Primality and Factoring in PIDs

We already know that ideals in a principal ideal domain are principal. This is like the ring of integers. In fact, we can generalise the fundamental theorem of arithmetic that factorises a number as a product of primes to a PID as well.

In this section we will only deal with commutative rings.

Irreducible and Prime elements in a ring

Recall that a unit in R is an element u for which there is an element v so that $u \cdot v = v \cdot u = 1$.

We say that a non-unit element p of R is *irreducible* if whenever we write $p = a \cdot b$ with a and b in R, either a or b is a unit.

Exercise: Note that the only irreducible elements in the ring of integers are of the form $\pm p$ where p is a prime number.

Exercise: Note that the elements of the form $T - a$ in the ring $\mathbb{Q}[T]$ are irreducible. (This is true with *any* field.)

Exercise: If p is an irreducible element of R and p lies in the ideal $q \cdot R$, then show that either q is a unit (so that $q \cdot R = R$) or $q = p \cdot u$ where u is a unit.

A *proper* ideal P in a ring R is said to be a *prime* ideal if the following property holds: whenever $a \cdot b$ lies in P (for a and b in R), either a or b lies in P.

Exercise: Check that P is a prime ideal if and only if R/P is a domain.

In particular, if R is a domain, then $\{0\}$ is a prime ideal!

In continuation of the terminology with integers, we say that a non-zero element p in R is a *prime* if the ideal generated by it is a prime ideal.

If p is a prime in a domain R (our convention is that domains are commutative) and $p = a \cdot b$, then $a \cdot b$ lies in $p \cdot R$. So, by primality of $p \cdot R$, we must have a or b in it. Suppose a is in $p \cdot R$, then $a = p \cdot c$. This means that $p = p \cdot c \cdot b$. Since we are in a domain and p is non-zero this means $1 = c \cdot b$. Hence b is a unit. Similarly, if b is in $p \cdot R$, then we can show that a is a unit. Thus, we have shown that p is irreducible.

In summary, a prime element of a domain is also irreducible.

Let R denote the ring consisting of matrices of the form $\begin{pmatrix} a & b \\ 5b & a \end{pmatrix}$ where a and b are integers. We can identify R as the subring of the field $\mathbb{C}$ of complex numbers that consists of elements of the form $a + b\sqrt{-5}$ where a and b are integers.

Exercise: Check that $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$. Show that 2 does not divide $1 + \sqrt{-5}$ or $1 - \sqrt{-5}$ in the ring R.

Exercise: Check that $1 + \sqrt{-5} = \alpha \cdot \beta$ with α and β in R is only possible if either α or β is ± 1.

Exercise: Conclude that $1 + \sqrt{-5}$ is irreducible but not prime.

However, as we shall see below, every irreducible element in a PID is prime.

Irreducible elements in a PID

Suppose that $a \cdot b = c \cdot d$ is an identity between four elements in R. Further, suppose that $a \cdot R + c \cdot R = R$. Then we have an identity $1 = a \cdot x + c \cdot y$. Multiplying both sides by b, we get

$$b = b \cdot a \cdot x + b \cdot c \cdot y = c \cdot d \cdot x + c \cdot b \cdot y = c \cdot (d \cdot x + b \cdot y)$$

So b is a multiple of c.

Now suppose that c is an irreducible element of a PID R and suppose $a \cdot b$ lies in $c \cdot R$. We wish to show that either a or b lies in $c \cdot R$.

We have an identity $a \cdot b = c \cdot d$ as above. The ideal $a \cdot R + c \cdot R$ is principal and hence there is an element p in R so that $a \cdot R + c \cdot R = p \cdot R$.

So c (which is irreducible) lies in $a \cdot R + c \cdot R = p \cdot R$. As seen above this means that either p is a unit or $p = c \cdot u$ for a unit u in R. In the second case, a lies in $c \cdot R = p \cdot R$.

If p is a unit, then $p \cdot R = R$ and thus $a \cdot R + c \cdot R = R$. We can apply the above calculation to show that c divides b; in other words, b lies in $c \cdot R$.

So irreducible elements of a PID are prime. Hence, primes and irreducible elements in a PID are the same.

Maximal ideals in a PID

A *proper* ideal P in a ring R is said to be *maximal* if it there are no ideals between it and R.

If a is an element of R that does not lie in a maximal ideal P, then $a \cdot R + P$ is a larger ideal than P. Hence, by maximality of P, we must have $a \cdot R + P = R$. It follows that there is an element b of R and an element p in P so that $a \cdot b + p = 1$. Hence, a is a unit in R/P.

Exercise: Use the above reasoning to conclude that, if P is a maximal ideal then R/P is a field.

Exercise: Conversely, if I is an ideal in a commutative ring R and R/I is a field, then show that I is a maximal ideal.

In particular, R/P is a domain and thus P is a prime ideal.

