Field Theory

Amol Jain

Long Island Mathematics Fair 2005

1 Introductory Number Theory

1.1 Functions

A function f maps each element a in a set A to a unique element b in a set B. For all $a \in A$, the unique element b is represented as $f(a)$. The notation $f : A \to B$ indicates that f maps elements of set A into set B.

An example of such would be a function $f : \mathbb{Z} \to \mathbb{Z}$ (where $\mathbb{Z}$ is the set of integers) that is defined as $f(x) = x - 2$. Using this function, $f(9) = 7$.

1.1.1 Composition of Functions

Let $f : A \to B$ and $g : B \to C$ be functions. We can then note the composition of f and g as $g \circ f$, or simply h, an entirely new function where $h : A \to C$. $h(x)$ is therefore the equivalent of $g(f(x))$.

For instance, let $f : \mathbb{Z} \to \mathbb{N}$ (where $\mathbb{N}$ is the set of natural numbers) be defined as $f(x) = x^4$ and $g : \mathbb{N} \to \mathbb{Z}$ be defined as $g(y) = 8 - y^3$. The composition of the two functions maps from integers to integers: $g \circ f : \mathbb{Z} \to \mathbb{Z}$. The function derived from the composition $h(x)$ may be written as follows: $h(x) = g(f(x)) = g(x^4) = 8 - x^{12}$ (RSA Laboratories).

1.2 Modular Arithmetic

1.2.1 The Modulus

The best analogue to modular arithmetic is a comparison standard 12-hour clock and a military clock. Both clocks read the same time throughout the morning until an hour after noon, when they diverge. The military clock reads 13:00, while the standard clock reads 1:00. The standard clock essentially wraps around every 12 hours to its initial position.

This concept was first introduced by Gauss in the 19th century through what he described as a modulus, a distinct value after which numbers would wrap around. In the aforementioned example, the modulus would be 12. The notation for this is as follows:

Given integers a, b, and n ($n > 0$), if $n \mid a - b$ (notation for n divides $a - b$ or $\frac{a-b}{n} \in \mathbb{Z}$), then a and b are considered congruent modulo n. This is written as $a \equiv b \pmod{n}$, where n is the modulus.

For example, $8 \equiv 3 \pmod{5}$ because $8 - 3$ is divisible by 5.

1.2.2 Properties of Modular Arithmetic

If a, b, c, and d are integers such that $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then

$$a + b \equiv c + d \pmod{n}$$

and

$$ab \equiv cd \pmod{n}$$

Furthermore, using the modulus n, it is possible to create congruence classes of integers (RSA Laboratories). In other words, for an integer a, its congruence class contains all other integers which are equivalent to a modulo n. The set of such integers is written as $[a]$ where

$$[a] := a + n\mathbb{Z} = \{\ldots, a - 2n, a - n, a, a + n, a + 2n, \ldots\}$$

For example, if $a = 12$ and $n = 7$, then the congruence class for 12 modulo 7 would be the set $\{\ldots, -2, 5, 12, 19, 26, \ldots\}$. This means that we could write $12 \equiv -1 \pmod{7}$, $12 \equiv 5 \pmod{7}$, $12 \equiv 12 \pmod{7}$, etc.

Addition and multiplication of congruence classes is fairly straightforward. It is defined that $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [ab]$.

It simplifies arithmetic if we represent a with the smallest nonnegative number a_r present in the congruence class $[a]$. Examining the example above once more, we see that $a = 12$ and $[a] := \{\ldots, -2, 5, 12, 19, 26, \ldots\}$. Thus, $a_r = 5$ because 5 is the smallest nonnegative element of $[a]$.

