

# A Rough Guide to Groups, Rings, and Fields

Elisha Peterson

November 6, 2003

## Contents

<b>1</b>	<b>Getting Oriented</b>	<b>2</b>
<b>2</b>	<b>Groups</b>	<b>2</b>
2.1	The Basics . . . . .	2
2.2	Examples . . . . .	2
2.3	Subgroups and Cyclic Groups . . . . .	3
2.4	Group Morphisms . . . . .	3
2.5	Permutation Groups . . . . .	4
2.6	Cosets and Factor Groups . . . . .	4
2.7	The Isomorphism Theorems . . . . .	5
2.8	Direct Products and Finite Abelian Groups . . . . .	5
2.9	Sylow Theory . . . . .	6
2.10	Finite Simple Groups . . . . .	6
<b>3</b>	<b>Rings</b>	<b>7</b>
3.1	Subrings . . . . .	8
3.2	Ideals and Factor Rings . . . . .	8
3.3	Integral Domains . . . . .	8
3.4	Ring Homomorphisms and Isomorphisms . . . . .	9
3.5	More on Polynomial Rings . . . . .	9
3.6	General Integral Domains . . . . .	9
<b>4</b>	<b>Fields</b>	<b>10</b>
4.1	Vector Spaces . . . . .	10
4.2	Extension Fields . . . . .	10
4.3	Algebraic Extensions . . . . .	11
4.4	Finite Fields . . . . .	11
4.5	Galois Theory . . . . .	11
<b>5</b>	<b>The Road Ahead</b>	<b>12</b>

# 1 Getting Oriented

The main goal in abstract algebra is extending the operations and properties we take for granted on sets we're used to working with (like integers, reals, complex numbers, etc.) to arbitrary sets. This requires precise definitions and requirements on the structure of the set in order to ensure the desired properties are present.

The starting point of abstract algebra is the *group*, which is just a set with an operation such as addition. A surprising number of sets fit into this category, allowing us to analyze things as diverse as the integers modulo  $k$ , invertible matrices, and symmetries of a polygon all at once. We'll eventually turn to the question of classification of groups, which is done both by size and by type.

Later, we will encounter the *ring*, which is just a set with two operations (traditionally addition and multiplication) such as the real numbers. A related structure is the *field*, which also has two operations but allows for division as well. Several more definitions fall somewhere between rings and fields with specific defining properties, such as the existence of a division algorithm. Our last goal will be proving the insolvability of the quintic, a subject which demonstrates a strong relationship between groups and fields.

Groups, rings, and fields are the three primary objects of study in abstract algebras, and the definitions intended to make them look like known sets give rise to a much more general theory. More definitions are made to accommodate this theory than in perhaps any other field of mathematics. Memorizing the most basic definitions is recommended, and will prove to make the rest more palatable.

## 2 Groups

### 2.1 The Basics

Without further ado, here is the most important definition in abstract algebra:

**Group:** a set  $G$  with binary operation  $\diamond$  with:

(1) **associativity:**  $(a \diamond b) \diamond c = a \diamond (b \diamond c)$  for all  $a, b, c \in G$ ;

(2) an **identity**  $e$ : an element  $e \in G$  with  $a \diamond e = e \diamond a$  for all  $a \in G$ ; and

(3) an **inverse** for all  $a \in G$ : an element  $a^{-1} \in G$  with  $a \diamond a^{-1} = a^{-1} \diamond a = e$ .

If, in addition, the operation is **commutative** ( $a \diamond b = b \diamond a$  for all  $a, b \in G$ ), then the group is **abelian**.

The group is denoted  $(G, \diamond)$  if one wishes to specify the operation explicitly. Some essential group properties include uniqueness of the identity, left and right cancellation laws, and uniqueness of inverses. Typical examples of group operation include addition and multiplication. Subtraction and division are usually not group operations since they are not associative.

The **order** of a group is the number of elements it contains (possibly infinite), giving a definition of a **finite group**. The **order** of an element  $a$  of a group is the smallest  $k \in \mathbb{Z}^+$  such that  $a^k = e$ , where exponentiation denotes repeated multiplication.

### 2.2 Examples

The most basic examples of groups under addition include  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ , vectors, and matrices. With addition modulo  $n$ ,  $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$  becomes a group. This is actually the same group as the complex roots of unity  $\{e^{2\pi ik/n}\}$  under the operation of complex multiplication.

Groups under multiplication include  $\hat{\mathbb{Q}}, \hat{\mathbb{R}},$  and  $\hat{\mathbb{C}}$  ( $\hat{\cdot}$  indicates the additive identity 0 is omitted). The  $m \times n$  matrices form a group  $M(m, n)$  under addition, and the  $n \times n$  matrices with nonzero determinant also form a group, denoted  $GL(n, \mathbb{R})$ , under matrix multiplication.

Another example of a finite group is the symmetries of a polygon of  $n$  sides, called the **dihedral group** and denoted  $D_n$ . It has  $2n$  elements:  $n$  rotations and  $n$  reflections. There

is also  $U(n)$ , consisting of the positive integers less than  $n$  which are relatively prime to  $n$ . The number of its elements defines the *Euler phi function*  $\phi(n) = |U(n)|$ .

### 2.3 Subgroups and Cyclic Groups

A **subgroup**  $H$  of a group  $G$  is a subset that is itself a group under the operation of  $G$ , denoted by  $H < G$ . For example,  $\mathbb{Z}, \mathbb{Q}$ , and  $\mathbb{R}$  are all subgroups of  $(\mathbb{C}, +)$ . A subset will be a subgroup iff it is closed under the group operation  $\diamond$  and inversion. In a finite group, one only need test for closure under  $\diamond$ .

