ALGEBRAIC NUMBER THEORY

LECTURE 1 SUPPLEMENTARY NOTES

Material covered: Sections 1.1 through 1.3 of textbook.

1. Section 1.1

Recall that to an integral domain $A$ we can associate its field of fractions $K = \text{Frac}(A) = \{ \frac{a}{b} : b \neq 0 \}$. More formally, $K = \{(a, b) : a, b \in A, b \neq 0\}/ \sim$, where $\sim$ is the equivalence relation $(a, b) \sim (c, d)$ iff $ad - bc = 0$ (i.e. “$\frac{a}{b} = \frac{c}{d}$”).

A general fractional ideal $\mathfrak{f}$ of $A$ is a subset of $K = \text{Frac}(A)$ such that

1. $af \in \mathfrak{f} \ \forall a \in A, f \in \mathfrak{f}$
2. $f_1 + f_2 \in \mathfrak{f} \ \forall f_1, f_2 \in \mathfrak{f}$
3. $\exists c \in A$ such that $cf$ is an ideal of $A$.

A non-example of a fractional ideal is the set $K$: it satisfies the first two properties but not the third one in general: the problem is that we have inverted “too many” elements.

Example. Some principal ideal domains (PIDs):

1. $\mathbb{Z}$ is a PID (any nonzero ideal is a subgroup, so is generated by a smallest positive element).
2. For a field $k$, the ring of univariate polynomials $k[X]$ is a PID (take a lowest degree element).

Some examples of non-PIDs:

Example. $(1)$ $\mathbb{Z}[\sqrt{-5}]$ is not a PID because of the failure of unique factorization $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. The ideal $(2, 1 + \sqrt{5})$ is not a principal ideal.

Proof. (of Thm 1.1.IV) Let $P$ be a set of representatives of the irreducible elements of $A$, modulo units (recall that this means $p \in A$ is a prime/irreducible if $p$ is not a unit and $p = xy$ implies $x$ or $y$ is a unit). Then given any $x \in K^*$ we want to show that $x$ can be uniquely written expressed as

$$x = u \prod_{p \in P} p^{v_p(x)}$$
First show existence of factorization. Uniqueness will follow from lemma III of Section 1.1. For existence, we can assume \( x \in A \) since we can write \( x = x_1/x_2 \) and express \( x_1, x_2 \in A \) in this form, and divide. So now assume \( x \in A \). Then \( xA \) is an ideal of \( A \). If it is the entire ring \( A \), then \( x \) is a unit and we are done. Else it is contained in a maximal ideal \( pA \) for some prime \( p \). Then \( p|x \) so write \( x = x_1p \). Again if \( x_1A = A \) we are done. Else find a prime dividing \( x_1 \) and so on. So this gives us a sequence of elements \( x = x_0, x_1, x_2, \ldots \) where \( x_{i+1} = x_i/p_i \) for some prime \( p_i \). Then the sequence of ideals \( a_i = x_iA \) is increasing. The set \( \bigcup a_i \) is an ideal of \( A \), hence it is generated by one element, say \( y \). Then \( y \) lies in some \( a_N \) and this means that the sequence must terminate at \( a_N \), i.e. \( x_n \) is a unit. So a finite factorization exists.

2. Section 1.2

Solving Pythagoras’ equation geometrically.

Write the equation as \( X^2 + Y^2 = 1 \), where \( X = x/z, Y = y/z \). It is sufficient to find all rational solutions of this equation. Now we know one point on this circle, for example \( P_0 = (-1, 0) \). For any other point with rational coordinates, it’s clear that the slope of the line joining it to \( P_0 \) must be rational (the converse is also not too hard to see). So write

\[
X = -1 + \frac{Y}{m}
\]

and plug into the equation to get

\[
\left(-1 + \frac{Y}{m}\right)^2 + Y^2 = 1
\]

which leads to the solution \( Y = 2m/(m^2 + 1), X = (1 - m^2)/(1 + m^2). \)

Section 1.3 is the Chinese remainder theorem for general rings.

3. GP/PARI example

Example. \( G = \text{bnfclassunit}(x^2+5) \)

This \( G \) contains lots of arithmetic information. For instance \( G[2, 1] = [0, 1] \) gives the number of real and complex embeddings of the number field. \( G[5, 1][1] \) is the class number of the field \( \mathbb{Q}(\sqrt{-5}) \) which is 2. \( G[5, 2] \) gives the structure of the class group in terms of its elementary divisors. Here it has to be \( \mathbb{Z}/2 \).
Finally, \( G[5, 1][3] \) gives the generators of the cyclic components. Here we get a matrix with columns \([2, 0]\) and \([1, 1]\) which means that the ideal is \( (2, 1 + \sqrt{5}) \).