Furthermore, $\mathbb{Z}_n$ is defined to represent the set of congruence classes modulo n. Meaning for all integers a and their respective congruence classes $[a]$, we take the unique a_r for the set $\mathbb{Z}_n$. Consider, for example $\mathbb{Z}_6$. Find the congruence classes of all elements in the set $\{\ldots, -1, 0, 1, \ldots\}$. For $a = -1$, we would have $\{\ldots, -5, -1, 3, \ldots\}$, $a = 0$ would yield $\{\ldots, -4, 0, 4, \ldots\}$, and $a = 1$ would give $\{\ldots, -3, 1, 5, \ldots\}$. The a_r for these congruence classes would be 3, 0, and 1 respectively. Continuing this for all a, we would find that $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. This is generalized to $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$.

In addition, $\mathbb{Z}_n^*$ is defined to be the set of congruence classes modulo n, or a_r, that are elements of the set $\{1, \ldots, n-1\}$ such that $\gcd(a_r, n) = 1$. Another way of saying this is to define $\mathbb{Z}_n^*$ as the set of all relatively prime numbers to n. Thus $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$.

2 Groups

2.1 Addition in $\mathbb{Z}_p$ and Multiplication in $\mathbb{Z}_p^*$

There are special properties of addition in $\mathbb{Z}_p$ and multiplication in $\mathbb{Z}_p*$ where p is a prime number.

In $\mathbb{Z}_p$:

1. Addition is associative.
$$a + (b + c) = (a + b) + c$$
2. There exists an additive identity element 0, such that for all a
$$a + 0 = 0 + a = a$$
3. For all $a \in \mathbb{Z}_p$, there exists b such that $a + b = 0$, where $b = -a$ and $-a$ is the additive inverse of a.

In $\mathbb{Z}_p^*$:

1. Multiplication is associative.
$$a(bc) = (ab)c$$
2. There exists a multiplicative identity element 1, such that for all a
$$a \cdot 1 = 1 \cdot 1 = a$$
3. For all $a \in \mathbb{Z}_p^*$, there exists an integer b such that $ab = 1$, where $b = a^{-1}$ and a^{-1} is the multiplicative inverse.

2.2 Properties of Groups

Sets with properties like those described above are considered groups. A more formal definition is as follows:

A group is comprised of a set G, which may be finite or infinite, and a binary operation $*$, where $* : G \times G \to G$. This means that the set G is closed under the operator $*$ because G

is mapped back onto G. Thus for any a, $b \in G$, $a * b \in G$ as well. In addition, a group must satisfy the now generalized axioms below:

1. The operation $*$ is associative.

$$a * (b * c) = (a * b) * c$$

2. There exists an identity element $e \in G$, such that for all $a \in G$

$$a * e = e * a = a$$

3. For all $a \in G$, there exists an inverse $b \in G$ (also denoted a^{-1}), such that $a*b = b*a = e$.

If the operation $*$ is also commutative, meaning $a * b = b * a$ for all a,$b \in G$, then the group is said to be abelian (Weisstein, Groups).

2.3 Theorems and Proofs

2.3.1 The identity element of a group is unique.

This can be rephrased as follows: If $a \in G$ has the property such that for some other element $x \in G$, $a * x = x * a = x$ then a is the identity element.

Proof Consider a member $x \in G$ such that $a * x = x$. Because G is a group, every member in it has an inverse. Furthermore, the group is closed under multiplication. Thus we have

$$(a * x) * x^{-1} = x * x^{-1}$$

We can use the associative property on the left side and the inverse property on the right to yield

$$a * (x * x^{-1}) = e$$

And again applying the inverse axiom:

$$a * e = e$$

Using the identity axiom, we finally prove the theorem:

$$a = e$$

2.3.2 If $a * x = b * x$, then $a = b$

This is known as the right cancellation law, because the x on the right-hand side is being "canceled."

Proof

$$a * x = b * x$$

$$(a * x) * x^{-1} = (b * x) * x^{-1}$$

$$a * (x * x^{-1}) = b * (x * x^{-1})$$

$$a * e = b * e$$

$$a = b$$

2.3.3 If $x * a = x * b$ then $a = b$

This is known as the left cancellation law.

