An Introduction to Division Rings

Constructing Division Rings for Fun and Profit

Geoff Vooys

Sept. 23, 2016

Introduction: The Basic Definitions

Hi! I'm a Ring!

Let R be a set with binary operations $+, \circ : R \times R \to R$. We then say that R is a **Ring** if and only if for all $r, s, t \in R$:

1. $+$ is associative, i.e., $(r+s)+t = r+(s+t)$;
2. $+$ is commutative, i.e., $r+s = s+r$;
3. $+$ has a unique identity $0 \in R$ so that $r+0 = r$;
4. For all $r \in R$ there exists a unique $-r \in R$ such that
$$r + (-r) = 0 = (-r) + r;$$
5. $\circ$ is associative, i.e., $(rs)t = r(st)$;
6. $\circ$ has a unique identity element 1 such that $r1 = r = 1r$.
7. The operations $+$ and $\circ$ are left and right distributive, i.e., $r(s+t) = rs + rt$ and $(s+t)r = sr + tr$.

If $rs = sr$ for all $r, s \in R$, we say that the ring R is **commutative**. If R is not commutative, we say that it is **noncommutative**.

Examples of Rings

Examples

Here are some rings that you may or may not know:

- The set of integers $\mathbb{Z}$, the set of rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$ are all commutative rings;
- If R is a nonzero ring, $n \geq 2$ is an integer, and $\mathrm{Mat}_n(R)$ is the set

  $$\mathrm{Mat}_n(R) := \left\{ (a_{ij}) = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \;\middle|\; a_{ij} \in R; 1 \leq i, j \leq n \right\}$$

  then $\mathrm{Mat}_n(R)$ is a noncommutative ring.
- If R is any ring and x is an indeterminate over R with $rx^n = x^n r$ for all $n \in \mathbb{N}$, then the ring

  $$R[x] := \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; a_i \in R; n \in \mathbb{N} \right\}$$

  is a ring. $R[x]$ is commutative if and only if R is commutative.

Domains and Division Rings

UNIVERSITY OF CALGARY

Domains and Integral Domains

Let R be a ring. We then say that R is a **Domain** if for all $r, s \in R$ the equation $rs = 0$ implies that $r = 0$ or $s = 0$. If R is a commutative domain, then we say that R is an **Integral Domain**.

Division Rings

Let R be a domain. If, for every $r \in R$ with $r \neq 0$ there exists a unique $s \in R$ such that

$$rs = 1 = sr$$

then we say that R is a **Division Ring**. If R is a commutative division ring, then we say that R is a **Field**.

Hi! We're some Division Rings!

UNIVERSITY OF CALGARY

Examples

- The ring $\mathbb{R}$ of real numbers, the ring $\mathbb{C}$ of complex numbers, and the ring $\mathbb{Q}$ of rational numbers are all fields.
- The ring of **Real Quaternions**

$$\mathbb{H} := \{x + yi + zj + wk \mid x, y, z, w \in \mathbb{R}; i^2 = j^2 = k^2 = ijk = -1\}$$

  is a noncommutative division ring. In fact, we can show that

$$ij = k, ji = -k.$$

- The ring of **Rational Quaternions**

$$\mathbb{H}_{\mathbb{Q}} := \{x + yi + zj + wk \mid x, y, z, w \in \mathbb{Q}\}$$

  is also a noncommutative division ring.

Even More Division Rings and Domains!

UNIVERSITY OF CALGARY

More Examples

- Let $p \in \mathbb{Z}$ be prime. Then the quotient ring $\mathbb{Z}/p\mathbb{Z}$ is a field;
- Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial. Then the quotient ring $\mathbb{Q}[x]/(f)$ is a field;
- Let R be a ring with a unique maximal left ideal $\mathfrak{m}$. Then the ring $R/\mathfrak{m}$ is a division ring (in fact, this defines local rings).
- Let R be any integral domain. Then the ring $R[x]$ is an integral domain.
- Let $D \subseteq \mathbb{C}$ be a domain (connected open set) and let $K(D)$ be the ring of meromorphic functions on D. Then $K(\mathfrak{X})$ is a field.
- Let D be any division ring and let x be an indeterminate over D with $dx = xd$ for all $d \in D$. Then $D[x]$ is a domain.
- If R is any nonzero ring and $n \geq 2$, then $\mathrm{Mat}_n(R)$ is never a domain.

