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 $\mathbb{Z}/7\mathbb{Z} \cong \mathbb{Z}_7$, find $n \in \mathbb{Z}$ so $n \mod 7\mathbb{Z}$ goes to $2/3 \mod 7\mathbb{Z}$. Express $n - 2/3$ as $7x$ with $x \in \mathbb{Z}_7$. For prime $p$, prove $\mathbb{Z}_p^\times$ consists of $q \in \mathbb{Q}^\times$ 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 $\mathbb{Z}_p(p)$ are precisely $pu$ for $u \in \mathbb{Z}_p^\times$. If $p$ is a uniformizer of $A$, show every nonzero $a \in A$ has the unique form $w\pi^n$ with $n \geq 0$ and $u \in A^\times$, in which case $aA = m^n$. Conversely, if $A$ is a domain with a nonzero nonunit $\pi$ 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 $\pi A$.

(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 $r \in R_\mathfrak{p}^\times$. Now apply $N$ is injective with finite cokernel. In particular, 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 $R = \mathbb{Z}[\sqrt{-5}]$ show $2$ is not a uniformizer at the unique prime $p_2$ over $2$ (i.e., $p_2 \cap \mathbb{Z} = 2\mathbb{Z}$) and find a uniformizer in $R$ at $p_2$. Also show $3$ is a uniformizer at both primes $p_3$ and $p_5$ over $3$, and find another $r \in \mathbb{Z}[\sqrt{-5}]$ 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 $m$ appears exactly ones in the prime factorization of $(a_0)$. Show it is equivalent that $f$ viewed in $A_m[X]$ is Eisenstein at $mA_m$, and deduce that such an $f$ is irreducible over $F$.

(ii) For any $x \in F$, define its ideal of denominators to be $\mathcal{D}_A(x) = \{a \in A | ax \in A\}$. Prove that this is a nonzero ideal of $A$, equal to (1) if and only if $x \in A$. Show that $\mathcal{D}_A(1) = \mathcal{D}_A(\mathfrak{p})$ for any multiplicative set $S \subseteq A - \{0\}$, and by taking $S = A - \mathfrak{m}$ for maximal ideals $\mathfrak{m}$ deduce that $\cap mA_m = A$ inside of $F$ (intersection over all $m$). 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 $A_m$.

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

(i) Assume $A$ is a dvr with $\pi$ a uniformizer. Suppose $a \in A'$ is the root of a monic Eisenstein polynomial over $A$ and $F' = F(\alpha)$. For $a_0, \ldots, a_{n-1} \in A$, 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 $\alpha^{n-1}$ to deduce that $a_i\alpha^{n-1} \in \pi A'$. Now apply $N_{F'/F}$ to get a contradiction, recalling that $N_{F'/F}(A') \subseteq A$.)

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

(iii) By (ii), if $K = \mathbb{Q}(a)$ with $a$ the root of a $p$-Eisenstein polynomial $f \in \mathbb{Z}[X]$, the inclusion $\mathbb{Z}[a] \subseteq \mathcal{O}_K$ becomes an equality after inverting $S = \mathbb{Z} - p\mathbb{Z}$. Prove $p \nmid [\mathcal{O}_K : \mathbb{Z}[a]]$ (hint: if $L \subset L'$ is a finite-index inclusion of lattices, so it becomes an equality after localizing at $p\mathbb{Z}$ if and only if $p \nmid [L' : L]$, and deduce $K = \mathbb{Q}(\sqrt[2^n]{a})$ with $n \in \{3, 4, 5\}$ has $\mathcal{O}_K = \mathbb{Z}[\sqrt[2^n]{a}]$. (Hint: $21/3 + 1$ and $21/5 - 2$ respectively have 3-Eisenstein and 5-Eisenstein minimal polynomials over $\mathbb{Q}$.)

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

(i) The $S$-integers $A_S = \{0\} \cup \{x \in F^\times | Ax \text{ has no negative powers of } \mathfrak{m} \notin S \text{ in its prime factorization}\}$; for $A = \mathcal{O}_K$, we write $\mathcal{O}_{K,S}$. Prove $A_S = \cap_{\mathfrak{m} \notin S} A_\mathfrak{m}$ and $\mathcal{O}_{\mathbb{Q}(\sqrt{-5}), S} = \mathbb{Z}[1/6] = \mathbb{Z}[1/72]$.

(ii) If $m^h_i = (a_i)$ for each $m_i \in S$ with $h_i > 0$, show $A_S = A[1/\prod a_i]$ inside $F$. For $A = \mathbb{Z}[\sqrt{-5}]$, write $A_S$ as $\mathbb{Z}[\sqrt{-5}/1/a]$ for $S = \{p_2\}, \{p_3\}$, and $\{p_2, p_3\}$, where $(2) = p_2^2$ and $(3) = p_3p_3$. (Hint: $p_2$ and $p_3$ are not principal, but $p_2^2$ and $p_3^2$ are; norm calculations help to find a generator.) Make your choice of $p_2$ explicit.

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

(iv) For $a_i$ as in (ii), show that the $a_i$‘s multiplicatively generate a free abelian group $\Gamma$ 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 $A = \mathcal{O}_K$ for any number field $K$) prove that $A_S^\times$ is as well, with $\text{rank}(A_S^\times) = \text{rank}(A^\times) + \#S$. Compute $\mathcal{O}_{\mathbb{Q}(-\sqrt{5}), S}$ for each of the three $S$’s as in (ii).