Proof

$$x * a = x * b$$

$$x^{-1} * (x * a) = x^{-1} * (x * b)$$

$$(x^{-1} * x) * a = (x^{-1} * x) * b$$

$$e * a = e * b$$

$$a = b$$

2.3.4 The inverse of $a * b$ is $b^{-1} * a^{-1}$

If $b^{-1} * a^{-1}$ is the inverse of $a * b$ then when operated on by $*$, the returned value should be e, the identity element.

Proof

$$(a * b) * (b^{-1} * a^{-1})$$

$$= a * [b * (b^{-1} * a^{-1})]$$

$$= a * [(b * b^{-1}) * a^{-1}]$$

$$= a * (e * a^{-1})$$

$$= a * a^{-1}$$

$$= e$$

2.3.5 If a and b are elements of a group and $a * b = e$, then $a = b^{-1}$

Proof

$$a * b = e$$

$$a^{-1} * (a * b) = a^{-1} * e$$

$$(a^{-1} * a) * b = a^{-1} * e$$

$$e * b = a^{-1} * e$$

$$b = a^{-1}$$

2.3.6 $(a^{-1})^{-1} = a$

Proof

$$a^{-1} * a = e$$

We now use the theorem above by letting $a = a^{-1}$ and $b = a$. Substituting, it follows that

$$a = (a^{-1})^{-1}$$

2.4 Cayley Tables

One of the most familiar instances of Cayley tables is one that many have seen in elementary school: the multiplication table (Dogfrey).

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	6	8
3	0	3	6	9	12
4	0	4	8	12	16

One can find the product of 2 and 3 by finding 2 on the left side and 3 on the top side and finding where their respective row and column intersect. In this case, they coincide at the number 6, meaning that $2 \times 3 = 6$.

2.4.1 Cayley Tables and Groups

Cayley tables can also be used to represent groups. Suppose we have a set of commands we can give to a soldier (Dogfrey):

- Stand at **A**ttention
- **R**ightface
- **L**eftface
- A**b**outface

Accompanying this set of commands we have the operator “followed by.” For instance, one could issue the following command to the soldier:

“Rightface followed by Aboutface!”

The soldier would then turn to his right and then turn completely around. This command would be the equivalent of a simple “Leftface!”

Suppose the solider were told,

“Stand at Attention followed by Rightface!”

“Stand at Attention” thus functions like an identity element. To verify whether or not these commands and the operator form a group, we can construct a Cayley table. The commands have been abbreviated to form the set $\{A, R, L, B\}$. The letters correspond to the bolded characters in the list of commands above. Similarly, the operator “followed by” has been replaced with $*$.

$*$	A	R	L	B
A	A	R	L	B
R	R	B	A	L
L	L	A	B	R
B	B	L	R	A

To find the result of “About face followed by Leftface!” we have to use the table and look up $A * L$. The result is R or “Rightface!”

There are several observations worth making here. First, the table is symmetrical with respect to the main diagonal. This indicates commutativity and labels this set an abelian group. Also A is the identity element because the A row is identical to the top reference row, and the A column is identical to the reference column on the left. It is also significant that the identity element is in each row and each column exactly once, meaning that for every element a there is an element b such that $a * b = A$. The symmetrical distribution of the identity elements is a testament to the third property of groups: there exists an inverse such that $a * b = b * a = e$, where it does not matter which side the inverse is on.

Every row and every column contains each element of the group precisely one time. This is due to conformity to the cancellation laws. For example, if R appeared two times in the B row, once in the L and B columns, we could say

$$B * L = R$$

and

$$B * B = R$$

Substituting, we get

$$B * L = B * R$$

Using the left cancellation law, $L = R$, which is clearly not true. Likewise, repeating elements in columns would violate the right cancellation law. We can therefore deduce that if a Cayley table is to be a group, it cannot contain the same element twice in any row or column.

2.4.2 Variations of the Soldier Example

It should be noted that although Cayley tables may differ in the way they appear, that does not necessarily mean that they are representations of different groups. Take, for example, the subsequent table:

$*$	A	B	R	L
A	A	B	R	L
B	B	A	L	R
R	R	L	B	A
L	L	R	A	B

This table is also an accurate depiction of the group of commands and operator that were given to the soldier. The only difference is the order of the columns and rows. In order for the two groups to truly be the same, however, all products between the two tables must be the same.

