Math 661
Algebraic Number Theory
Problem Set 3

(1) In Problem (6) of the previous problem set you were asked to find an irreducible element of $\mathbb{Z}[\sqrt{-13}]$ that was not prime by copying the example of $\mathbb{Z}[\sqrt{-5}]$ in Baker's notes, i.e., by finding two different factorizations into irreducibles of some element of $\mathbb{Z}[\sqrt{-13}]$. Exactly as in Baker's notes (and as done in class), take the two different factorizations you came up with in $\mathbb{Z}[\sqrt{-13}]$, say $a = uv$ and $a = xy$, and write the ideals $\langle u\rangle$, $\langle v\rangle$, $\langle x\rangle$, $\langle y\rangle$, and $\langle a\rangle$ as products of prime ideals, and show that the two factorizations into prime ideal of $\langle a\rangle$ that you get are the same. (You need to prove that your ideals are prime and prove that your factorizations are correct.)

(2) This exercise and the next shows how things can go wrong in subrings of number fields that are not Dedekind domains! In $R = \mathbb{Z}[\sqrt{-3}]$, consider the ideal I generated by 2 and $1 + \sqrt{-3}$.
   (a) Show that $I^2 = (2)I$, yet $I \neq \langle 2\rangle$. Conclude that ideals of R do not factor uniquely into a product of prime ideals (and therefore R is not Dedekind).
   (b) Show that I is prime. (Hint: show it is maximal by showing that $R/I \cong \mathbb{F}_2$. One way to do this is to view R as $\mathbb{Z}[x]/(x^2+3)$ via the map that sends x to $\sqrt{-3}$. The ideal I corresponds then to the ideal generated by 2 and $1 + x$.)
   (c) Show that I is the unique prime ideal of R that contains $\langle 2\rangle$, and conclude that $\langle 2\rangle$ cannot be written as a product of primes (and therefore R is not Dedekind).

(3) Continuing with R and I of Problem 2 above, we will show that $I^{-1}I \neq R$—another way in which R fails to be a Dedekind domain!
   (a) Show that I^{-1} is the ring $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. (Hint: Check that $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}] \subseteq I^{-1}$. For the other direction, suppose that $x = \frac{a+b\sqrt{-3}}{c+d\sqrt{-3}} \in I^{-1}$ for suitable integers a, b, c, and d. Use the fact that $2x \in R$ to show that $x = \frac{p+q\sqrt{-3}}{2}$ for some integers p and q. Write $p = 2m + \mu$ and $q = 2n + \nu$ for suitable integers m and n, and $\mu, \nu \in \{0, 1\}$. Show that $(\mu, \nu) = (0, 0)$ or $(1, 1)$. Conclude that $x \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.
   (b) Show that $I^{-1}I = I$ (and therefore R is not Dedekind).

(4) Some computations in $\mathcal{O}_{\mathbb{Q}(\sqrt{-17})}$ to get a feel for concepts:
   (a) Show that the ideal generated by 2 and $\sqrt{-17}$ is the whole ring $\mathcal{O}_{\mathbb{Q}(\sqrt{-17})}$.
   (b) Show that the ideal $I = \langle 2, 1 + \sqrt{-17}\rangle$ is prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{-17})}$. (Hint: See the hint for Problem 2b above.)
   (c) Show that the ideal I is not principal.(Hint: Prove that 2 is irreducible.)
   (d) Determine the order of I in $\mathrm{Cl}(\mathbb{Q}(\sqrt{-17}))$. (Hint: It is a very small prime!)

(5) Let R be a PID. We will show here that R is Noetherian and a UFD.
   (a) Show that R is Noetherian. (Hint: Let $I_1 \subset I_2 \subset \ldots$ be an ascending chain of ideals. What can you say about $\cup_{j=1}^{\infty} I_j$?)
   (b) Show that every irreducible is prime. (Hint: Suppose x is irreducible, and suppose that $bc \in \langle x\rangle$. Suppose that $b \notin \langle x\rangle$. Note that $\langle x, b\rangle$ is

principal, so generated by some l. Thus, $x = lm$ for some m. If m is a unit, show we get a contradiction. Thus, l is a unit, so $\langle x, b\rangle = R$. Hence, $rx + sb = 1$ for some r and s. Multiply both sides by c.)