Exercise: Given a maximal ideal P, try to prove directly that if $a \cdot b$ lies in P and a does not lie in P then b lies in P.

By the Noetherian property of a PID, any increasing chain of ideals in a PID R must stop. This means that any proper ideal in R must be contained in a maximal ideal. (Using the Axiom of Choice, it is possible to prove this for all rings, even those without the Noetherian property.)

Note that a maximal ideal P in a PID is of the form $p \cdot R$ and since P is a proper ideal p is not a unit. If $p = 0$ then P is the 0 ideal and so R is a field. Thus, if R is a PID which is not a field, then a maximal ideal P in R is of the form $p \cdot R$ where p is a prime in R.

Given any non-unit non-zero element a in a PID R, the ideal $a \cdot R$ is a proper ideal in R and hence it must be contained in a maximal ideal P which we have seen is of the form $p \cdot R$. In other words, a is a multiple of the prime p.

Exercise: If a prime q is a multiple of a prime p in a domain R then show that $q = p \cdot u$ where u is a unit. (Hint: Look at the proof that primes are irreducible.)

Exercise: If a is an element of a PID R which is not a multiple of a prime p, then show that $a \cdot R + p \cdot R = R$. (Hint: a gives a non-zero element of R/p which is a field.)

We conclude that, in a PID which is not a field, primes generate maximal ideals and every maximal ideal generated by a prime.

Prime power extraction

Given a non-zero element a in a domain R which can be written as $a = u \cdot b$. Further suppose that $b = v \cdot a$. Then we have $a = u \cdot v \cdot a$. Since R is a domain, this gives $1 = u \cdot v$. In other words, u is a unit; in particular, it is *not* a prime.

So, if $a = p \cdot b$ where p is a prime in R, then b is *not* in $a \cdot R$. Put differently $a \cdot R$ is a *proper* subset of $b \cdot R$.

Given a non-zero element a in a PID R and a prime p in R, either a is a multiple of p or not.

If a is a multiple of p then we put $a_0 = a$ and write $a_0 = p \cdot a_1$. If a_1 is not a multiple of p then we stop, else we write $a_1 = p \cdot a_2$. Continuing this way, we write $a_k = p \cdot a_{k+1}$ or a_k is not a muliple of p.

As seen above, we get a strictly increasing chain of ideals $a_k \cdot R$. On the other hand, by the Noetherian property of R, this cannot happen. Hence, there is a k for which a_k is not a multiple of p.

In other words, we have shown that for every non-zero a in R and prime p in R, there is a non-negative integer k so that $a = p^k \cdot b$ where b is not a multiple of p.

Factorisation

Given a non-zero element a in a PID R and p a prime in R. Suppose $a = p^k \cdot b$ for some $k \geq 1$. As seen above this means that $a \cdot R$ is a *proper* subset of $b \cdot R$.

On the other hand, we have also seen that if a is a non-unit in R, then $a \cdot R$ is contained in a maximal ideal and a maximal ideal is of the form $p \cdot R$ for some prime p. Thus, extracting the largest power of p from a and writing $a = p^k \cdot b$, we must have $k \geq 1$.

We put $a_0 = a$, $p_1 = p$, $k_1 = k$ and $a_1 = b$. We have $a_0 = p_1^{k_1} \cdot a_1$ with $k_1 \geq 1$, a_1 is not a multiple of p_1 and $a_0 \cdot R$ a proper subset of $a_1 \cdot R$.

If a_1 is not a unit, then we can repeat the process and find p_2, k_2 and a_2 so that $a_1 = p_2^{k_2} \cdot a_2$ with $k_2 \geq 1$, a_2 is not a multiple of p_2 (or of p_1) and $a_1 \cdot R$ a proper subset of $a_2 \cdot R$.

We can repeat this process with a_2 as long as a_2 is not a unit and so on.

By the Notherian property of the PID R, we cannot have an infinite strictly increasing chain of ideals. Hence, at some stage we must have a_n is a unit.

It follows that $a = u \cdot p_1^{k_1} \cdots p_n^{k_n}$ is a factorisation of a into prime powers upto a unit.

Due to the presence of a unit, we do not have the familiar unique-ness of this factorisation as in the case of integers. However, if q is a prime which divides a then q divides the right-hand side. By the definition of primality, it must divide one of the p_i (since something which divides a unit must be a unit!). As seen above these means that it is a unit multiple of that p_i. By repeated application of this we can show that if there are distinct primes q_i and a unit v so that

$$vq_1^{r_1} \cdots q_m^{r_m} = a = u \cdot p_1^{k_1} \cdots p_n^{k_n}$$

then $n = m$, and for each i between 1 and n, there is a unique $s(i)$ so that q_i is a unit multiple of $p_{s(i)}$ and $r_i = k_{s(i)}$.