Here are a few ways to construct a subgroup (in the notation of multiplicative groups):

- $\langle a \rangle$ : the **cyclic subgroup**  $\{1, a, a^{-1}, a^2, a^{-2}, \dots\}$  generated by  $a$ ;
- $Z(G)$ : the **center** of  $G$ , containing elements of  $G$  commuting with all other elements;
- $C(a)$ : the **centralizer** of  $a \in G$ , containing elements of  $G$  which commute with  $a$ .

The first two,  $\langle a \rangle$  and  $Z(G)$ , are always abelian. In general, a **cyclic group**, such as  $\langle a \rangle$ , is one generated by a single element (and its inverse). These groups are all abelian and behave like either the integers  $\mathbb{Z}$  or the finite group  $\mathbb{Z}_n$ . Some elementary properties of cyclic groups follow, with  $G = \langle a \rangle$  having order  $n$ :

- if  $a^k = e$ , then  $n$  divides  $k$  ( $n|k$ );
- $G = \langle a^k \rangle$  if and only if  $\gcd(n, k) = 1$  (these are the **generators** of the group);
- each divisor  $k$  of  $n$  corresponds to one subgroup of order  $k$ , namely  $\langle a^{n/k} \rangle$ ;
- the number of elements of order  $n$  is given by  $\phi(n)$ , the *Euler phi function*.

### 2.4 Group Morphisms

Two groups may be defined differently, but behave in exactly the same way. This leads us to the notion of equivalence among groups:

**Isomorphism:** a bijective map  $\phi : G \rightarrow G'$  which preserves the group operation, so that  $\phi(ab) = \phi(a)\phi(b)$ . The groups  $G$  and  $G'$  are **isomorphic**, and we write  $G \cong G'$ .

If the map is not bijective, but still preserves the group operation, it is a **homomorphism**.

The importance of this lies in the fact that every property of a group (other than the names of its elements), is preserved under isomorphism. It also indicates a fundamental question: how many non-isomorphic groups are there? Proving that two groups are not isomorphic is usually not too hard: one just needs to find properties of the two that differ. But proving that two groups are isomorphic can be more tedious since one must produce the actual isomorphism  $\phi$ .

Homomorphisms also preserve many properties of a group, taking (abelian or normal) subgroups to (abelian or normal) subgroups. The same is true for the inverse image of a homomorphism. They are useful in the study of groups because they can simplify the problem at hand by removing some of a group's excess structure. As such, it is often easier to study homomorphisms of a group than the group itself.

An **automorphism** is an isomorphism from a group to itself, and such maps form the **automorphism group**  $(\text{Aut}(G), \circ)$  under function composition. Maps of the form  $\phi_a(x) = axa^{-1}$  for some  $a \in G$  are always automorphisms and form the **inner automorphism group**  $\text{Inn}(G) < \text{Aut}(G)$ . As a quick example,  $\text{Aut}(\mathbb{Z}_n) \cong U(n)$ . Homomorphisms from  $G$  to another group  $G'$  also form a group, denoted  $\text{Hom}(G, G')$ ; with group operation inherited from the operation on  $G'$ .

## 2.5 Permutation Groups

A **permutation group** is a group of bijective maps from a set  $A$  to itself under the group operation of composition. A first example is the automorphisms  $\text{Aut}(G)$ . Permutations are important due to:

**Cayley's Theorem:** every group is isomorphic to a group of permutations.

To specify a permutation, one must clearly show where each element of the set  $A$  is taken. In the finite case, one can use the following notation:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{bmatrix}.$$

This indicates that 1 is mapped to 2, 2 to 3, and so on.

A more compact notation is **cycle notation**. This would give the above as  $(1\ 2\ 3)(4\ 6)$ , which means swap 4 and 6, and then rotate 1, 2, and 3. Note that, as for functions, you always start on the right and work left. Thus, the permutation can also be written as  $(1\ 3)(2\ 3)(4\ 6)$ . Disjoint cycles commute, and all permutations can be written as a product of disjoint cycles; in this case, the order of the permutation is the LCM of the cycle lengths.

The group of all  $n!$  permutations of  $n$  elements is known as the **Symmetric Group**  $S_n$ . Every finite permutation can be written as the product of *transpositions*, or 2-cycles, and the number of such cycles will always have the same parity. Thus, we can speak of *even* or *odd* permutations. The even permutations form the **Alternating Group**  $A_n$ , which has exactly  $n!/2$  elements.

A given element  $a \in A$  determines an important subgroup of permutations called the **stabilizer subgroup**  $\text{stab}(a)$ , which consists of the permutations which fix  $a$ . The element also determines a subset of  $A$  called the **orbit**  $\text{orb}(a)$ , which consists of all the elements mapping to  $a$  under permutations in the group (or all the elements  $a$  maps to). The **Orbit-Stabilizer Theorem** says that  $|G| = |\text{orb}(a)||\text{stab}(a)|$  for any  $a \in A$ .

## 2.6 Cosets and Factor Groups

Any subgroup naturally partitions a group into disjoint subsets, called *cosets*. Formally, a **left coset** of a subgroup  $H < G$  is a subset  $aH = \{ah : h \in H\}$  for some  $a \in G$ , while a **right coset** is given analogously by  $Ha$ . The fact that the cosets partition the group, and also that  $aH = H$  iff  $a \in H$ , follows from:

**Lagrange's Theorem:** the **index**  $[G : H] = |G|/|H|$  of any subgroup is an integer, equal to the number of distinct left (or right) cosets of  $H$ .

It follows immediately that all groups of prime order are cyclic (since they have no nontrivial subgroups), that  $a^{|G|} = e$  for all elements  $a \in G$ , and that  $a^p \equiv a \pmod{p}$  for  $p$  prime (*Fermat's Little Theorem*).

When a subgroup is normal (meaning the left and right cosets always coincide), the set of cosets actually has a group structure:

**Normal Subgroup:** a subgroup  $H$  such that  $aH = Ha$  for all  $a \in G$ , or equivalently  $aHa^{-1} = H$ . Normalcy is denoted by  $H \triangleleft G$ . The set of cosets form the **factor group**  $G/H$ , with the operation inherited from the group.

