Math 154. Homework 7

1. A *discrete valuation ring* (dvr) is a Dedekind domain A with a unique maximal ideal. Any such A is a PID by the weak approximation theorem (HW5, Exercise 5(ii)).

(*i*) Via $\mathbf{Z}/7\mathbf{Z} \simeq \mathbf{Z}_{(7)}/7\mathbf{Z}_{(7)}$, find $n \in \mathbf{Z}$ so $n \bmod 7\mathbf{Z}$ goes to $2/3 \bmod 7\mathbf{Z}_{(7)}$. Express $n - 2/3$ as $7x$ with $x \in \mathbf{Z}_{(7)}$. For prime p, prove $\mathbf{Z}_{(p)}^\times$ consists of $q \in \mathbf{Q}^\times$ with numerator and denominator not divisible by p.

(*ii*) A *uniformizer* of a dvr A is a generator of the maximal ideal $\mathfrak{m}$. Show the uniformizers of $\mathbf{Z}_{(p)}$ are precisely pu for $u \in \mathbf{Z}_{(p)}^\times$. If π is a uniformizer of A, show every nonzero $a \in A$ has the unique form $u\pi^n$ with $n \geq 0$ and $u \in A^\times$, in which case $aA = \mathfrak{m}^n$. Conversely, if A is a domain with a nonzero nonunit π so that each $a \in A - \{0\}$ has the form $u\pi^n$ for some $u \in A^\times$ and $n \geq 0$ then show A is a dvr with maximal ideal πA.

(*iii*) If R is Dedekind and $\mathfrak{p}$ is a maximal ideal, say $r \in R - \{0\}$ is a *uniformizer at* $\mathfrak{p}$ if r is a uniformizer in $R_\mathfrak{p}$, and r is a *unit at* $\mathfrak{p}$ if $r \in R_\mathfrak{p}^\times$. Show r is a uniformizer (resp. unit) at $\mathfrak{p}$ if and only if rR has $\mathfrak{p}$ appear exactly once (resp. not appearing) in its prime factorization, and that a uniformizer at $\mathfrak{p}$ in R always exists. In $R = \mathbf{Z}[\sqrt{-5}]$ show 2 is not a uniformizer at the unique prime $\mathfrak{p}_2$ over 2 (i.e., $\mathfrak{p}_2 \cap \mathbf{Z} = 2\mathbf{Z}$) and find a uniformizer in R at $\mathfrak{p}_2$. Also show 3 is a uniformizer at both primes $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ over 3, and find another $r \in \mathbf{Z}[\sqrt{-5}]$ which is a uniformizer at one of them and a unit at the other.

2. We now use localization to generalize Exercise 5, HW3 to any Dedekind domain A, with fraction field F.

(*i*) A monic $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$ with nonzero constant term is *Eisenstein* at a maximal ideal $\mathfrak{m}$ if $a_i \in \mathfrak{m}$ for all i and $\mathfrak{m}$ appears exactly once in the prime factorization of (a_0). Show it is equivalent that f viewed in $A_\mathfrak{m}[X]$ is Eisenstein at $\mathfrak{m}A_\mathfrak{m}$, and deduce that such an f is irreducible over F.

(*ii*) For any $x \in F$, define its *ideal of denominators* to be $D_A(x) = \{a \in A \,|\, ax \in A\}$. Prove that this is a nonzero ideal of A, equal to (1) if and only if $x \in A$. Show that $D_A(x) \cdot S^{-1}A = D_{S^{-1}A}(x)$ for any multiplicative set $S \subseteq A - \{0\}$, and by taking $S = A - \mathfrak{m}$ for maximal ideals $\mathfrak{m}$ deduce that $\cap_\mathfrak{m} A_\mathfrak{m} = A$ inside of F (intersection over all $\mathfrak{m}$). As an application, prove Gauss' Lemma over A (if $f \in A[X]$ is monic then its monic irreducible factors over F all lie in $A[X]$) by using the known PID case over each $A_\mathfrak{m}$.

3. Let A be Dedekind, $F = \mathrm{Frac}(A)$, F'/F finite separable, $n = [F' : F]$, $A' \subseteq F'$ the integral closure of A.

(*i*) Assume A is a dvr with π a uniformizer. Suppose $\alpha \in A'$ is the root of a monic Eisenstein polynomial over A and $F' = F(\alpha)$. For $a_0, \dots, a_{n-1} \in A$, show that $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in \pi A'$ if and only if $a_i \in \pi A$ for all i. (Hint: if i is minimal such that $a_i \notin \pi A$, which is to say $a_i \in A^\times$, multiply through by α^{n-i-1} to deduce that $a_i\alpha^{n-1} \in \pi A'$. Now apply $\mathrm{N}_{F'/F}$ to get a contradiction, recalling that $\mathrm{N}_{F'/F}(A') \subseteq A$.)

