Divisibility

Definition 1. *Let R be a commutative, unital ring, with $a, b \in R$. We say a* divides *b, denoted $a|b$, if there is an element $c \in R$ such that $b = ac$. We say a is* associate to *b if there is a* unit *c such that $b = ac$.*

Proposition 1. *Let R be a C.U. ring with $a, b, c \in R$.*

1. *$a|a$*
2. *If $a|b$ and $b|c$ then $a|c$*
3. *If u is a unit, then $u|a$.*
4. *"Is associate to" is an equivalence relation.*
5. *The only associate of 0 is 0.*
6. *The associates of 1 are precisely the units.*

Proposition 2. *If R is a domain, then $a|b$ and $b|a$ if and only if a and b are associates.*

In a domain, every element is divisible by (1) units and (2) its associates. These are called *trivial divisors*. In general, a ring element will have more divisors. Some ring elements, however, have *only* the trivial divisors. These are special.

Definition 2 (Irreducible)**.** *Let R be a domain and $x \in R$ a nonzero nonunit. We say that x is* irreducible *in R if, whenever $a, b \in R$ such that $x = ab$, either a or b is a unit.*

$$\boxed{\text{Given a domain } R\text{, what are the irreducible elements of } R\text{?}}$$

Examples

- In $\mathbb{Z}$ the irreducible elements are precisely the prime integers.
- If R is a field, then R has no irreducible elements. (There are no nonzero nonunits!)

Brief Aside: Norms

For some rings (not all!) we can make progress on the problem of finding irreducibles by mapping the multiplicative structure of R to the $\mathbb{N}$ - doing this we can take advantage of what we know about natural numbers and, sometimes, recover the benefits of induction.

Definition 3. *Let R be a domain. A mapping $N : R \to \mathbb{N}$ is called a* multiplicative norm *if $N(\alpha) = 0$ if*

- *$N(\alpha) = 0$ iff $\alpha = 0$ and*
- *$N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in R$, and*
- *If $N(u) = 1$, then u is a unit in R.*

Examples

- $N : \mathbb{Z} \to \mathbb{N}$ given by $N(a) = |a|$ is a multiplicative norm.
- $N : \mathbb{Z}[i] \to \mathbb{N}$ given by $N(a + bi) = a^2 + b^2$ is a multiplicative norm.
- More generally, $N : \mathcal{O}(\sqrt{D}) \to \mathbb{N}$ given by $N(a + b\sqrt{D}) = |a^2 + Db^2|$ if $D \equiv 2, 3 \mod 4$ and $N(a + b\frac{1+\sqrt{D}}{2}) = |a^2 + ab + b^2\frac{1-D}{4}|$ if $D \equiv 1 \mod 4$ is a multiplicative norm.

Multiplicative norms allow us to detect irreducible elements.

Proposition 3. *Let R be a domain and $N : R \to \mathbb{N}$ a multiplicative norm. If $\alpha \in R$ such that $N(\alpha)$ is prime in $\mathbb{N}$, then α is irreducible in R.*

For example, consider $\mathbb{Z}[i]$. Applying this result here, we see that $a \pm bi$ is irreducible if $a^2 + b^2$ is prime. In particular $1 \pm i$, $1 \pm 2i$, $2 \pm 3i$, and many other Gaussian integers are irreducible (since $1^2 + 1^2 = 2$, $1^2 + 2^2 = 5$, and $2^2 + 3^2 = 13$ are prime). This leads to a natural question about the natural numbers: for which primes p does the equation $a^2 + b^2 = p$ have a solution?

As this example shows, a good multiplicative norm can turn questions in R into number theory problems. This turns out to be a useful technique more generally: given a problem about some object, look for a way to map the relevant structure of that object to some other object which either is well-understood or with which we can compute things. A good strategy for solving algebraic problems is to try to reduce to number theory or to linear algebra.

Primes

Definition 4. *Let R be a domain. We say that $p \in R$ is* prime *if whenever $p|ab$, either $p|a$ or $p|b$.*

Proposition 4. *If R is a domain, then every prime element is also irreducible.*

Proof. Suppose $p \in R$ is prime, and factor p as $p = ab$. In particular, $p|ab$, and since p is prime, WLOG we have $p|a$. Say $a = pt$. Now $p = ab = ptb$, and by cancellation, $tb = 1$. In particular b is a unit. Thus p is irreducible. $\square$

Exercises

1. (Divisibility in noncommutative rings.)