By Lagrange's Theorem,  $|G/H| = |G|/|H|$ . Elements of a factor group  $G/H$  are usually denoted  $gH$  for some  $g \in G$ .

The center of a group  $Z(G)$  is always normal, and the factor group  $G/Z(G)$  is isomorphic to the inner automorphism group  $\text{Inn}(G)$ . In particular, it is cyclic/trivial iff  $G$  is abelian (this is the  **$G/Z$  Theorem**). This can be used to show that an abelian group  $G$  has elements of each prime order dividing  $|G|$ .

## 2.7 The Isomorphism Theorems

In this section we look at three theorems that hold, with slight modifications, for rings and other algebraic structures besides groups. They are useful tools both in algebra and in other areas of mathematics. We have:

**First Isomorphism Theorem:** Given a group homomorphism  $\phi : G \rightarrow \bar{G}$ , there is an isomorphism  $\frac{G}{\ker \phi} \cong \phi(G)$  given by  $g \ker \phi \mapsto \phi(g)$ .

This is somewhat intuitive: it says that the image of a homomorphism looks like a factor group of  $G$  with the elements mapping to the identity being trivial.

As a corollary, we have the **N/C Theorem**, which states that  $N(H)/C(H)$  is isomorphic to a subgroup of  $\text{Aut}(H)$ . Recall that  $N(H)$  is the **normalizer** of  $H$ , the set of elements  $g \in G$  with  $gHg^{-1} \in H$ , and  $C(H)$  is the **centralizer** of  $H$ , the elements of  $G$  commuting with all elements of  $H$ . The isomorphism corresponds to the map  $N(H) \rightarrow \text{Aut}(H)$  taking  $g$  to  $\phi_g : h \mapsto ghg^{-1}$ , which is a group homomorphism with kernel  $C(H)$ .

A simple application of this result is the proof that every group of order 35 is cyclic. First, counting arguments show that  $G$  must have elements of order both 5 and 7. Let  $H$  be a cyclic subgroup of order 7. One can show that  $N(H) = G$  and that  $H \leq C(H)$ . But  $|N(H)/C(H)|$  must divide 6, the order of  $\text{Aut}(H)$ , which is possible only if  $|C(H)| = 35$ . Then, an element  $hk$ , where  $h \in H$  is nontrivial and  $k$  has order 5, will generate the group.

The second and third isomorphism theorems have a flavor similar to the first:

**Second Isomorphism Theorem:** Given a subgroup  $K \leq G$  and a normal subgroup  $N \triangleleft G$ , we have  $\frac{K}{K \cap N} \cong \frac{KN}{N}$ .

**Third Isomorphism Theorem:** Given subgroups  $N \triangleleft M \triangleleft G$ , we have  $\frac{G/N}{M/N} \cong \frac{G}{M}$ .

## 2.8 Direct Products and Finite Abelian Groups

Having analyzed subgroups and factor groups, which in a sense ‘make a group smaller’, we now look at direct products, which form bigger groups out of smaller ones. The simplest product group is the **external direct product** of groups  $G$  and  $G'$ , denoted  $G \oplus G'$  and defined as the set of elements  $(g, g')$  with operation acting separately on each coordinate.  $(G, e') \cong G$  and  $(e, G') \cong G'$  are then factor groups.

It is easy to see that the order of an element  $(g, g')$  is just the LCM of the orders of  $g$  and  $g'$ . Thus, a group  $G \oplus G'$  is cyclic iff both  $G$  and  $G'$  are cyclic, with  $|G|$  and  $|G'|$  relatively prime. In particular, for  $(m, n) = 1$ , we have  $\mathbb{Z}_m \oplus \mathbb{Z}_n = \mathbb{Z}_{mn}$  and  $U(m) \oplus U(n) = U(mn)$ .

The **internal direct product** is a way of representing a given group as a direct product of its subgroups; thus, we write  $G = H \times K$  if  $G = HK$  where  $H$  and  $K$  are normal subgroups and  $H \cap K = \{e\}$ . Actually,  $H \oplus K \cong H \times K$ , so the only difference between the products is that the external sum builds bigger groups from smaller ones, while the internal sum breaks groups into smaller pieces.

Finite abelian groups are completely classified by the following theorem:

**Fundamental Theorem of Finite Abelian Groups:** Every finite abelian group is isomorphic to a unique direct product of cyclic groups whose orders are prime powers, that is  $G \cong \mathbb{Z}_{p_1}^{n_1} \oplus \cdots \oplus \mathbb{Z}_{p_k}^{n_k}$ .

This fundamental result usually caps the undergraduate study of groups. As a corollary, such a group has subgroup of order  $m$  for each  $m$  dividing the group order.

To prove this result, we begin by noting that it is sufficient to consider groups of order  $p^k$ ; otherwise if  $|G| = p^n m$  we can write  $G = H \times H'$  where  $H$  has the elements with  $x^{p^k} = e$  and  $H'$  has those with  $x^m = e$ . Now, an abelian group of order  $p^k$  is isomorphic to  $\langle a \rangle \times K$ , where  $a$  is an element of maximal order. Using induction, this means  $G$  is a direct sum of cyclic groups. The final step is to verify uniqueness.

## 2.9 Sylow Theory

It is much more difficult to write down all the nonabelian groups of a certain order. The answer is best achieved with the Sylow theorems, a collection of tools for determining properties of groups of a certain order. We begin by developing some of the theory used in the proofs of the Sylow theorems.