Basic Facts about Division Rings

UNIVERSITY OF CALGARY

The Center of a Ring

Let R be a ring. Then we say that the **Center of** R, denoted $Z(R)$, is the subring

$$Z(R) := \{r \in R \mid \forall\, s \in S.rs - sr = 0\}.$$

Center of a Division Ring

Let D be a division ring. Then $Z(D)$ is a field.

Finite Fields

Let K be a field. Then if K is finite, $|K| = p^n$ for some $n \in \mathbb{N}$ positive.

Wedderburn's Little Theorem

Let D be a finite division ring. Then D is a field.

A Key Ring in Building Division Rings

UNIVERSITY OF CALGARY

Ring of Formal Power Series

Let R be a ring and let x be an indeterminate with $rx^n = x^n r$ for all $n \in \mathbb{N}$ and all $r \in R$. Then define the ring $R[[x]]$, the **Ring of Formal Power Series of R** to be the set of formal power series

$$\sum_{n=0}^{\infty} a_n x^n$$

where elements are added and multiplied formally. Then $R[[x]]$ is a ring and is a domain if and only if R is a domain.

Units in $R[[x]]$

UNIVERSITY OF CALGARY

Characterizing Units in $R[[x]]$

Let $f = \sum a_n x^n \in R[[x]]$. Then f there exists a $g = \sum b_n x^n \in R[[x]]$ with $fg = 1 = gf$ if and only if a_0 is a unit in R.

Proof

To see this note that if $fg = 1 = gf$, then we have automatically that $a_0 b_0 = 1 = b_0 a_0$. So assume that a_0 is a unit in R. If we could find a $g \in R[[x]]$ we would have the simultaneous equations

$$1 = a_0 b_0, 0 = a_0 b_1 + a_1 b_0, \cdots, \sum_{k=0}^{n} a_k b_{n-k} = 0, \cdots$$

hold for all $n \in \mathbb{N}$. If such a polynomial $g = \sum b_n x^n$ existed, it would have $fg = 1$ automatically. Note that we can solve the first equation with $b_0 = a_0^{-1}$ and we can get $b_1 = a_0^{-1}(-a_1 b_0) = a_0^{-1}(-a_1 a_0^{-1})$. An induction shows the b_n may be calculated in terms of the a_k and we can determine a polynomial g with $fg = 1$; similarly, we can find an $h \in R[[x]]$ with $hf = 1$. A quick calculation shows that $h = g$ and we are done. $\square$

Rings of Formal Laurent Series

UNIVERSITY OF CALGARY

Rings of Formal Laurent Series

Let R be a ring. Then the *Ring of Formal Laurent Series*, denoted $R((x))$, is the ring of formal polynomials

$$\sum_{k=n}^{\infty} a_k x^k$$

where $n \in \mathbb{Z}$ and $x^{-m}x^m = 1$ for all $m \in \mathbb{Z}$.

Units in $R((x))$

If D is a division ring then so is $D((x))$. To see this let $f \in D((x))$ be a nonzero element $\sum_{k=n}^{\infty} a_k x^k$ with $a_n \neq 0$ and pick the power $x^{-n} \in D((x))$. Then

$$fx^{-n} = \sum_{k=0}^{\infty} a_{k-n} x^k = x^{-n} f$$

Since $a_0 \neq 0$, $a_0 \in \mathrm{Unit}(D)$ and $fx^{-n} \in \mathrm{Unit}(D[[x]])$ it follows that $fx^{-n} \in U(D((x)))$ and hence $f \in U(D((x)))$.

Examples of Building Division Rings from Laurent Series

Examples

- The ring $\mathbb{C}((x))$ is a field (we know this from complex analysis!);
- The rings $\mathbb{H}((x))$ and $\mathbb{H}_{\mathbb{Q}}((x))$ are both division rings;
- The ring $(\mathbb{Q}((x)))((y)) =: \mathbb{Q}((x, y))$ is a field;
- The ring $((\mathbb{H}((x)))((y)))((z)) =: \mathbb{H}((x, y, z))$ is a division ring.

