that any finite field of characteristic p has a Frobenius automorphism $x \mapsto x^p$. This is injective on a finite set, hence surjective. For a field of size p^e, any nonzero element x satisfies $x^{p^e-1} = 1$. So for all x in the field, $x^{p^e} = x$. So the e'th power of the Frobenius map is trivial.

Take an algebraic closure K of $\mathbb{F}_p$. Now if L is any finite algebraic extension of degree e of $\mathbb{F}_p$, then every element of L is a root of $x^{p^e} - x$. But there are exactly $p^e = |L|$ solutions to this equation in the algebraic closure K. Hence L is unique.

On the homework, you will count irreducible polynomials of degree e over $\mathbb{F}_p$. Any such polynomial leads to the unique field of p^e elements.

An interesting exercise is to prove Wedderburn's theorem: any finite division algebra (i.e. satisfying the axioms of a field, except that multiplication is not assumed to be commutative) must be a field.

2. gp session

```
f = x^3 + 3*x + 1;
F = bnfinit(f);
F.disc

idealprimedec(F,3)
```

```
p = %[1]

i1 = idealhnf(F,3)
idealval(F,i1,p)

i2 = idealhnf(F,1+x)
idealnorm(F,i2)
bnfisprincipal(F,i2)
```

The above sequence of statements makes a number field K generated by an element with minimal polynomial $x^3 + 3x + 1$, which is irreducible over $\mathbb{Q}$. Then it computes the discriminant of this field. Then we compute the decomposition of the prime 3 into ideals of $\mathcal{O}_K$. We see that 3 is the third power of the prime ideal $(1 + x)$.

The next few statements compute the norm of the ideal (hnf means Hermite normal form: ignore this for now) $(1 + x)$ which must be 3, and checks that it is pricipal, which is true.

18.786 Topics in Algebraic Number Theory
Spring 2010