First, we define **conjugate subgroups** to be subgroups  $H, K < G$  such that  $H = gKg^{-1}$  for some  $g \in G$ . Similarly, we define the **conjugacy class** (of  $a \in G$ ) to be the set of elements  $xax^{-1}$  for  $x \in G$ , denoted  $\text{cl}(a)$ . These sets partition the group, but not like cosets since  $\text{cl}(e) = \{e\}$ . It is easy to show that  $|\text{cl}(a)| = |G : C(a)|$ , where  $C(a)$  is the centralizer subgroup. Thus, we have the **class equation**  $|G| = \sum |G : C(a)|$ , the sum taken over conjugacy classes. This can alternately be written

$$|G| = |Z(G)| + \sum |G : C(a)|,$$

taking the sum over elements outside of  $Z(G)$ . This formula reveals a lot about the orders of subgroups.

We'll now look at some theorems arising from the class equation. First, if  $|G| = p^n$ , we can divide the class equation by  $p$  to see that  $Z(G)$  must be nontrivial. Applying the  $G/Z$  Theorem to this result, we see that all groups of order  $p^2$  are abelian. We also have the Sylow Theorems:

- **(Sylow's First Theorem)** If  $p^k$  divides  $|G|$ , then  $G$  has a subgroup of order  $p^k$  (an inductive proof using the class equation). Such a group of maximal order is called a **Sylow  $p$ -subgroup**;
- **(Sylow's Second Theorem)** Every subgroup  $H$  of order  $p^k$  of a finite group  $G$  is contained in some Sylow  $p$ -subgroup (a harder proof using the notion of conjugate subgroups and the Orbit-Stabilizer Theorem);
- **(Sylow's Third Theorem)** The number of Sylow  $p$ -subgroups (denoted  $n_p$ ) is equal to 1 modulo  $p$  and divides  $|G|$ , and any two such subgroups are conjugate (again uses the Orbit-Stabilizer Theorem).

Note that the second theorem implies that a group  $G$  has an element of order  $p$  for every  $p$  dividing  $|G|$ . The third theorem implies that a Sylow  $p$ -subgroup is unique (so  $n_p = 1$ ) iff it is a normal subgroup.

The above results are extremely useful in classifying the groups of a certain order. As an example, Sylow's Third Theorem implies that a group of order 40 has only one Sylow 5-subgroup; hence that group is normal. A group of order 30 must have either 1 or 6 Sylow 5-subgroups, and 1 or 10 Sylow 3-subgroups. Counting shows that one of these subgroups is normal, giving us a cyclic, normal subgroup of order 15.

A more general case is  $|G| = 2p$ , for  $p$  an odd prime. In this case  $G$  is isomorphic to either  $\mathbb{Z}_{2p}$  or the dihedral group  $D_p$ ; in fact there are at most 2 groups of order  $pq$  for any primes  $p, q$ . It is also true that for  $|G| = pq$ , with  $p < q$  not dividing  $q - 1$ , then  $G \cong \mathbb{Z}_{pq}$ .

## 2.10 Finite Simple Groups

In this section, we continue with the question 'how many?' by looking at a special class of groups which has been completely classified, the *finite simple groups*:

**Simple Group:** a group whose only normal subgroups are the identity and itself; thus, it has no factor groups.

One can think of simple groups as the building blocks of groups; factoring out the largest normal subgroup  $G_1$  of a group  $G_0$  gives a simple group  $H_1 = G_0/G_1$ . This process may be continued, and the groups  $H_i = G_{i-1}/G_i$  are called the **composition factors**. Using this

decomposition, many problems in group theory can be reduced to the case of simple groups using induction.

Finite simple groups have been completely classified, divided into seven infinite families (such as  $A_n$  for  $n \geq 5$ ) and an additional 26 *sporadic* groups fitting no specific criterion. There are a variety of tests for nonsimplicity. We know that  $n$  is not the order of a simple group if either of the following hold:

- **(Sylow Test)**  $p|n$  and 1 is the only divisor of  $n$  which is  $\equiv 1 \pmod p$  (proved using Sylow's Third Theorem and the fact that prime power groups have nontrivial centers);
- **(2\*Odd Test)**  $n = 2m$  with  $m > 1$  odd (proved using Cayley's Theorem).

Cayley's Theorem on permutations can be generalized to the following: if  $H < G$  and  $S$  is the group of permutations of left cosets of  $H$  in  $G$ , then there is a homomorphism  $G \rightarrow S$  whose kernel is in  $H$  and contains every normal subgroup of  $G$  that is also in  $H$ . This result gives two more tests:

- **(Index Test)** if  $G$  is a finite group and  $H < G$  with  $|G|$  not dividing  $|G : H|!$ , then  $H$  contains a nontrivial normal subgroup and is not simple;
- **(Embedding Test)** if a finite non-abelian group  $G$  with a subgroup of index  $n$  is not isomorphic to a subgroup of  $A_n$ , then it is not simple.

A simple application of these four tests shows that the only possible orders less than 200 for a non-abelian simple group are 60, 72, 112, 120, 144, 168, and 180. Of these, only 60 and 168 actually correspond to simple groups. The others may be eliminated with some work. In the case of 72, Sylow's Third Theorem implies that there are either 1 or 4 Sylow 3-subgroups. The first case would imply a normal subgroup, so  $n_3 = 4 = |G : N(H)|$ . But then  $G$  cannot be simple by the Index Test, since  $|G|$  does not divide  $4!$ . The order 60 simple group is  $A_5$ , which may be proven to be simple by eliminating also possible orders for subgroups.

### 3 Rings

Having studied sets with one operation, it is time to move on to sets with two operations, called *rings*:

**Ring:** a set  $R$  with two operations  $+$  and  $*$  (usually suppressed) such that:

- (1)  $R$  is an abelian group under  $+$ ;
- (2)  $R$  is associative under  $*$ ;
- (3)  $R$  is **distributive**, meaning  $a(b + c) = ab + ac$ .

The additive identity is denoted 0. If  $ab = ba$ ,  $R$  is a **commutative ring**, and if there is a multiplicative identity 1,  $R$  is a **ring with unity**. A commutative ring with unity which is an abelian group under  $*$ , excluding 0, is called a **field**.

