6.885 Algebra and Computation	September 12, 2004
Lecture 2	
Lecturer: Madhu Sudan	*Scribe: Joshua A. Grochow*

This lecture begins a brief introduction to the algebraic structures we will be using throughout the course – groups, rings, and fields – and some of their elementary properties. We recommend *Finite Fields and Their Applications* by Lidl and Niedereitter as a reference.

1 Groups

A group is one of the most basic algebraic structures, specified by a single binary operation and its properties:

Definition 1 *A **group** G consists of a set, usually also denoted G, and a binary operation $\cdot : G \times G \to G$ satisfying the following properties:*

1. *Associativity: for all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*
2. *Identity: there exists an identity element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$.*
3. *Inverses: For each $a \in G$, there exists an element a^{-1} such that $a^{-1} \cdot a = a \cdot a^{-1} = e$.*

*A **semigroup** is defined similarly, but need not have inverses*[1]*.*

*A group or semigroup is called **Abelian** if in addition the operation is commutative:*

4. *For all $a, b \in G$, $a \cdot b = b \cdot a$*

Typically the group operation $\cdot$ is called "multiplication" and is omitted in notation: thus we write ab rather than $a \cdot b$. Generally if the group operation is denoted by addition $+$, it is assumed that the group is Abelian. When we wish to emphasize the group operation, we may write $(G, \cdot)$.

The standard Boolean algebra with the operation of $\wedge$ is an example of a semigroup: 1 is the identity, but 0 does not have an inverse, since $0 \wedge x = 0$ for any x.

The following are some useful properties of groups that are not difficult to prove. Let G be a group.

- Multiplication by any $x \in G$ is injective: that is, $ax = bx$ iff $a = b$.
- The equation $ab = c$, $a, b, c \in G$ has a unique solution whenever any two of a, b, c are specified. In particular, the identity is unique, and inverses are unique.

The **order** of a group G is the number of elements of G, and is denoted $|G|$.

A **subgroup** H of a group G is a subset of G which is a group under the operation of G restricted to H. We write $H \leq G$. In particular, a subset $H \subseteq G$ is a subgroup if it is closed under the operation of G.[2]

A (left) **coset** of a subgroup $H \leq G$ is a set $aH = \{ah | h \in H\}$. Two (left) cosets aH and bH are either disjoint or equal. Since multiplication is injective, the cosets of H are the same size as H, and thus H partitions G into equal-sized parts. This leads to Lagrange's Theorem: $|H|$ divides $|G|$.[3] We can now prove a generalized version of Fermat's Little Theorem:

Theorem 2 (Fermat's Little Theorem) [4] *For every finite group G, for all $a \in G$, $a^{|G|} = e$.*

[1]Some authors also allow semigroups to lack an identity element, and call semigroups with identity **monoids**.

[2]When G is infinite, a subset H must also contain inverses to be a subgroup. When G is finite, closure under the operation of G provides inverses, since for all $a \in G$, $a^{-1} = a^n$ for some finite positive n.

[3]For those who know something about multiplication of infinite cardinals, this theorem holds when H and G are infinite as well.

[4]Abstract group theory was not developed until well after Fermat's time. Fermat's Little Theorem was originally that $a^{p-1} \equiv 1 \bmod p$ for all nonzero a in the integers modulo any prime p. Note that the nonzero integers modulo p form a multiplicative group of order $p - 1$.

Proof Consider the subgroup H generated by a: $H = \{a^i | i \in \mathbb{Z}\}$. Since G is finite, the infinite sequence $a^0 = e, a^1, a^2, a^3, \ldots$ must repeat, say $a^i = a^j$, $i < j$. Let $k = j - i$. Multiplying both sides by $a^{-i} = (a^{-1})^i$, we get $a^{j-i} = a^k = e$. Suppose k is the least positive integer for which this holds. Then $H = \{a^0, a^1, a^2, \ldots, a^{k-1}\}$, and thus $|H| = k$. By Lagrange's Theorem, k divides $|G|$, so $a^{|G|} = (a^k)^{|G|/k} = e$. ■

The **order** of $a \in G$ is the least k such that $a^k = e$. This is consistent with the definition of order of a group, as the order of a is the order of the subgroup generated by a.

