Visual Algebra

Lecture 8.3: Units and zero divisors

Dr. Matthew Macauley

School of Mathematical & Statistical Sciences
Clemson University
South Carolina, USA
http://www.math.clemson.edu/~macaule/

Units

Informally, a ring is a set where we can add, substract, multiply, but not necessarily divide.

Definition

A unit is any $u \in R$ that has a multiplicative inverse: some $v \in R$ such that $uv = vu = 1$.

Let $U(R)$ be the set (a multiplicative group) of units of R.

Proposition

If an ideal I of R contains a unit, then $I = R$.

Proof

Consider a unit $u \in I$. Then for any $r \in R$: $r = (ru^{-1})u \in I$, hence $I = R$. $\square$.

Examples

1. Let $R = \mathbb{Z}$. The units are $U(R) = \{-1, 1\}$.
2. Let $R = \mathbb{Z}_{10}$. Then 7 is a unit (and $7^{-1} = 3$) because $7 \cdot 3 = 1$. But 2 is not a unit.
3. Let $R = \mathbb{Z}_n$. A nonzero $k \in \mathbb{Z}_n$ is a unit if $\gcd(n, k) = 1$.
4. The units of $M_2(\mathbb{R})$ are the invertible matrices.

Zero divisors

Definition

An element $x \in R$ is a left zero divisor if $xy = 0$ for some $y \neq 0$. (Right zero divisors are defined analogously.)

Examples

1. There are no (nonzero) zero divisors of $R = \mathbb{Z}$.
2. The zero divisors of $R = \mathbb{Z}_{10}$ are $0, 2, 4, 5, 6, 8$.
3. A nonzero $k \in \mathbb{Z}_n$ is a zero divisor $\gcd(n, k) > 1$.
4. The ring $R = M_2(\mathbb{R})$ has zero divisors, such as:

$$\begin{bmatrix} 1 & -2 \\ -2 & 4 \end{bmatrix} \begin{bmatrix} 6 & 2 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

One particular type of zero divisor will be important later.

Definition

An element a in a ring R is nilpotent if $a^n = 0$ for some $n \in \mathbb{N}$.

Group rings

A rich family of examples of rings can be constructed from multiplicative groups.

Let G be a finite (multiplicative) group, and R a commutative ring (usually, $\mathbb{Z}$, $\mathbb{R}$, or $\mathbb{C}$).

The group ring RG is the set of formal linear combinations of group elements with coefficients from R. That is,

$$RG := \{a_1 g_1 + \cdots + a_n g_n \mid a_i \in R,\ g_i \in G\},$$

where multiplication is defined in the "obvious" way.

For example, let $R = \mathbb{Z}$ and $G = D_4$, and take $x = r + r^2 - 3f$ and $y = -5r^2 + rf$ in $\mathbb{Z}D_4$.

Their sum is

$$x + y = r - 4r^2 - 3f + rf,$$

and their product is

$$\begin{aligned} xy &= (r + r^2 - 3f)(-5r^2 + rf) = r(-5r^2 + rf) + r^2(-5r^2 + rf) - 3f(-5r^2 + rf) \\ &= -5r^3 + r^2 f - 5r^4 + r^3 f + 15fr^2 - 3frf = -5 - 8r^3 + 16r^2 f + r^3 f. \end{aligned}$$

Tip

Think of $\mathbb{Z}D_4$ as linear combinations of the "basis vectors"

$$\{\mathbf{e}_1,\ \mathbf{e}_r,\ \mathbf{e}_{r^2},\ \mathbf{e}_{r^3},\ \mathbf{e}_f,\ \mathbf{e}_{rf},\ \mathbf{e}_{r^2 f},\ \mathbf{e}_{r^3 f}\}.$$

Group rings

For another example, consider the group ring $\mathbb{R}Q_8$. Elements are formal sums

$$a + bi + cj + dk + e(-1) + f(-i) + g(-j) + h(-k), \qquad a, \dots, h \in \mathbb{R}.$$

Every choice of coefficients gives a different element in $\mathbb{R}Q_8$!