In a ring with unity, elements with multiplicative inverses are called **units**, so in a field every element but 0 is a unit. As with groups, inverses and identities, if they exist, are unique.

Examples of rings include:

- $\mathbb{Z}$ : commutative with unity, units  $\pm 1$ ;
- $\mathbb{Z}_n$ : commutative with unity, units  $U(n)$ ;
- $\mathbb{Z}[x]$  (polynomials in  $x$  with integer coefficients): commutative with unity, units  $\pm 1$ ;
- $M_2(\mathbb{Z})$  ( $2 \times 2$  integer matrices): noncommutative with unity  $[10; 01]$ ;
- $2\mathbb{Z}$  (even integers): commutative without unity.

The **characteristic** of a ring is the smallest integer  $n$  such that  $na = 0$  for all  $a \in R$ . or 0 if no such exists. If a unity exists, it is just the order of the unity (or 0 if infinite order). All of the above examples except  $\mathbb{Z}_n$  have characteristic 0;  $\mathbb{Z}_n$  has characteristic  $n$ .

### 3.1 Subrings

**Subrings** are subsets of rings that are themselves subrings; equivalently they are closed under subtraction and multiplication. For example,  $\mathbb{Q}$  is a subring of  $\mathbb{R}$ , and  $2\mathbb{Z}$  is a subring of  $\mathbb{Z}$ . Actually,  $R$  is always a subring of  $R[\diamond]$ , the set  $a_0 + a_1\diamond + a_2\diamond^2 + \dots$  with  $a_i \in R$ , called  $R$  with  $\diamond$  adjoined. Elements of  $R[\diamond]$  are denoted  $f(\diamond)$ , but it is important to note that they are not actual functions; they could just as easily be described by  $[a_0, a_1, \dots]$ . One example is  $\mathbb{Z}[x]$  above; more generally, the set of polynomials in  $x$  with coefficients in any ring is itself a ring. One may also consider the case with some  $\diamond^k \in R$ , such as the Gaussian Integers  $\mathbb{Z}[i]$  where  $i^2 = -1$ . This notation is extremely important for rings.

In the study of abstract algebra, things such as subgroups/subrings are repeated in different contexts, although the ideas are very similar. Another example is direct sum, which carries over directly to rings.

### 3.2 Ideals and Factor Rings

With groups, we needed a *normal subgroup* to form a factor group; with rings, we need a:

**(2-sided) Ideal:** a subring  $A$  of  $R$  with  $ra, ar \in A$  for all  $a \in A, r \in R$ . This gives a well-defined **factor ring**  $R/A$ .

Any element  $a \in R$  generates a **principal ideal**  $\langle a \rangle = \{ar, ra : r \in R\}$ .

For example,  $\mathbb{Z}/4\mathbb{Z}$  is a factor ring, as is  $M_2(\mathbb{Z})/M_2(2\mathbb{Z})$ , where  $M_2(2\mathbb{Z})$  is the set of  $2 \times 2$  matrices with even integer entries.  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$  is an example of a factor ring formed from a principal ideal. It can be thought of as polynomials with real coefficients and the relation  $x^2 = -1$ , and is thus equivalent to the complex ring  $\mathbb{C}$ .

A **prime ideal** is one with  $ab \in A$  implying either  $a \in A$  or  $b \in A$ . This is a similar notion to prime numbers; indeed,  $\mathbb{Z}_n$  is a prime ideal of  $\mathbb{Z}$  iff  $n$  is prime. A **maximal ideal** is a proper ideal  $A$  such that if  $A \subseteq B \subseteq R$  for another ideal  $B$ , then either  $B = A$  or  $B = R$ . The ideal  $\langle x^2 + 1 \rangle$  in  $\mathbb{R}[x]$  is an example of a maximal ideal. These ideals are important because  $R/A$  is a field iff  $A$  is maximal, and an integral domain (the topic of the next section) iff  $A$  is prime.

### 3.3 Integral Domains

An *integral domain* is one of many types of rings with a specific structure, in this case meant to ensure behavior like the integers (hence the name):

**Integral Domain:** a commutative ring with unity and no *zero divisors* (elements with  $ab = 0$ ); equivalently, the cancellation laws  $ab = ac \implies b = c$  and  $ba = ca \implies b = c$  hold.

Integral domains have characteristic 0 or  $p$  prime.

Examples of integral domains include  $\mathbb{Z}_3[i]$  and  $\mathbb{Q}[\sqrt{2}]$  (recall this notation from the previous section). The first is also a field, as all finite integral domains are fields. Finite fields, such as this and  $\mathbb{Z}_p$ , are extremely well-known.

For every integral domain  $D$ , there is a field  $F$  with  $D$  as a subring, called the **field of quotients**, the analog of the rationals for integers. As can be expected,  $F$  is constructed by looking at all pairs (quotients) of elements of  $D$  and an appropriate equivalence relation.

The study of polynomials is central to ring theory. A ring of polynomials  $D[x]$  over an integral domain  $D$  is itself an integral domain. Working in an integral domains allows us to say that if  $(x - a)(x - b) = 0$ , then either  $x = a$  or  $x = b$ ; this is not always the case in a ring with zero divisors. If  $D$  is a field, then one has a division algorithm in  $D[x]$ , and polynomials are factored in the usual manner.

A **principal ideal domain**, or **PID**, is one in which every ideal is principal, i.e., of the form  $\langle a \rangle = \{ra : r \in D\}$  for some  $a$ . The polynomials  $F[x]$  over a field form a PID. In fact, an ideal  $I$  of  $F[x]$  is generated by precisely the polynomials  $g(x)$  of minimal degree in  $I$ .

Integral domains also lack **nilpotent** elements ( $a^n = 0$  for some  $n$ ) and **idempotent** elements ( $a^2 = a$ ), except for the special elements 0 and 1.

