All Ideals in Dedekind Domains can be generated by two generators
presented with CRT for Rings

The goal of this note is to prove that any ideal in a Dedekind domain can be generaged by two generators. In fact, the first generator can be chosen by random as long as it is nonzero. Some basic notation of product rings are presented along with a proof of the CRT. Then, we prove the theorem in question.

Assume all rings to be commutative.

Proposition Cartesian product of rings are also rings

Let R, S be rings. From the cartesian product $R \times S$, define addition and multiplication as follows:

$$(r, s) \cdot (\bar{r}, \bar{s}) = (r\bar{r}, s\bar{s})$$

$$(r, s) + (\bar{r}, \bar{s}) = (r + \bar{r}, s + \bar{s})$$

The following binary operations along with the set $R \times S$ forms a ring.

Proof It is trivial to show closure under subtraction and multiplication. Write:

$$(r, s) - (\bar{r}, \bar{s}) = (r - \bar{r}, s - \bar{s}) \in R \times S$$

The line of algebra is justified by the fact that R, S are rings. Similarly, the set is closed under multiplicaiton. Associativity and distributivity follows from the ringness of R, S. □

Theorem Chinese Remainder Theorem for Rings

Let I, J be ideals of a ring R. Suppose $I + J = R$. The following sets are isomorphic:

$$R/I \cup J \cong R/I \times R/J$$

Proof Define a ring homeomorphism:

$$\varphi : R \to R/I \times R/J$$

It suffices to show that φ is surjective along with:

$$\ker(\varphi) = I \cup J$$

Then, the isomorphism can be proved by the first isomorphsm theorem for rings.

Define:

$$\varphi(a) = (a + I, a + J)$$

Take any two cosets $x + I, y + J$. By the condition $R = X + Y$, it is possible to rewrite elements x, y as:

$$x = x_i + x_j \quad \text{and} \quad y = y_i + y_j$$

where $x_i, y_i \in I$ and $x_j, y_j \in J$. It is possible to construct an element in R that maps into the two randomly selected cosets. Namely:

$$\varphi(x_j + y_i) = (x_j + y_i + I, x_j + y_i + J) = (x_j + I, y_i + J)$$
$$= (x_i + x_j + I, y_i + y_j + J) = (x + I, y + J)$$

This shows surjectivity. Move on to prove that the kernel of φ is $I \cup J$. $\varphi(a) = (I, J)$ implies $a \in I, a \in J$ so $a \in I \cap J$. Also, choose arbitrary $b \in I \cap J$. $\varphi(b) = (I, J)$. This shows that $\ker(\varphi) = I \cap J$. □

Remark The result can be generalized to multiple ideals. That is, for ideals I_i that satisfy:

$$\sum_{i=1}^{n} I_i = R$$

$$R/(\bigcap_{i=1}^{n} I_i) \cong R/I_1 \times R/I_2 \cdots \times R/I_n$$

A simple proof can be written by induction, and is left for the reader as an exercise.

Now we are ready to present the main theorem and proof.

Theorem Any ideal in a Dedekind domain can be generated by two geneators. In fact, the first generator can be any nonzero element in the ring.

Proof Let D be the Dedekind domain and I be an ideal in D. If the ideal I is principal, the theorem holds. Choose any nonzero element $\alpha \in I$.

The principal ideal generated by α is in the ideal I. Inclusion of an ideal implies that the large ideal divides the small ideal. In symbols:

$$\langle \alpha \rangle \subsetneq I \implies I | \langle \alpha \rangle$$

We know that ideals uniquely factor into prime ideals. In light of the divisibility relation above, we write the prime factorization of I and $\langle \alpha \rangle$:

$$I = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_t^{e_t}$$
$$\langle \alpha \rangle = \mathfrak{p}_1^{f_1} \mathfrak{p}_2^{f_2} \cdots \mathfrak{p}_t^{f_t} Q_1 Q_2 \cdots Q_l$$

Where the the indicies e, f satisfy $e_i \leq f_i$ for any $1 \leq i \leq t$. Q_i are ideals that are not in the family of ideals $\{\mathfrak{p}_1 \ldots \mathfrak{p}_n\}$ but are not necessarily distinct.

