ALGEBRAIC NUMBER THEORY

LECTURE 10 NOTES

1. Section 5.1

Example (Rings of fractions). Let A be an integral domain.

(1) If $S = A\backslash\{0\}$, we get the entire field of fractions of A.
(2) If $S = \{1, x, x^2, \dots\}$, we get the localization $A_x = \{a/x^n : a \in A, n \geq 0\}$ of A in x. For instance, if $A = \mathbb{Z}$ and $x = p$ a prime, we get rational numbers whose denominators are powers of p. Note that in this particular case, we will not call the ring $\mathbb{Z}_p$, because of possible confusion with the p-adic integers, which is a completely different ring.
(3) If $S = A\backslash\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of A, we get the localization of A in $\mathfrak{p}$, $A_{\mathfrak{p}} = \{a/s : a \in A, s \notin \mathfrak{p}\}$. For instance, if $A = \mathbb{Z}, \mathfrak{p} = (p)$ then we get $S^{-1}A = \{a/b : p \not| b\} \subset \mathbb{Q}$.

Example (Primes in rings of fractions). The primes of $S^{-1}A$ are in bijective correspondence with primes of A not intersecting A. For example, if $A = \mathbb{Z}$ and $S = \{2^m 3^n : m, n \geq 0\}$, then (2) and (3) are not primes in $S^{-1}A$ any more, since they equal the unit ideal. But (p) is still a prime in $S^{-1}A$ for $p \neq 2, 3$.

Localization (the process of taking rings of fractions) commutes with taking quotients, in the following sense:

Proposition 1. *If $S \cap \mathfrak{a} = \phi$ then*

$$\frac{S^{-1}A}{\mathfrak{a}S^{-1}A} \cong \overline{S}^{-1}\left(\frac{A}{\mathfrak{a}}\right)$$

where $\overline{S}$ is the image of S in $A/\mathfrak{a}$.

Proof. Homework. □

Localization also commutes with completion in the following sense: recallt that if A is a Dekekind domain with fraction field K, and $\mathfrak{p}$a prime ideal of A, then $\mathfrak{p}$ defines a valuation of K by

$$|x|_p = c^{-v_{\mathfrak{p}}(x)}$$

where $c > 1$ is any real number, and $v_{\mathfrak{p}}(x)$ is the power of $\mathfrak{p}$ dividing the ideal (x) (different choices of c give equivalent valuations).

Then the valuation ring of K with respect to $|\ |_{\mathfrak{p}}$ is $A_{\mathfrak{p}}$, the localization of A in $\mathfrak{p}$. This is a DVR. The completion of K is $\widehat{K}$, say, and the valuation ring of $\widehat{K}$ is the completion $\widehat{A}$ of A with respect to $|\ |_{\mathfrak{p}}$, which is the same as the completion of $A_{\mathfrak{p}}$.

So we have $\widehat{A_{\mathfrak{p}}} \cong \widehat{A} \cong (\widehat{A})_{\mathfrak{p}\widehat{A}}$, the last isomorphism following from the fact that any element of $\widehat{A} \backslash \mathfrak{p}\widehat{A}$ is a unit, so localization doesn't affect anything.

Example. The completion of $\mathbb{Z}_{(p)} = \{a/b : p \not| b\}$ is just $\mathbb{Z}_p$, the p-adic integers, the completion of $\mathbb{Z}$ with respect to the p-adic valuation $|\ |_p$.

2. Section 5.2

The following proposition, which we will prove next time, is very useful for studying the decomposition of primes in number fields.

Proposition 2. *Let A be a Dedekind domain with fraction field K. Let L/K be a finite separable extension, and B the integral closure of A in L. Assume B is* monogenic *over A, i.e. $B = A[\alpha]$ for some $\alpha \in B$. Then let $f(X) \in A[X]$ be the minimal polynomial of α over K. Let $\mathfrak{p}$ be a prime of A and let $\overline{f}$ be the reduction of f mod $\mathfrak{p}$. If $\overline{f}$ factors as*

$$\overline{f}[X] = \overline{P}_1(X)^{e_1} \dots \overline{P}_r(X)^{e_r}$$

where $P_1, \dots, P_r \in (A/\mathfrak{p})[X]$ are irreducible and monic, then

$$\mathfrak{p}B = \mathfrak{B}_1^{e_1} \dots \mathfrak{B}_r^{e_r}$$

where $\mathfrak{B}_i = \mathfrak{p}B + P_i(\alpha)B$, the ramification index of $\mathfrak{B}_i$ is e_i, and the residue degree of $\mathfrak{B}_i$ is $f_i = \deg \overline{P}_i$.

Example. Let $K = \mathbb{Q}(\sqrt[3]{2})$. You showed on the homework that $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$. So $\mathcal{O}_K$ is monogenic over $\mathbb{Z}$, and we can use this to compute the decomposition of integer primes, using the above proposition with $\alpha = \sqrt[3]{2}$. The minimal polynomial of α is $X^3 - 2$. It's reduction mod 5 factors as

$$X^3 - 2 \equiv (X + 2)(X^2 - 2X - 1) \bmod 5$$

So the prime $5 = \mathfrak{p}_1\mathfrak{p}_2$ with $e(\mathfrak{p}_1) = 1, f(\mathfrak{p}_1) = 1, e(\mathfrak{p}_2) = 1, f(\mathfrak{p}_2) = 2$. Modulo 2 the polynomial reduces to X^3, so 2 factors as $\mathfrak{p}^3$, where $\mathfrak{p} = (\alpha)$.

Now most extensions of number fields L/K do not have a ring of integers that's monogenic. Nevertheless, it turns out that the localizations are monogenic at all but finitely many primes: if we choose $\alpha \in \mathcal{O}_L$ such that $K(\alpha) = L$, then $\mathbb{Z}[\alpha]_{\mathfrak{p}} = (\mathcal{O}_L)_{\mathfrak{p}}$ for all but finitely many primes $\mathfrak{p} \subset O_K$ (and we can say what this exceptional finite subset is) . This enables us to study prime decomposition rather effectively, since the prime decomposition above $\mathfrak{p}$ is not affected by localizing at $\mathfrak{p}$.

18.786 Topics in Algebraic Number Theory
Spring 2010