Math 114

Adam Topaz

Davis Foote[*]

University of California, Berkeley

August 27^{th}, 2015 – December 10^{th}, 2015

Contents

1 Review of Prerequisites

1.1 *Group Theory*

Group Actions

Lecture 1
September 3^{rd}, 2015

1.1 DEFINITION. $s \in S$

1) $Orb(s) = \{g \cdot s : g \in G\} \subseteq S$

2) $Stab(s) = \{g \in G : gs = s\}$

1.2 THEOREM (Orbit-stabilizer). *The map $G \to Orb(s)$ induces a bijection $G/Stab(s) \xrightarrow{\cong} Orb(s)$. The map is $g \cdot Stab(s) \mapsto g \cdot s$.*

1.3 COROLLARY. *If G is finite then $\frac{|G|}{|Stab(s)|} = [G : Stab(s)] = Orb(s)$*

[*]djfoote@berkeley.edu

1.2 *Ring Theory*

1.4 definition. A **ring** is a triple $(R, +, \times)$ that satisfies the following axioms:

1) $(R, +, 0)$ is an abelian group
2) $\times$ is associative
3) $\times$ distributes over $+$ (left and right)
4) $\times$ is associative

1.5 definition. The following are adjectives which may describe a ring:

- A **commutative ring** is a ring in which $\times$ is commutative.
- A **ring with unity** is one in which $(R \setminus \{0\}, \times)$ has an identity element.
- A **division ring** is one in which $(R \setminus \{0\}, \times)$ is a group
- A **field** is a commutative division ring.

1.6 example. $\mathbb{H}_{\mathbb{R}} = \{a + bi + cj + dij : a, b, c, d \in \mathbb{R}\}$ with the rules $i^2 = -1 = j^2, ij = -ji$ is called the **Hamiltonian quaternion group**. It is not commutative, but it is a division ring.

1.7 example. Let A be a commutative with unit. Then $A[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_i \in A\}$ is called the **polynomial ring with coefficients in A**. $A[x]$ is a commutative ring with unit, but it is not a division ring.

1.8 definition. A **zero divisor** is a nonzero element $a \in R$ such that there exists a nonzero element $b \in R$ such that $ab = 0$. An **integral domain** is a commutative ring which has no zero divisors.

1.9 definition. An **unit** is a multiplicatively invertible element. An element is **irreducible** is it cannot be written as a product of two elements which are not units. A **uniform factorization domain** is an integral domain such that any element can be written as a product of irreducible elements in a unique way (up to permutation of terms in product and replacement of one term by a unit times that term).

TODO: add definition of principal ideal

1.10 definition. An **ideal** of a ring A is an additive subgroup of A such that $\forall a \in A$, $aI \subseteq I$. A **principle ideal domain** is an integral domain in which every ideal is principal.

1.11 theorem. *Let K be a field. Then $K[x]$ is a principal ideal domain.*

TODO: complete this proof

Proof. It is clear that $K[x]$ is an integral domain. Let $I \trianglelefteq K[x]$. If $I = (0)$ or $I = (1)$. Suppose I is not either of these. Let $f \in I$ with $f \neq 0$ have $\square$

1.12 DEFINITION. A **Euclidean domain** is one in which there is a division algorithm, i.e. there exists some function $N : A \to \mathbb{Z}_{\geq 0}$ such that $\forall a, b \in A$, $b \neq 0$, $\exists q, r \in A$ with $a = bq + r$ such that $N(r) < N(b)$. Intuitively, this function N, called a norm, encodes the notion of the degree of an element.

1.13 EXAMPLE. $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a Euclidean domain where $N : \alpha \mapsto |\alpha|^2$

The hierarchy of the sets of all of these different algebraic objects is outlined as follows:

$$\begin{aligned} \text{Fields} &\subset \text{Euclidean domains} \\ &\subset \text{Principal ideal domains} \\ &\subset \text{Unique factorization domains} \\ &\subset \text{Integral domains} \\ &\subset \text{Commutative rings} \\ &\subset \text{Rings} \end{aligned}$$

Greatest Common Divisor

The GCD is a well-defined term in any unique-factorization domain up to multiplication by a unit (expand each one into a product of irreducible elements; the GCD is the factors that the elements have in common).

However, in a Euclidean domain, the Euclidean algorithm can be used to compute the GCD.

TODO: typeset this pseudocode $a = q_0 b + r_0$
$b = q_1 r_0 + r_1$
$r_0 = q_2 r_1 + r_2$
$\vdots$

Terminates because by the division algorithm, the degree of each r_i must be smaller than that of r_{i-1}, so eventually for some i we have $r_i = 0$.