october 24:

Math 432 Class Lecture Notes

- Ideals in a Dedekind domain
- Chinese Remainder Theorem
- An application

0.1 Ideals in a Dedekind domain

We reviewed and finished the proof that ideals in a Dedekind domain factor uniquely intro prime ideals (described in the notes for 10/12). The main steps were

1. Showing that every ideal I in a Dedekind domain R is invertible, i.e., that there is an ideal J such that IJ is principal.
2. Using this to show that if $I \subset J$ is equivalent to $J|I$ (the latter meaning that there is an ideal K such that $IK = J$.
3. Showing that Cancellation holds for ideal multiplication, i.e., that $IJ = IK$ implies that $J = K$.
4. Showing that every ideal factors uniquely into a product of ideals.

If two ideals I and J have factorizations

$$I = \prod_{i=1}^{r} P_i^{a_i}, \qquad J = \prod_{i=1}^{r} P_i^{b_i}$$

then their greatest common divisor is

$$\gcd(I, J) := \prod_i P_i^{\min(a_i, b_i)}.$$

By the divisibility/inclusion result, this means that $\gcd(I, J)$ is the smallest ideal containing I and J, i.e., that

$$\gcd(I, J) = I + J.$$

Similarly, the least common multiple of I and J is

$$\mathrm{lcm}(I, J) := \prod_i P_i^{\max(a_i, b_i)}$$

and this turns out to be the largest ideal contained in both I and J, i.e.,

$$\mathrm{lcm}(I, J) = I \cap J.$$

The reverse relationship between inclusion and divisibility takes a little bit of time to become comfortable with, but a moment's thought shows that it is consistent with our experience in, e.g., the ring of integers $\mathbf{Z}$.

0.2 Chinese Remainder Theorem

For this section, we let the ring R be any ring (commutative, with identity).

Lemma 1. If $I + J = (1) = R$ then $IJ = I \bigcap J$.

Proof. Clearly, if $x \in IJ$, then $x \in I \bigcap J$, so $IJ \subset I \bigcap J$. Suppose $u \in I \bigcap J$. There exist elements i and j of I and J, respectively, such that $i + j = 1$. Then $u = u(i + j) = ui + uj \in IJ$. □

The Chinese Remainder Theorem says that a ring element can be specified by giving its congruence class modulo each ideal in a collection of pairwise relatively prime ideals, and this element is unique modulo the product (intersection) of the ideals.

Example 2. If you are give constants a, b, c and told that $x \equiv a \bmod 7$, $x \equiv b \bmod 11$, $x \equiv c \bmod 13$ then x is uniquely determined modulo 1001. This has been used as a basis for a magic trick.

Theorem 3. (Chinese Remainder Theorem) If $I_1, I_2, \cdots, I_n$ are pairwise relatively prime ideals (i.e., $I_i + I_j = R$, for $i \neq j$) then

$$R/\bigcap I_i \simeq R/\prod I_i \simeq \bigoplus R/I_i.$$

Proof. Consider the case $n = 2$. Let ϕ_1 and ϕ_2 be the natural maps from R to R/I_1 and from R to R/I_2, respectively, and define $\phi : R \longrightarrow R/I_1 \bigoplus R/I_2$ by $\phi(x) = (\phi_1(x), \phi_2(x))$. It is clear that $\ker(\phi) = I_1 \cap I_2$, so that all that has to be done is to show that ϕ is surjective.

Let $y = (y_1 \bmod I_1, y_2 \bmod I_2)$ be an element of $R/I_1 \bigoplus R/I_2$. Then since $I_1+I_2 = 1$, there are $i_1 \in I_1, i_2 \in I_2$ such that $i_1+i_2 = 1$. Let $sx = y_2i_1+y_1i_2$. A simple calculation shows that $x \equiv y_1 \bmod I_1$ and $x \equiv y_1 \bmod I_1$, so ϕ is surjective.

The case of arbitrary n can be proved by an induction argument based on the $n = 2$ case, or by generalizing the proof in that case in a straightforward way □

0.3 An application

As an example application of this result, we will prove the following useful result that says that ideals in a number ring can be generated by two elements, and one of them can even be specified arbitrarily.

Theorem 4. Let $R = \mathbf{Z}_F$ be the ring of integers of a number field F. If I is an ideal and α is a nonzero element of I, then there is a β such that $I = (\alpha, \beta)$.

Proof. Let $I = \prod_i P_i^{a_i}$ be the prime factorization of I. Then the principal ideal (α) can be factored in the form

$$(\alpha) = J \prod_i P_i^{b_i}$$

where $b_i \geq a_i$, and the prime ideals dividing J are disjoint from the P_i. Choose $\beta_i \in P_i^{a_i} - P_i^{a_i+1}$. (The ideals P^a and P^{a+1} are distinct, by unique factorization, so such elements exist.) Now use the Chinese Remainder Theorem to find a β such that

$$\text{for each } i, \beta \equiv \beta_i \bmod P_i^{a_i+1}$$

and $\beta \equiv 1 \bmod J$. Then the ideal (β) has a factorization of the form

$$(\beta) = K \prod_i P_i^{a_i}$$

where K is relatively prime to J. It follows that

$$(\alpha, \beta) = (\alpha) + (\beta) = \gcd(\alpha, \beta) = \prod_i P_i^{a_i} = I$$

as desired. □