We construct a β that satisfies:

$$\mathfrak{p}_i^{e_i} || I \qquad \text{for any} \quad 1 \leq i \leq t$$

$$Q_i \nmid I \qquad \text{for any} \quad 1 \leq i \leq l$$

As long as I is not principle, there must exist an ideal Q_i. Otherwise, if $\langle\alpha\rangle$ was in the form of:

$$\langle\alpha\rangle = \mathfrak{p}_1^{f_1}\mathfrak{p}_2^{f_2}\cdots\mathfrak{p}_t^{f_t}$$

Then $\langle\alpha\rangle = I$, and otherwise the principal ideal will be greater than the original ideal, which is a contradiction.

We recognize:

$$\mathfrak{p}_1^{e_1} + \cdots + \mathfrak{p}_t^{e_t} + Q_1 + \cdots + Q_l = D$$

This is because the ideal Q_1 is distinct from $\mathfrak{p}_1^{e_1}$, and the gcd of the ideal is the whole ring. By the Chinese Remainder Theorem for Rings, it is possible to construct an isomorphism between:

$$R/(\mathfrak{p}_1^{e_1} \cap \cdots \cap \mathfrak{p}_t^{e_t} \cap Q_1 \cap \cdots \cap Q_l) \cong R/\mathfrak{p}_1^{e_1} \times \cdots \times R/\mathfrak{p}_t^{e_t} \times R/Q_1 \cap \times \cap R/Q_l$$

Also, we know exactly what the isomorphism is. We choose a series of elements β_i from the set $\mathfrak{p}_i^{e_i} \setminus \mathfrak{p}^{e_1+1}$. Consider an element is the right product ring:

$$(\beta_1 + \mathfrak{p}_1^{e_1}, \ldots, \beta_t + \mathfrak{p}_t^{e_t}, 1 + Q_1, \ldots, 1 + Q_l)$$

As a consequence of CRT, it is possible to draw a single element β such that:

$$\beta + \mathfrak{p}_i^{e_i} = \beta_i + \mathfrak{p}_i^{e_i} \qquad \text{for any} \quad 1 \le i \le t \quad \text{and}$$
$$\beta + Q_j = 1 + Q_j \qquad \text{for any} \quad 1 \le j \le l$$

We deduce $\beta - \beta_i \in \mathfrak{p}_i^{e_i}$ and $\beta - 1 \in Q_j$. The first statemeint implies $\beta \in \mathfrak{p}_1^{e_1}$. If $\beta \in \mathfrak{p}_i^{e_i+1}$, we reach $\beta_i \in \mathfrak{p}_i^{e_i+1}$, a contradiction. Likewise, $\beta \in Q_j$ implies $1 \in Q_j$ which contradicts the fact that Q_j is proper.

From $\beta \in \mathfrak{p}_i^{e_i}$, we deduce $\langle\beta\rangle \subseteq \mathfrak{p}_i^{e_i}$ which implies $\mathfrak{p}_i^{e_i} | \langle\beta\rangle$. The prime ideal $\mathfrak{p}_i$ divides $\langle\beta\rangle$ exactly e_i times. Otherwise, $\mathfrak{p}_i^{e_i+1} | \langle\beta\rangle$ and β will be in the ideal $\mathfrak{p}_i^{e_i+1}$ which we have shown not to be true. Also, $Q_j \nmid \langle\beta\rangle$ by a similar argument.

Thus:

$$\langle\alpha,\beta\rangle = \langle\alpha\rangle + \langle\beta\rangle = \gcd(\langle\alpha\rangle, \langle\beta\rangle)$$
$$= \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_t^{e_t} = I$$

□