(*ii*) Consider $\alpha \in A'$ such that $F' = F(\alpha)$ and the minimal polynomial f of α over F is Eisenstein at a maximal ideal $\mathfrak{m}$. Prove $A'_\mathfrak{m} = A_\mathfrak{m}[\alpha]$. (Hint: if $\pi \in A$ is a uniformizer at $\mathfrak{m}$, show $A'_\mathfrak{m} \cap (1/\pi)A_\mathfrak{m}[\alpha] = A_\mathfrak{m}[\alpha]$.)

(*iii*) By (*ii*), if $K = \mathbf{Q}(\alpha)$ with α the root of a p-Eisenstein polynomial $f \in \mathbf{Z}[X]$, the inclusion $\mathbf{Z}[\alpha] \subseteq \mathscr{O}_K$ becomes an equality after inverting $S = \mathbf{Z} - p\mathbf{Z}$. Prove $p \nmid [\mathscr{O}_K : \mathbf{Z}[\alpha]]$ (hint: if $L \subset L'$ is a finite-index inclusion of lattices, so it becomes an equality after localizing at $p\mathbf{Z}$ if and only if $p \nmid [L' : L]$), and deduce $K = \mathbf{Q}(2^{1/n})$ with $n \in \{3, 4, 5\}$ has $\mathscr{O}_K = \mathbf{Z}[2^{1/n}]$. (Hint: $2^{1/3} + 1$ and $2^{1/5} - 2$ respectively have 3-Eisenstein and 5-Eisenstein minimal polynomials over $\mathbf{Q}$. By the end of §2.7, $\mathrm{disc}(X^n + b) = (-1)^{n(n-1)/2} n^n b^{n-1}$.)

4. Let A be Dedekind such that $\mathrm{Cl}(A)$ is torsion; i.e., each maximal ideal has a power which is principal. (We'll later show $\mathrm{Cl}(\mathscr{O}_K)$ is even *finite* for number fields K.) Fix a finite set S of maximal ideals of A.

(*i*) The S*-integers* A_S is $\{0\} \cup \{x \in F^\times \,|\, Ax$ has no negative powers of $\mathfrak{m} \notin S$ in its prime factorization$\}$; for $A = \mathscr{O}_K$ we write $\mathscr{O}_{K,S}$. Prove $A_S = \cap_{\mathfrak{m} \notin S} A_\mathfrak{m}$ and $\mathscr{O}_{\mathbf{Q},\{2,3\}} = \mathbf{Z}[1/6] = \mathbf{Z}[1/72]$.

(*ii*) If $\mathfrak{m}_i^{h_i} = (a_i)$ for each $\mathfrak{m}_i \in S$ with $h_i > 0$, show $A_S = A[1/\prod a_i]$ inside F. For $A = \mathbf{Z}[\sqrt{-5}]$, write A_S as $\mathbf{Z}[\sqrt{-5}][1/a]$ for $S = \{\mathfrak{p}_2\}$, $\{\mathfrak{p}_3\}$, and $\{\mathfrak{p}_2, \mathfrak{p}_3\}$, where $(2) = \mathfrak{p}_2^2$ and $(3) = \mathfrak{p}_3\mathfrak{p}_3'$. (Hint: $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are not principal, but $\mathfrak{p}_2^2$ and $\mathfrak{p}_3^2$ are; norm calculations help to find a generator.) Make your choice of $\mathfrak{p}_3$ explicit.

(*iii*) Using (*ii*), prove the map $\mathrm{Cl}(A) \to \mathrm{Cl}(A_S)$ induced by $I \mapsto I \cdot A_S$ for fractional ideals I of A is surjective with kernel generated by $[\mathfrak{m}]$ for $\mathfrak{m} \in S$. Deduce that $\mathrm{Cl}(A_S)$ is finite if $\mathrm{Cl}(A)$ is finite.

(*iv*) For a_i as in (*ii*), show that the a_i's multiplicatively generate a free abelian group Γ with rank $\#S$ in $A_S^\times$, and that $A^\times \times \Gamma \to A_S^\times$ is injective with finite cokernel. In particular, if $A^\times$ is finitely generated (to be proved later for $A = \mathscr{O}_K$ for any number field K) prove that $A_S^\times$ is as well, with $\mathrm{rank}(A_S^\times) = \mathrm{rank}(A^\times) + \#S$. Compute $\mathscr{O}_{\mathbf{Q}(\sqrt{-5}),S}^\times$ for each of the three S's as in (*ii*).