ALGEBRAIC NUMBER THEORY

LECTURE 5 SUPPLEMENTARY NOTES

Material covered: Chapter 3 of textbook.

1. Section 3.3

If $A' \subset A$ and $\mathfrak{p}$ is a prime ideal of A, then $\mathfrak{p}' = \mathfrak{p} \cap A$ is a prime ideal of A', called the *restriction* of $\mathfrak{p}$ to A'.

Lemma 1. *Suppose $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ are ideals of A such that $\mathfrak{a}_1$ is relatively prime to the other two: $\mathfrak{a}_1 + \mathfrak{a}_i = A$ for $i = 2, 3$. Then $\mathfrak{a}_1$ is relatively prime to their product.*

Proof. We have $1 = a_1 + a_2$ and $1 = a_1' + a_3$ for some $a_1, a_1' \in \mathfrak{a}_1$, $a_2 \in \mathfrak{a}_2, a_3 \in \mathfrak{a}_3$. Multiplying we get

$$1 = (a_1 + a_2)(a_1' + a_3) = a_1 a_1' + a_1 a_3 + a_1' a_2 + a_2 a_3$$

The first three terms are in $\mathfrak{a}_1$ and the last is in $\mathfrak{a}_2 \mathfrak{a}_3$. □

2. Section 3.4

Proof of Theorem 2: We define $\mathfrak{m}' = \{x \in K \mid x\mathfrak{m} \subset A\}$. This is the *conductor* of $\mathfrak{m}$ into A. This is a natural candidate for the inverse of $\mathfrak{m}$: suppose that $\mathfrak{m}$ has an inverse fractional ideal $\mathfrak{n}$. Then for any $x \in \mathfrak{m}'$, we have $x\mathfrak{m} \subset A$, so multiplying by $\mathfrak{n}$ we get $xA = x\mathfrak{m}\mathfrak{n} \subset \mathfrak{n}$, which implies $x \in \mathfrak{n}$ since $1 \in A$. Conversely, by $\mathfrak{n}\mathfrak{m} = A$, we see that $\mathfrak{n}$ is contained in $\mathfrak{m}'$ by definition. So $\mathfrak{m}' = \mathfrak{n}$ if the inverse $\mathfrak{n}$ exists.

The intuition behind the last paragraph of the proof is as follows: we want an element of $K \backslash A$ which takes $\mathfrak{m}$ into A. We transfer this problem by multiplying by $(a)\mathfrak{m}^{-1}$ (which we haven't shown exists) to saying that we want an element which takes (a) into $(a)\mathfrak{m}^{-1}$, where $a \in \mathfrak{m}$ So if we could factor (a) into $\mathfrak{p}_1 \dots \mathfrak{p}_r$, with say $\mathfrak{p}_1 = \mathfrak{m}$ this would be saying that we want an element in $\mathfrak{p}_2 \dots \mathfrak{p}_r$ but not in (a), which is what b is (and b/a is the required element of $K \backslash A$ which takes (a) into $\mathfrak{p}_2 \dots \mathfrak{p}_r$). Since we don't have the factorization theorem into ideals yet, we settle for $(a) \supset \mathfrak{p}_1 \dots \mathfrak{p}_r$ with r minimal.

Remark. If $\mathfrak{p}$ and $\mathfrak{q}$ are two distinct maximal ideals of a Dedekind domain, then $\mathfrak{p} + \mathfrak{q} = A$ since $\mathfrak{p} + \mathfrak{q}$ contains $\mathfrak{p}$ which is maximal, and doesn't equal it (else $\mathfrak{q} \subset \mathfrak{p}$ contradincting maximality of $\mathfrak{q}$). So with the lemma above we have that if $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ are all distinct maximal ideals of the Dedekind domain A, then for any nonnegative integers e_i and f_j

$$\prod_i \mathfrak{p}_i^{e_i} + \prod_j \mathfrak{q}_j^{f_j} = A$$

This leads directly to the proof that $n_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \inf(n_{\mathfrak{p}}(\mathfrak{a}), n_{\mathfrak{p}}(\mathfrak{b}))$.

18.786 Topics in Algebraic Number Theory
Spring 2010