For example, if all coefficients are zero except $a = e = 1$, we get

$$1 + (-1) \neq 0 \in \mathbb{R}Q_8 \qquad \text{(because "}\mathbf{e}_1 + \mathbf{e}_{-1} \neq \mathbf{0}\text{")}.$$

In contrast, in the Hamiltonians, $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$,

$$1 + (-1) = [1 + 0i + 0j + 0k] + [(-1) + 0i + 0j + 0k] = (1 - 1) + 0i + 0j + 0k = 0.$$

Therefore, $\mathbb{H}$ and $\mathbb{R}Q_8$ are different rings.

Remarks

- If $g \in G$ has finite order $|g| = k > 1$, then RG always has zero divisors:

$$(1 - g)(1 + g + \cdots + g^{k-1}) = 1 - g^k = 1 - 1 = 0.$$

- RG contains a subring isomorphic to R.
- the group of units $U(RG)$ contains a subgroup isomorphic to G.

Fields and division rings

Definition

If every nonzero element of R has a multiplicative inverse, then R is a division ring. It is a

- field if R is commutative,
- skew field if R is not commutative.

Examples of fields we've seen include $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_p$ for prime p.

The Hamiltonians $\mathbb{H}$ are a skew field.

Definition

A quadratic field is any field of the form

$$\mathbb{Q}(\sqrt{m}) = \left\{ r + s\sqrt{m} \mid r, s \in \mathbb{Q} \right\},$$

where $m \neq 0, 1$ is a square-free integer. We say "$\mathbb{Q}$ *adjoin* $\sqrt{m}$."

This is a field because:

$$(r + s\sqrt{m})(r - s\sqrt{m}) = r^2 - s^2 m, \qquad (r + s\sqrt{m})^{-1} = \frac{r - s\sqrt{m}}{r^2 - s^2 m}.$$

Integral domains

Definition

An integral domain is a commutative ring with 1 and with no (nonzero) zero divisors.

An integral domain is a "field without inverses".

A field is just a commutative division ring. Moreover:

$$\text{fields} \subsetneq \text{division rings}, \qquad \text{fields} \subsetneq \text{integral domains}.$$

Examples

- Rings that are not integral domains: $\mathbb{Z}_n$ (composite n), $2\mathbb{Z}$, $M_n(\mathbb{R})$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{H}$.
- Integral domains that are not fields $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{R}[[x]]$ (formal power series).

The ring "$\mathbb{Z}$ adjoin $\sqrt{m}$," defined as

$$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\},$$

is an integral domain, but not a field.

Cancellation

When doing basic algebra, we often take for granted basic properties such as cancellation:

$$ax = ay \implies x = y.$$

This need not hold in all rings!

Examples where cancellation fails

- In $\mathbb{Z}_6$, note that $2 = 2 \cdot 1 = 2 \cdot 4$, but $1 \neq 4$.
- In $M_2(\mathbb{R})$, note that $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 4 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$.

However, everything works fine as long as there aren't any (nonzero) zero divisors.

Proposition

Let R be an integral domain and $a \neq 0$. If $ax = ay$ for some $x, y \in R$, then $x = y$.

Proof

If $ax = ay$, then $ax - ay = a(x - y) = 0$.

Since $a \neq 0$ and R has no (nonzero) zero divisors, then $x - y = 0$. □

Finite integral domains

Remark

If R is an integral domain and $0 \neq a \in R$ and $k \in \mathbb{N}$, then $a^k \neq 0$. □

Theorem

Every finite integral domain is a field.

Proof

Suppose R is a finite integral domain and $0 \neq a \in R$. It suffices to show that a has a multiplicative inverse.

Consider the infinite sequence $a, a^2, a^3, a^4, \dots,$ which must repeat.

Find $i > j$ with $a^i = a^j$, which means that

$$0 = a^i - a^j = a^j(a^{i-j} - 1).$$

Since R is an integral domain and $a^j \neq 0$, then $a^{i-j} = 1$.

Thus, $a \cdot a^{i-j-1} = 1$. □