(c) Conclude that R is a UFD. (No need to write this down. I just want you to do the two parts above, since concluding that R is a UFD is standard, just like with the integers. First, since R is Noetherian, the existence of the factorization into irreducibles is guaranteed–recall we proved this in class. Next, for the uniqueness, if $a = x_1 \cdots x_n = y_1 \cdots y_m$ are two factorizations of a nonzero non unit a into irreducibles, then since we have shown that irreducibles are prime, we find from the fact that x_1 divides $y_1 \cdots y_m$ that x_1 must divide, and therefore be an associate of, one of the y_i, say y_1. Now cancel x_1 and its associate y_1 from both sides (replacing y_1 by some unit) and proceed.)

(6) We will show in this problem if R is a Dedekind domain that is a UFD, then it is a PID. (Since any PID is a UFD by Problem 5 above, we find that for a Dedekind domain, being a PID and a UFD are equivalent. This explains why it is natural to define the class group as the set of invertible ideals modded out by the principal ideals—it measures the deviation from the ring being a UFD.)

(a) Let P be any nonzero prime ideal of R. Show that if $a_1, \ldots, a_k$ are generators of P (note that R is Noetherian, so only finitely many elements are needed to generate P), then P may also be generated by $x_1, \ldots, x_k$ for some irreducible factors of $a_1, \ldots, a_k$ (respectively). (Hint: Work with a_1 first, and do induction on the number of irreducible factors of a_1. If a_1 itself is irreducible, then we have already "replaced" the generator a_1 by an irreducible factor! Else, write $a_1 = y_1 b_1$, where y_1 is irreducible. Since P is maximal—as R is Dedekind—the containment $P \subseteq \langle y_1, a_2, \ldots, a_k\rangle$ shows that either $P = \langle y_1, a_2, \ldots, a_k\rangle$, in which case we have replaced a_1 by the irreducible y_1, or else, $\langle y_1, a_2, \ldots, a_k\rangle = 1$. Write $r_1 y_1 + r_2 a_2 + \ldots r_k a_k = 1$, multiply by b_1, and show that $P = \langle b_1, a_2, \ldots, a_k\rangle$. Note that b_1 has fewer irreducible factors than a_1. Alternatively, and more simply, you could say that if a_i is a product of irreducibles $x_{i,j}$, then at least one $x_{i,j}$, say $x_{i,j*}$, should be in P since P is prime. Now show that P must be generated by these $x_{i,j*}$, one for each i.)

(b) Prove that in a UFD, irreducible elements are prime, and generate a prime ideal.

(c) Now prove that every prime ideal of R is principal and is generated by an irreducible element. (Hint: Use the previous two parts along with the fact that in a Dedekind domain, all nonzero prime ideals are maximal.)

(d) Now show that every ideal of R is principal. (Hint: Use the factorization of ideals of R.)

(7) (This exercise and the next help give a characterization of the radical of an ideal, a crucial concept in commutative ring theory. The result of this exercise is needed for this characterization but is also of independent interest.) Let S be a multiplicatively closed set in a (commutative) ring R. Let

I be an ideal maximal with respect to the property that $I \cap S = \emptyset$. Show that I is a prime ideal. (Hint: Suppose $ab \in I$, but $a \notin I$ and $b \notin I$. What can you say about the ideals $\langle I, a\rangle$, $\langle I, b\rangle$, as well as their product?)

(8) Let I be an ideal of a (commutative) ring R. The *radical* of I, denoted $\sqrt{I}$ or $\mathrm{Rad}(I)$, is the set $\{r \in R \mid r^n \in I \text{ for some } n \geq 0\}$. Prove that $\sqrt{I}$ equals $\bigcap_{\substack{\text{prime ideals} \\ P \supseteq I}} P$. (Hint: One direction—left side contained in right side—should be obvious. As for the other direction, take r in the right side, and suppose $r \notin \sqrt{I}$. Then I is disjoint from the multiplicatively closed set consisting of the nonnegative powers of r. Use Problem 7 above along with Zorn's lemma.)