2.4.3 Isomorphisms of Groups

The symbols $\{A, B, R, L\}$ used for the group could have been changed to anything else as long as the structure of the table remained the same. The following is a Cayley table for the group consisting of $\{1, -1, i, -i\}$.

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Although the soldier group and this group, consisting of real and imaginary number, are different, they can be described via the same Cayley table. The two groups have the same shape and structure, meaning that they are isomorphisms of one another (Dogfrey).

2.5 Subgroups

If we took two elements from the soldier group, “Attention!” and “Aboutface!” it would yield the following Cayley table:

$*$	A	B
A	A	B
B	B	A

This table is simply the top left corner of the variation for the soldier group’s Cayley table. It is also an instance of a subgroup.

A subset S is a subgroup of a group G if it satisfies the following:

1. S is closed under the operator for G
2. The identity element of G is also present in S
3. There exists an inverse a^{-1} for all $a \in S$

If G is truly a group, then S automatically inherits the associative property from G’s operator, and it does not have to be specifically enumerated among the prerequisites for a subgroup.

An example of a group and a subgroup is the set $\mathbb{Z}$ and the set of even integers under addition, respectively. Any even integer added to another yields another even integer. The identity element, 0, is present within the set of even integers. Finally, every even integer has its opposite, whose sum with itself is 0, the identity element. We can then conclude that even integers are indeed a subgroup of the set of integers.

Every group of two or more members contains at least two subgroups: the identity element and the group itself. These are known as trivial subgroups, and any other subgroups that the group has are known as nontrivial subgroups.

2.5.1 A finite subset of a group that is closed under the group operation is a subgroup of that group

In other words, if a finite subset of a group is closed, it is a subgroup that satisfies the other two axioms automatically.

Proof If one is to imagine a group as a Cayley table, we know that the cancellation laws restrict each element to appearing at most once in each row and column. As the subgroup is closed, each row and column contains the elements in the subset in some certain order. Thus for any $a \in S$, the row and column labeled a both contain a as well. This means that something, when multiplied by a, yields a itself, indicating the existence of an identity element, e. If e is in the subset, it must also show up once in every row and column. If e is in every row and column, that means that that for every a, there is another b (also known as a^{-1}) such that $a * b = e$. Finally, we now have a subset that is closed under the group's operator, an identity element, and inverses for every element. Therefore a finite subset of a group that is closed under the group operation is indeed a subgroup of that group.

An important distinction to make is that this only applies to finite subsets. For example, take the set of all positive integers. Although they are a subset of the group of integers under addition and are closed under the same operation, they do not form a subgroup of integers. This is because positive integers do not contain the additive identity element 0. In addition, it does not contain additive inverses of its elements either.

2.5.2 If S is a subset of a group G and if for every a and b in S the product $a * b^{-1}$ is in S, then S is a subgroup of G.

Proof Because $a*b^{-1} \in S$ for all a, $b \in S$, if we let $a = b$, then $a*a^{-1} \in S$. Since $a*a^{-1} = e$, we can say that e exists in S and $e \in G$. Since it has been established that $e \in S$ and $a \in S$, then there must be some inverse that when multiplied by a gives e. Finally, for a, $b \in S$, it is already stated in the premise that b^{-1} is in S. Since a and b^{-1} are present in S, if we let

$b = b^{-1}$, then it is given that $a * (b^{-1})^{-1} \in S$. From a previous proof, we know $(b^{-1})^{-1} = b$, and therefore $a * b \in S$, and S is closed.

2.6 Cosets

The subgroup of integers divisible by 3 can be written as follows:

$$\{\ldots, -9, -6, -3, -, 3, 6, 9, \ldots\}$$

. If we are to add 1 to all the integers in the set, a new subgroup is formed:

$$\{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$$

. Adding 2 to the original subgroup we achieve:

$$\{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

. Together, these three sets comprise the entire set of integers. Furthermore, if we take any a and b from one particular subset, then $a - b$ is a multiple of 3 and is also in the same subset.

