Math 145: Algebra (Advanced Level) Notes

by Arnav Kumar

Web: https://arnavcs.github.io

These are takeaway notes for the fall 2022 offering of Math 145, instructed by Blake Madill at the University of Waterloo.

Note	Example	Definition	Results

Rings	A ring, $(R,+,\times)$, is a set, R, along with two functions, $+:R^2\to R$ and $\times:R^2\to R$, which we call addition and multiplication. We must have the following ring axioms: 1. There exists an additive identity. 2. Every element has an additive inverse. 3. Addition is commutative. 4. Addition is associative. 5. Multiplication is associative. 6. Multiplication distributes over addition. We often simply denote this ring by it set of elements, R.
Unital Rings, Units, and the Group of Units	A unital ring is a ring with a multiplicative identity. In a unital ring, R, an element with a multiplicative inverse is called a unit. The group of units of R is $R^\times := \{a\in R : a^{-1} \text{ exists}\}$. By convention, we say that the trivial ring, $\{0\}$ is non-unital.
Commutative Rings	A ring, R, is commutative if multiplication commutes, which is to say that $(\forall a,b\in R)(a\,b=b\,a)$.
Properties of Rings	From the ring axioms, we get the following results for a ring, R: 1. The additive inverse of any $a\in R$ is unique and denoted $-a$. 2. The additive identity is unique, and denoted 0_R. 3. $(\forall a\in R)(a\cdot 0_R = 0_R\cdot a = 0_R)$. 4. $(\forall a,b\in R)((-a)\,b = a\,(-b) = -(a\,b))$ And for a unital ring, R, we see: 1. The multiplicative identity is unique, and denoted 1_R. 2. If $a\in R^\times$, then the multiplicative inverse of a is unique and denoted a^{-1}.
Ring Notation	In a ring, R, and for some $n\in\mathbb{N}$, we generally say that 1. $a-b\equiv a+(-b)$ 2. $n\,a\equiv \underbrace{a+a+\cdots+a}_{n\,\text{times}}$. 3. If R is unital, $n\equiv n\,1\equiv \underbrace{1+1+\cdots+1}_{n\,\text{times}}$ 4. $a^n\equiv \underbrace{a\times a\times\cdots\times a}_{n\,\text{times}}$

Checking Commutativity	Let R be a ring. $$(R\,\text{commutative}) \Leftrightarrow (\forall a, b \in R)((a+b)^2 = a^2 + 2\,a\,b + b^2)$$
Binomial Theorem	Let R be a commutative ring. $(\forall a, b \in R)(\forall n \in \mathbb{N})$ $$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k\, b^{n-k}$$
Subring	A subring, S, of R is a subset of R which maintains the same ring structure of R. This means it is a ring under the same addition and multiplication definitions for R.
Subring Test	Let R be a ring, and let $\varnothing \neq S \subseteq R$. $$(S\,\text{subring of}\,R) \Leftrightarrow (\forall a, b \in S)(a \times b \in S \wedge a - b \in S)$$
Center of a Ring	Let R be a ring. The center of the ring is defined by: $$Z(R) := \{a \in R : (\forall b \in R)(a\,b = b\,a)\}$$ We have that $Z(R)$ is always a subring of R, and is commutative.
Zero Divisors and Integral Domains	Let R be a commutative ring. We call $0_R \neq a \in R$ a zero divisor if $(\exists b \in R, b \neq 0)(a\,b = 0_R)$. If a ring is commutative, unital, and has no zero divisors, it is an integral domain (or ID for short).
Cancellation	Let R be an integral domain. $(\forall a, b, c \in R, a \neq 0_R)$ $$a\,b = a\,c \Rightarrow b = c$$
Fields	A field is a commutative unital ring where every non-zero element is a unit.
Polynomial Rings	Let R be a commutative ring. We say the polynomial ring in x over R is the ring of polynomials in x with coefficients in R. This is to say $$R[x] := \{p_0 + p_1 x + \cdots + p_m x^m : m \in \mathbb{N}, p_i \in R, p_m \neq 0_R\,\text{if}\, m \neq 0\}$$
Properties of Fields and Integral Domains	Let R be a commutative, unital ring. 1. $(R\,\text{integral domain}) \Rightarrow (R[x]\,\text{integral domain})$. 2. If $0_R \neq a \in R$ is a zero divisor, then $a \notin R^{\times}$. 3. $(R\,\text{field}) \Rightarrow (R\,\text{integral domain})$. 4. $(R\,\text{integral domain}) \wedge (R\,\text{finite}) \Rightarrow (R\,\text{field})$.

buffer: division algorithm, division, mod integers, Bezout's identity, $[a]_n \in \mathbb{Z}_n^{\times} \Leftrightarrow (a, n) = 1$, $\mathbb{Z}_n$ field iff n prime