### 3.4 Ring Homomorphisms and Isomorphisms

Ring homomorphisms preserve both group operations, rather than just one, and isomorphisms are still the bijective homomorphisms. One example is the *evaluation homomorphism* from  $\mathbb{R}[x]$  to  $\mathbb{R}$  given by  $f(x) \mapsto f(1)$ .

Analogous to the situation for groups, kernels of homomorphisms are ideals, and all ideals are kernels of some ring homomorphism. We also have:

**First Isomorphism Theorem for Rings:** Given a ring homomorphism  $\phi : R \rightarrow S$ , we have an isomorphism  $R/\ker\phi \cong \phi(R)$  given by the map  $r + \ker\phi \mapsto \phi(r)$ .

Thus, for example,  $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ . Since  $\mathbb{Z}$  is an integral domain but not a field, we see (from the previous section) that  $\langle x \rangle$  is a prime but not maximal ideal.

One important homomorphism is the map  $\phi : \mathbb{Z} \rightarrow R$  taking  $n \mapsto ne$ , where  $e \in R$  is the unity. This implies that every ring with unity has a subring isomorphic to either  $\mathbb{Z}$  or  $\mathbb{Z}_n$ ; which depends on whether the characteristic is 0 or positive. Analogously, a field always has a subfield isomorphic to either  $\mathbb{Q}$  or  $\mathbb{Z}_n$ , again depending on the characteristic. This subfield is actually the intersection of all nontrivial subfields, and called the **prime subfield**.

### 3.5 More on Polynomial Rings

Polynomials are widely studied in ring theory because they are the simplest generalization of the integers, with many properties carrying over. We'll see that integral domains, in general, have many of the same properties.

Over an integral domain  $d$ , an **irreducible polynomial**  $f(x) \in D[x]$  is one for which  $f(x) = g(x)h(x)$  implies either  $g$  or  $h$  is a unit. (Otherwise, the polynomial is **reducible**.) In a field  $F$ , a polynomial of degree 2 or 3 is reducible iff it has a zero in  $F$ .

A **primitive polynomial**  $f(x) \in \mathbb{Z}[x]$  is one with no common factor among its coefficients. The product of two primitive polynomials is also primitive (the *Gauss Lemma*). This property is mostly just used to simplify proofs.

If a polynomial in  $\mathbb{Z}[x]$  is reducible over  $\mathbb{Q}$ , then it is also reducible over  $\mathbb{Z}$ ; equivalently, if it is irreducible over  $\mathbb{Z}$ , then it is irreducible over  $\mathbb{Q}$ . Hinting at some properties we'll see later, every polynomial of degree  $> 1$  is reducible over some (extension) field. Actually, every polynomial  $\mathbb{Z}[x]$  can be uniquely factored into a product of nonunits of degree 0 and irreducible polynomials, similar to the unique factorization of integers.

Here are a few tests for irreducibility over  $\mathbb{Z}[x]$ . First, given a prime  $p$ , a polynomial  $f(x) \in \mathbb{Z}[x]$  gives a unique polynomial  $\bar{f}(x) \in \mathbb{Z}_p[x]$ , found by reducing the coefficients mod  $p$ . If this polynomial has the same degree and is irreducible over  $\mathbb{Z}_p$ , then  $f(x)$  is irreducible over  $\mathbb{Z}$ . Second, the **Eisenstein criterion** states that if  $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$  and some prime  $p$  divides  $a_0, \dots, a_{n-1}$  but  $p \nmid a_n$  and  $p^2 \nmid a_0$ , then  $f$  is irreducible over  $\mathbb{Q}$ . Thus, for example, the *cyclotomic polynomial*  $\Phi_p(x) = x^{p-1} + \dots + x + 1$  is irreducible over  $\mathbb{Q}$ , for  $p$  prime.

In a field,  $p(x)$  is irreducible iff  $\langle p(x) \rangle$  is a maximal ideal; hence, in this case,  $F[x]/\langle p(x) \rangle$  is also a field. This gives a way to construct fields. A simple consequence of this result is that for irreducible  $p(x) \mid a(x)b(x)$ , one must have either  $p(x) \mid a(x)$  or  $p(x) \mid b(x)$ .

### 3.6 General Integral Domains

The properties of the integers and polynomials often carry over to general integral domains. In place of prime numbers/irreducible polynomials, an **irreducible element**  $a \in D$  is one for which  $a = bc$  implies either  $b$  or  $c$  is a unit; a **prime element**  $a \in D$  is one for which  $a \mid bc$  implies either  $a \mid b$  or  $a \mid c$  (which happens iff  $\langle a \rangle$  is a prime ideal). These definitions are rather

similar, and all prime elements are irreducible. In  $\mathbb{Z}[\sqrt{-3}]$ , however, the element  $1 + \sqrt{-3}$  is irreducible but not prime. However, in a PID, elements are irreducible iff they are prime.

We now introduce a few more classes of integral domains. Unique factorization holds in all PIDs; a general integral domain with this property is called a **Unique Factorization Domain**, or UFD. Thus, for example, unique factorization holds in  $F[x]$  for  $F$  a field (and if  $D$  is a UFD, then  $D[x]$  is also a UFD). The proof that every PID is a UFD uses the fact that a strictly increasing chain of ideals  $I_1 \subset I_2 \subset \dots$  in a PID must be finite (this property in general is what characterizes a **Noetherian Domain**).

Another class of PID is the **Euclidean domain**, basically an integral domain with a division algorithm. Precisely, given the ED  $D$ , one has a function  $d : D^* \rightarrow \mathbb{Z}_0^+$  from the nonzero elements to the nonnegative integers such that whenever  $d(a) \leq d(ab)$  and  $b \neq 0$  one has  $q, r \in D$  such that  $a = bq + r$  and  $d(r) < d(b)$ . The obvious prototype is  $\mathbb{Z}$ , with  $d(a) = |a|$ ; a less obvious example is  $F[x]$  with  $d(f(x)) = \deg f(x)$ . (Actually, there are a remarkable number of similarities between  $\mathbb{Z}$  and  $F[x]$ .) In one diagram, we have

$$ED \implies PID \implies UFD,$$

although the reverse implications are not true.

