18.786: Topics in Algebraic Number Theory (spring 2006)
Problem Set 2, due Thursday, March 2

Reminder: no class on February 21 or 23! That's why this set is on the long side.

1. Put $R = \mathbb{Z}[\sqrt{5}]$. Exhibit:
   (a) a failure of unique factorization of ideals in R;
   (b) a failure of a local ring of R to be a DVR.

2. These are not actually related; they were run together by mistake on the original version, and to preserve the numbering I have left them together here.
   (a) Let R be an integrally closed domain. Prove that $R[x]$ is also integrally closed.
   (b) Let R be a noetherian local domain with maximal ideal $\mathfrak{m}$. Prove that R is a DVR if and only if $\mathfrak{m}/\mathfrak{m}^2$, when viewed as a vector space over $R/\mathfrak{m}$, is one-dimensional. (The space $\mathfrak{m}/\mathfrak{m}^2$ is called the *cotangent space* of R, because that's what it is in the case where R is the local ring of a point on a smooth manifold.)

3. Determine the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[x]/(x^3 - 2)$ and in $\mathbb{Q}[x]/(x^3 - x - 4)$. (Remember: this means you have to first state the answer, then prove that nothing else in the field is integral!)

4. Let $P \in \mathbb{C}[x, y]$ be an irreducible polynomial such that P is nonsingular in the affine plane, that is, $P, \frac{\partial P}{\partial x}, \frac{\partial P}{\partial y}$ generate the unit ideal. Prove that $\mathbb{C}[x, y]/(P)$ is a Dedekind domain; among other things, this will reveal the origin of the term "uniformizer" as an abbreviation for "uniformizing parameter". (Hint: by the Nullstellensatz, the maximal ideals of $\mathbb{C}[x, y]$ correspond to points in $\mathbb{C}^2$, and the maximal ideals of $\mathbb{C}[x, y]/(P)$ correspond to points where P vanishes. Now use condition 2 from Theorem I.3.16.)

5. Demonstrate an example to show that in the previous problem, the nonsingularity condition cannot be omitted. (Hint: the simplest example is a *node*, where analytically two branches of the zero locus appear to cross.)

6. Prove the following converse of the unique factorization theorem: let R be an integral domain in which every nonzero ideal has a unique factorization into prime ideals. Prove that R is a Dedekind domain. (Hint: suppose that R has a maximal ideal $\mathfrak{m}$ of height greater than 1, and then construct a $\mathfrak{m}$-primary ideal which is not a power of $\mathfrak{m}$.)

7. Let R be a Dedekind domain, let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be nonzero prime ideals of R, and let S be the multiplicative subset $R - (\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n)$. Prove that R_S is a PID. (Hint: prove that R_S has only the "obvious" prime ideals.)

8. Exercise I.1 (page 13).

9. (a) Do Exercise I.4 (page 19).

(b) Prove that if S is the multiplicative set generated by a single element f, the kernel of the map $\mathbf{C}(R) \to \mathbf{C}(R_S)$ is generated by the classes of the prime ideals in the prime factorization of (f).

(c) Deduce that if $\mathbf{C}(R)$ is finite, then there exists a nonzero $f \in R$ such that R_f is a PID.

(c) Exhibit an explicit example where the map $\mathbf{C}(R) \to \mathbf{C}(R_S)$ fails to be injective.

10. Here is a variant of the concept of a PID which is sometimes useful. A *Bézout ring* is a ring in which every *finitely generated* ideal is principal. That is, a Bézout ring is like a PID except it may not be noetherian, e.g., the ring $\cup_{n=1}^{\infty} \mathbb{C}[\![x^{1/n}]\!]$ from lecture.

   (a) Prove that every finitely generated torsion-free module over a Bézout domain is free, by imitating the proof in the PID case. (Optional: generalize other results to the Bézout case, e.g., the fact that a finitely presented projective module over a Bézout domain is free.)

   (b) Let R be the integral closure of $\mathbb{Z}$ in $\mathbb{C}$. Prove that the localization of R at any maximal ideal is a Bézout ring which is not noetherian.

   (c) For $0 < r < 1$, let R_r be the ring of complex analytic functions on the annulus $r < |z| < 1$. Prove that $R = \cup_r R_r$ is a Bézout domain which is not noetherian. (Hint: recall that the zeroes of an analytic function have no accumulation point in the region of definition.)

   (d) Optional: prove that the ring R in (b) is itself a Bézout ring. For this, you may use results from Janusz that we have not yet covered in class, e.g., the fact that the integral closure of $\mathbb{Z}$ in a finite extension of $\mathbb{Q}$ is a Dedekind ring, or the finiteness of the class group of said ring.

11. Find out how to use SAGE built-in functions to compute the class group of the ring of integers in a quadratic number field. Then write a program to compute the sizes of the class groups of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-d})$ for $d \leq 1000$, and tell me what you notice. Pay particular attention to factors of 2. (Optional: repeat with some cubic number fields and pay attention to the factors of 3.)

12. (Not to be turned in) Read the proof of Theorem I.3.16, particularly any parts I skipped in class.

13. (Optional, not to be turned in) Read the beginning of Silverman's *The Arithmetic of Elliptic Curves* to find out why the class group of $\mathbb{C}[x,y]/(y^2 - x^3 - Ax - B)$, where $A, B \in \mathbb{C}$ are such that $x^3 - Ax - B$ has no repeated roots, is isomorphic to a complex torus (i.e., $\mathbb{C}$ modulo a lattice), and so in particular is infinite.