2 Rings and Fields

A ring is, in some sense, the next most basic algebraic structure, involving two related binary operations:

Definition 3 *A **ring** R consists of a set R and two binary operations $+$ ("addition") and $\cdot$ ("multiplication") on R satisfying:*

1. *$(R, +)$ is an Abelian group with identity denoted 0.*
2. *$(R, \cdot)$ is a semigroup with identity denoted 1. (Some authors do not require a ring to contain a multiplicative identity.)*
3. *Multiplication distributes over addition: $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.*

We will generally only be concerned with commutative rings, i.e. rings in which multiplication is commutative. The canonical example of a ring is the integers $\mathbb{Z}$ under the standard operations of addition and multiplication.

Definition 4 *A **field** F is a commutative ring in which every non-zero element has a multiplicative inverse. Equivalently, $(F - \{0\}, \cdot)$ is an Abelian group.*

The rationals, the reals, and the complex numbers are all fields. The integers modulo p for prime p are also fields.

An **integral domain** is a ring in which $ab = 0$ implies $a = 0$ or $b = 0$. An example of a non-integral domain is the integers modulo n, where n is not prime: if $n = pq$ is a nontrivial factorization of n, then $pq \equiv 0$ modulo n, but neither p nor q is zero mod n. Square matrices are another example.

We will now prove two facts which make integral domains similar to fields.

Fact 5 *Any finite integral domain R is a field.*

We will prove this fact two different ways: the first is often used in abstract algebra textbooks, while the second lends itself to a slightly better algorithm for computing the inverse of an element.

Proof Let a be a nonzero element of R. Examine the products $P = \{ba | b \in R\}$. These are all distinct, as $ba = ca \Rightarrow (b - c)a = 0 \Rightarrow b = c$. Since R is finite, $P = R$, and thus there is some $b \in R$ such that $ba = 1$. ■

Proof Let a be a nonzero element of R. Examine the powers of a. The sequence $a^0, a^1, a^2, \ldots$ must repeat eventually since R is finite, say $a^i = a^j$, $i < j$. Then $a^i(1 - a^{j-i}) = 0$. Since R is an integral domain, $a^i \neq 0$, so $1 - a^{j-i} = 0$, and thus the inverse of a is given by a^{j-i-1}. ■

Definition 6 *The **field of fractions** $\tilde{R}$ of an integral domain R is $\{(a, b) | a, b \in R, b \neq 0\}$ modulo the equivalence $(a, b) \sim (c, d)$ iff $ad = bc$, with addition and multiplication defined as follows:*

$$\begin{aligned}(a, b) \cdot (c, d) &= (ac, bd) \\ (a, b) + (c, d) &= (ad + bc, bd)\end{aligned}$$

Note that $\tilde{R}$ is a field[5] containing R as the elements $(a, 1)$.

Given a ring R, we now construct the ring $R[x]$ of polynomials in one variable x with coefficients in the ring R. An element of $R[x]$ is given by the coefficients of a polynomial $(a_0, a_1, \ldots, a_d)$ with $a_i \in R$. (We take these modulo the equivalence relation $(a_0, a_1, \ldots, a_d, 0, 0, \ldots, 0) \sim (a_0, \ldots, a_d)$.) Addition of two such sequences is carried out component-wise, where one sequence may be extended by zeros on the right to match the length of the other sequence. Multiplication of two sequences is given by:

$$(a_0, \ldots, a_d) \cdot (b_0, \ldots, b_e) = (c_0, \ldots, c_{e+d})$$

where $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.

The polynomial ring $R[x]$ often inherits many properties of R. Note that if R is an integral domain, then so is $R[x]$.

A **subring** is a subset of a ring which is itself a ring, except that it need not contain the identity element. The subrings of $\mathbb{Z}$ are of the form $n\mathbb{Z} = \{nk | k \in \mathbb{Z}\}$.

Definition 7 *An* ***ideal*** $I \subseteq R$ *is a subring with the additional property that* $a \in I$ *implies* $ar \in I$ *for any* $r \in R$.

If an ideal $I \subseteq R$ contains 1, then $I = R$. As an example, any subring of $\mathbb{Z}$ is also an ideal (this is a very special property of the integers and does not hold in most rings).