Another Key Ring in Building Division Rings

UNIVERSITY OF CALGARY

Hilbert's Twisted Polynomial Rings

This ring is quite exotic in nature. Let K be any commutative ring and let $\sigma : K \to K$ be an endomorphism of K. Now define the ring $K[x;\sigma]$ to be the ring with underlying set

$$\left\{ \sum_{k=0}^{n} a_k x^k \,\middle|\, a_k \in K, n \in \mathbb{N} \right\}$$

with addition defined as standard polynomial addition. Generate multiplication by the equation $x^n b = \sigma^n(b)x^n$ for all $n \in \mathbb{N}$ so that multiplication takes the form

$$\left(\sum a_k x^k\right)\left(\sum b_\ell x^\ell\right) = \sum a_k \sigma^k(b_\ell) x^{k+\ell}.$$

Properties of Twisted Polynomials

Here we collect some basic properties of $K[x;\sigma]$:

- If $\sigma = \mathrm{id}_K$ is the identity endomorphism (where $\mathrm{id}_K(b) = b$ for all $b \in K$), then $K[x;\sigma] = K[x]$.
- If σ is nontrivial, i.e., if there is a $k \in K$ where $\sigma(k) \neq k$, then $K[x;\sigma]$ is noncommutative. In particular, if σ is not injective (so there is some $k \neq 0$ with $\sigma(k) = 0$), then $kx \neq 0$ but $xk = \sigma(k)x = 0x = 0$.
- If σ is injective (so that $\ker \sigma = 0$) and if K is an integral domain, then $K[x;\sigma]$ is a domain.

Formal Skew Power Series

Consider the ring $K[[x;\sigma]]$ of formal power series in x, with multiplication again defined by the rule

$$\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{m=0}^{\infty} b_m x^m\right) = \sum_{n,m=0}^{\infty} a_n \sigma^n(b_m) x^{n+m}.$$

Note that if K is a field, $f = \sum a_k x^k \in \mathrm{Unit}(K[[x;\sigma]])$ if and only if $a_0 \neq 0$.

Formal Skew Laurent Series

Skew Laurent Series

Let $\sigma : K \to K$ be an automorphism of K. Then we define the **Ring of Twisted (Skew) Laurent Series**, denoted $K((x;\sigma))$, is the ring of Laurent series in x over K, generated by the twist equation

$$\left(\sum_{k=n}^{\infty} a_k x^k\right)\left(\sum_{\ell=m}^{\infty} b_\ell x^\ell\right) = \sum_{k=n,\ell=m}^{\infty} a_n \sigma^n(b_m) x^{m+n}$$

for $m, n \in \mathbb{Z}$ and $\sigma^{-n} := (\sigma^{-1})^n$.

Properties of $K((x;\sigma))$

Begin by observing that if K is a field, then $K((x;\sigma))$ is a division ring. Let $\operatorname{ord}\sigma$ be the smallest positive $n \in \mathbb{N}$ such that $\sigma^n = \mathrm{id}_K$, with $\operatorname{ord}\sigma := \infty$ if no such $n \in \mathbb{N}$ exists. Then if K_0 denotes the field $K_0 := \{k \in K \mid \sigma(k) = k\}$, the center of $K((x;\sigma))$ is given by

$$\begin{cases} K_0 & \text{if } \operatorname{ord}\sigma = \infty; \\ K_0((x^{\operatorname{ord}\sigma})) & \text{if } \operatorname{ord}\sigma \in \mathbb{N}. \end{cases}$$

Now! Time to Build Division Rings!

UNIVERSITY OF CALGARY

Example

Let $K = \mathbb{C}$ be the field of complex numbers and let $\sigma = *$ be the complex conjugation automorphism, i.e., $\sigma(x+iy) = x - iy$. Then for all $n \in \mathbb{Z}$ we have

$$x^n(x+iy) = \sigma^n(x+iy)x^n = \begin{cases} (x-iy)x^n & \text{if } n \text{ odd;} \\ (x+iy)x^n & \text{if } n \text{ even.} \end{cases}$$

Then $C_0 = \{z \in \mathbb{C} \mid \sigma(z) = z\} = \mathbb{R}$ and since $\operatorname{ord}\sigma = 2$, we have $Z(\mathbb{C}((x;\sigma))) = \mathbb{R}((x^2))$. Thus $\mathbb{C}((x;\sigma))$ is the division ring of complex conjugation twisted polynomials with centre field the field of real even order Laurent series.

References

UNIVERSITY OF CALGARY

- Thomas W. Hungerford, *Algebra*, Springer-Verlag, New-York, 1980. Graduate Texts in Mathematics 73.
- T. Y. Lam, *A First Course in Noncommutative Rings*, 2001, Springer-Verlag, New-York, 2001. Graduate Texts in Mathematics 131.