## 4 Fields

### 4.1 Vector Spaces

Recall that fields are rings with dual abelian group structures, one under each operation. Vector spaces are constructed from a base field:

**Vector Space  $V$  (over a field  $F$ ):** a space  $V$  with a map  $F \times V \rightarrow V$  such that for  $a, b \in F$  and  $u, v \in V$  one has  $a(u + v) = au + av$ ,  $(a + b)v = av + bv$ ,  $a(bv) = (ab)v$ , and  $1v = v$ .

One has, of course *scalars* in  $F$  and *vectors* in  $V$ . A few examples include  $\mathbb{R}^n$ , the matrix group  $M_2(\mathbb{Q})$ , and  $\mathbb{Z}_p[x]$  for  $p$  prime (its basis is  $\{1, x, \dots, x^{p-1}\}$ ). Notions such as *subspace*, *linear dependence/independence*, *basis*, *dimension*, *linear combination*, and *span* carry over from linear algebra. It is true in general that a basis for a vector space always has the same number of elements.

### 4.2 Extension Fields

An **extension field  $E$  of  $F$**  is the opposite of a subfield, namely a field  $E \supset F$  containing  $F$ . The **Fundamental Theorem of Field Theory** states that for any polynomial  $f(x) \in F[x]$ , there exists an extension field  $E \supset F$  in which  $f$  has a zero. The proof is constructive, basically taking  $E = F[x]/\langle f(x) \rangle$ . More generally, a **splitting field  $E$  for  $f(x)$  over  $F$**  is one which contains all zeros of  $f$  (equivalently, one in which  $f$  may be factored into a product of linear factors; thus, it “splits”). An example is the polynomial  $f(x) = x^2 + 1 \in \mathbb{Q}[x]$ , which splits over  $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$  (or over  $\mathbb{C}$  if we consider  $f(x) \in \mathbb{R}[x]$ ).

This gives rise to the notation  $F(a_1, \dots, a_n)$ , defined to be the smallest extension of  $F$  containing all  $a_i$ . Indeed, this field is the splitting field for  $f(x) = b \prod (x - a_i)$ . Note that parentheses are used to indicate a field. We have the following results:

- Every polynomial has a splitting field;
- Given an irreducible polynomial  $p(x) \in F[x]$ , with a zero  $a$  in an extension field of  $F$ , then  $F(a) \cong F[x]/\langle p(x) \rangle$ , and the elements of  $F(a)$  can be expressed uniquely as polynomials of degree less than  $\deg p(x)$ ;
- In the above case, if  $a$  and  $b$  are both zeros of  $f$ , then  $F(a) \cong F(b)$ ;
- Splitting fields are unique up to isomorphism.

### 4.3 Algebraic Extensions

An element  $a \in E \supset F$  which is a zero of a polynomial in  $F[x]$  is said to be **algebraic over  $F$** ; other elements are **transcendental**. The standard examples are  $\sqrt{2}$ , an algebraic element over  $\mathbb{Q}$ , versus  $\pi$ , which is transcendental. If every element of an extension field  $E$  is algebraic,  $E$  is an **algebraic extension**.

An extension  $F(a)$  generated by a single element is a **simple extension**. Actually, all finite extensions over a field of characteristic 0 are simple. An element  $a$  of an extension  $E \supset F$  which generates that extension (so  $E \cong F(a)$ ) is called a **primitive element**.

If  $a$  is transcendental, then  $F(a) \cong F(x)$ , the field of quotients. Otherwise,  $a$  is algebraic and  $F(a) \cong F[x]/\langle p(x) \rangle$ , where  $p(x)$  is irreducible over  $F$  and  $p(a) = 0$ . In fact,  $p$  is unique if taken to be monic (and divides any other polynomial  $f(x)$  with  $f(a) = 0$ ).

Every extension  $E \supset F$  has a subfield consisting of all algebraic elements over  $F$ , called the **algebraic closure of  $F$  in  $E$** . An **algebraically closed field** is one with no proper algebraic extensions, such as  $\mathbb{C}$ , so that every polynomial has its zeros in the field.

The **degree of an extension  $E \supset F$**  is the dimension of  $E$  considered as a vector space over  $F$  (or  $\infty$  if the extension is transcendental), and denoted  $[E : F]$ . Actually, the degree of  $F(a) \supset F$  is just the degree of the minimal polynomial. For  $K \supset E \supset F$ , the degrees satisfy  $[K : F] = [K : E][E : F]$ .

### 4.4 Finite Fields

As may be expected, finite fields are as easy to classify as finite abelian groups: there is a unique field  $GF(p^n)$  of order  $p^n$ , called the *Galois field*, and these are the only finite fields. As an additive group,  $GF(p^n) \cong \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ , and as a multiplicative group,  $GF(p^n)^*$  is cyclic and isomorphic to  $\mathbb{Z}_{p^n-1}$ . The degree of  $GF(p^n)$  over  $GF(p)$  is  $n$ , and a generator of  $GF(p^n)^*$  is algebraic over  $GF(p)$  with degree  $n$ . The field  $GF(p^n)$  has a unique subfield of order  $p^m$  for every  $m|n$ , and these are the only subfields. An example is  $GF(16)$ , which may be constructed as  $\{a_3x^3 + a_2x^2 + a_1x + a_0 + \langle x^4 + x + 1 \rangle : a_i \in \mathbb{Z}_2\}$ , with generator  $x$ .

One example is  $GF(16)$ , which may be realized as the polynomial group  $\{a_3x^3 + a_2x^2 + a_1x + a_0 + \langle x^4 + x + 1 \rangle : a_i \in \mathbb{Z}_2\}$ , and is generated by  $x$ .