Ideals are particularly nice subrings, because they allow for the following construction:

Definition 8 *Given a ring* R *and ideal* I*, the quotient ring* R/I*, read "*R *modulo* I*", is the set of cosets* $a+I$ *of* I *as an additive subgroup of* $(R, +)$*. Addition and multiplication are as expected:* $(a+I)+(b+I) = (a+b)+I$ *and* $(a+I)(b+I) = ab+I$.

In studying a ring, it is often useful to examine its quotient rings R/I, as they are usually simpler than R itself but may retain many of its properties. One fimilar example of this is when we examine the integers modulo n, which we may now write $\mathbb{Z}/n\mathbb{Z}$. In particular, we have the Chinese Remainder Theorem (CRT). Over the integers, the CRT says that m modulo n is uniquely specified by m modulo p_i where $\prod p_i = n$ and the p_i are relatively prime. We will now generalize this to rings and ideals.

Given two ideals $I, J \subset R$, we have that $I \cap J$ and $IJ = \{\sum r_i a_i b_i | r_i \in R, a_i \in I, b_i \in J\}$ are both ideals. While this last definition is somewhat unwieldy, note that it is the smallest ideal containing all elements of the form ab where $a \in I$ and $b \in J$, since ideals must be closed under addition and multiplication by arbitrary ring elements. Note that $IJ \subseteq I \cap J$.

We will say that I and J are relatively prime if $IJ = I \cap J$. (Note that this indeed holds for the ideals $n\mathbb{Z}$ and $m\mathbb{Z}$ when n and m are relatively prime integers.) We can now state the more general form of the CRT:

Theorem 9 (Chinese Remainder Theorem) *If* $I_1, \ldots, I_k$ *are relatively prime ideals of a ring* R*, then* $R/(\prod I_i) \cong (R/I_1) \times \cdots \times (R/I_k)$.

The proof of this is not much more difficult than the proof of the CRT for the integers, and is left as an exercise.

3 Factorization

Definition 10 *An element* $a \in R$ *is called a* ***unit*** *if* a *has a multiplicative inverse in* R.

[5] A similar construction can be defined for non-integral domains R, but the details are a bit more complicated, and the resulting structure will not be a field.

Definition 11 *A ring R is a **factorization domain** if given any non-unit $a \in R$, there exists a positive integer d such that any factorization of a into non-units $a_1, \ldots, a_k$ (that is, $a = a_1 a_2 \cdots a_k$) has $k \leq d$. (This is not a standard definition.)*

Definition 12 *An element $a \in R$ is **irreducible** if $a = pq$ implies that one of p or q is a unit.*

Definition 13 *A ring R is a **unique factorization domain**, or UFD, if every element of $a \in R$ may be factored uniquely into irreducibles. This uniqueness is taken up to re-ordering and multiplication by units: if p_i and q_i are irreducible, and $a = p_1 \cdots p_d = q_1 \cdots q_e$, then $e = d$ and there is some permutation π such that $p_i = u_i q_{\pi i}$ for some units u_i, $1 \leq i \leq d$.*

The integers are a UFD.

As an example of a factorization domain which is not a UFD, we adjoin the square root of 5 to $\mathbb{Z}$: $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} | a, b \in \mathbb{Z}\}$. Then we have $4 = 2 \cdot 2 = (\sqrt{5}+1)(\sqrt{5}-1)$. For this to be a valid example, you must verify that 2 and $\sqrt{5} \pm 1$ are irreducible in $\mathbb{Z}[\sqrt{5}]$.

As an example of a ring which is not even a factorization domain, we adjoin the n-th roots of 2 to the integers for all positive n. Then we have $\mathbb{Z}[2^{1/2}, 2^{1/3}, 2^{1/4}, \ldots]$. Suppose this were a factorization domain, and let d be the bound on the length of factorizations of 2. Let $n = d+1$. Then we can factor 2 as $2 = 2^{1/n} \cdot 2^{1/n} \cdots 2^{1/n}$, which has $n > d$ non-unit factors. Thus no such d exists, and this is not a factorization domain.

Finally, as a claim which we will prove next time, if R is a UFD, then so is the polynomial ring $R[x]$.