### 4.5 Galois Theory

We now explore the relationship between extensions of fields and groups given by Galois Theory, originally used to prove the insolvability of the quintic, i.e., the nonexistence of an algebraic formula giving the roots of a fifth-order polynomial. We have:

**Galois Group  $\text{Gal}(E/F)$** : for a field extension  $E > F$ , it is the group of automorphisms of  $E$  which fix every element of  $F$ .

We also define the **fixed field  $E_H$**  of a group  $H < \text{Gal}(E/F)$  as the set of elements  $x \in E$  fixed by every automorphism in  $H$ .

There is a remarkable relationship between the subgroups of  $\text{Gal}(E/F)$  and the extension fields  $K$  with  $E > K > F$  encapsulating the **Fundamental Theorem of Galois Theory**: when  $F$  is a field of characteristic 0 or finite and  $E$  is a splitting field of a polynomial in  $F[x]$ , then the map from the set of subfields  $K$  with  $E > K > F$  to the set of subgroups of  $\text{Gal}(E/F)$  given by  $K \mapsto \text{Gal}(E/K)$  is a 1 : 1 correspondence. We also have:

- The index  $[E : K]$  of  $E$  over  $K$  as a vector field equals  $|\text{Gal}(E/K)|$  and  $[K : F] = |\text{Gal}(E/F)|/|\text{Gal}(E/K)|$ ;
- If  $K$  is the splitting field of a polynomial in  $F[x]$  and  $\text{Gal}(E/K) \triangleleft \text{Gal}(E/F)$ , then  $\text{Gal}(K/F) \cong \text{Gal}(E/F)/\text{Gal}(E/K)$ ;
- The fixed field of  $\text{Gal}(E/K)$  is  $E_{\text{Gal}(E/K)} = K$ , and for  $H < \text{Gal}(E/F)$  we have  $H = \text{Gal}(E/E_H)$ .

Let's look at some examples. The simplest **Galois extensions**, those satisfying the requirements in the above theorem, are those adjoining a root of a polynomial. The extension  $\mathbb{Q}(\sqrt{2})$  of  $\mathbb{Q}$  can be viewed as  $\{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ , and the Galois group  $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$  is  $\mathbb{Z}_2$ , with the nonidentity automorphism taking  $\sqrt{2} \mapsto -\sqrt{2}$ . The fixed field of  $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$  is  $\mathbb{Q}$ , as must be the case since any automorphism must fix  $\mathbb{Q}$ . A second example is the extension  $\mathbb{Q}(\omega, \sqrt[3]{2})$  with  $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$  a root of  $x^3 - 1$ . The Galois group in this case is actually  $S^3$  and thus non-abelian.

A more general example is the extension  $GF(p^n)$  of  $F = GF(p)$ . This can actually be viewed as  $F(b)$ , where  $b$  is the zero of some irreducible degree  $n$  polynomial  $p(x) \in F[x]$ . Any automorphism of  $GF(p^n)$  fixes 1 and therefore  $GF(p)$  as well. So if  $p(b) = 0$  then  $p(\phi(b)) = 0$ . Thus, there are at most  $n$  possibilities for  $\phi(b)$ . On the other hand the map  $a \mapsto a^p$  is an automorphism of  $E$  with order  $n$  (since  $GF(p^n)^*$  is cyclic). Therefore,  $\text{Gal}(GF(p^n)/GF(p)) \cong \mathbb{Z}_n$ .

To prove insolvability of the quintic, we must give a precise definition of solvable: we say that  $f(x) \in F[x]$  is **solvable by radicals** if it splits in some extension  $F(a_1, \dots, a_n)$  and there exist  $k_i \in \mathbb{Z}^+$  such that  $a_i^{k_i} \in F(a_1, \dots, a_{i-1})$ ; basically, it means one can obtain all the zeros of  $f$  by adjoining  $n$ th roots. A condition which will then hold for the Galois group is:

**Solvable group  $G$ :** there exists a series  $\{e\} = H_0 \subset H_1 \subset \dots \subset H_k = G$  such that  $H_i \triangleleft H_{i+1}$  and each  $H_{i+1}/H_i$  is abelian.

If a function  $f(x) \in F[x]$  is solvable by radicals, and  $E$  is the splitting field of  $f$  over  $F$ , then  $\text{Gal}(E/F)$  is a solvable group. This is basically proven using induction, and the converse is actually true as well. One can show that the Galois group of  $3x^5 - 15x + 5$  is  $S^5$ , which is not solvable. Thus, the polynomial is not solvable by radicals, and so there is no formula for the general quintic.

## 5 The Road Ahead

There are a number of structures that come into the picture in more advanced abstract algebra. The most useful is probably the **module**, which is a generalization of a vector space, this time over a ring. It also generalizes the notion of a group acting on a set (like a permutation group). All groups are modules, and many theorems for groups (like the classification of finite abelian ones) carry over to modules. There is also the **algebra**, which one can think of as a ring with a little less structure.

One also encounters a good deal of **category theory**. Categories specify which structure one is working with, and often theorems can be phrased in terms of category theory so as to encompass several structures. It is especially useful for modules, and allows the introduction of tensor products (generalized linear algebra). Category theory is ubiquitous in mathematics.

Finally, there are **representations**. One can think of a representation of a group as a homomorphism from a group to a matrix group. The properties of the trace of this map's image give a great deal of information about the group itself. Representation theory also happens to be used everywhere in mathematics.

Finally, although outside a strict Algebra course, the notions of the **Lie group** and the **Lie algebra** are also paramount. A Lie group is a group with a differential structure, or equivalently a manifold with a group structure. A Lie algebra is an algebra with an anti-commutative product  $[X, Y] = -[Y, X]$ . Lie algebras can be completely classified, and, amazingly, there is a close correspondence between Lie groups and Lie algebras; with a few minor conditions on the Lie group, there is in fact a 1 : 1 correspondence. Lie theory lies at the intersection of geometry, topology, and algebra, and therefore is used by almost all mathematicians.