Something similar happens with the second Cayley table for the soldier group. We already know that A and B form a subgroup. What is interesting, is that R and L form a coset of that subgroup, meaning that if an element of $\{R, L\}$ is multiplied by the inverse of any member of $\{R, L\}$ (in other words, either R or L, because they are inverses of each other), then the product is a member of the $\{A, B\}$ subgroup.

3 Fields

A field is a superset of a group and can be most essentially defined as an abelian group with two binary operations and the distributive property.

3.1 Field Axioms

A field F with operators $*$ (multiplicative) and $+$ (additive) must conform to the following properties where $a, b, c, e_1, e_2 \in F$:

1. Commutativity.
$$a + b = b + a$$
$$a * b = b * a$$

2. Associativity.
$$(a + b) + c = a + (b + c)$$
$$(a * b) * c = a * (b * c)$$

3. Distributivity.
$$a * (b + c) = a * b + a * c$$
$$(a + b) * c = a * c + b * c$$

4. Identity.
$$a + e_1 = e_1 + a = a$$
$$a * e_2 = e_2 * a = a$$

5. Inverse.
$$a + (-a) = -a + a = e_1$$
$$a * a^{-1} = a^{-1} * a = e_2 \ \ (a \neq 0)$$

The field described above could be written as (F,+,$*$). Examples of sets which would qualify as fields are complex numbers ($\mathbb{C}$), rational numbers ($\mathbb{Q}$), and real numbers ($\mathbb{R}$) (Weisstein, Fields).

3.2 Finite Fields

The groups mentioned thus far are all of infinite nature. Finite fields exist as well. Take, for example, the simplest instance of a finite field: $\mathbb{Z}_2 = \{0, 1\}$. Cayley tables can be used to verify this. Note that the operations are performed modulus 2.

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Addition and multiplication modulus tables can be sketched out to show that $\mathbb{Z}_3$ is a field as well, but $\mathbb{Z}_4$ is not. Perhaps we can generalize for which m $\mathbb{Z}_m$ is a field. In order to do this, we must perform two elementary proofs.

3.2.1 $a * e_1 = e_1$ for all $a \in F$, where F is a finite field and e_1 is the additive identity

Proof The additive identity e_1, when added to itself, returns itself, meaning $e_1 = e_1 + e_1$. We can therefore say

$$a * e_1 = a * (e_1 + e_1) = a * e_1 + a * e_1$$

$$a * e_1 + (-a * e_1) = a * e_1 + a * e_1 + (-a * e_1)$$

$$e_1 = a * e_1 + e_1)$$

$$e_1 = a * e_1)$$

3.2.2 $a * b = e_1 \rightarrow a = e_1 \vee b = e_1$, where F is a finite field and e_1 is the additive identity

Proof If it is given that $a * b = e_1$, then we want to demonstrate that if $a \neq e_1$, then $b = e_1$. By the inverse property, if $a \neq e_1$, then there exists c such that $c * a = e_2$. We can thus prove $b = e_1$ as follows:

$$b = e_2 * b = (c * a) * b = c * (a * b) = c * e_1 = e_1$$

If this is slightly confusing, consider substituting e_1 with 0, and e_2 with 1, and it may become clearer. Before we prove the next theorem, it is important to note that it is the nature of modulus arithmetic to remain consistent under the laws of commutativity, associativity, and distributivity. Thus, if one proves the existence of the additive and multiplicative identities along with the validity of the inverse law, one can declare some set $\mathbb{Z}_m$ a field.

3.2.3 $\mathbb{Z}_m$ is a field $\leftrightarrow m$ is prime

Proof First we assume that m is non-prime. If this is the case, $m = ab$ for $0 < a, b < m$ and $ab = 0 \pmod{m}$. If $ab = 0$ then $a = 0 \vee b = 0$ by the proofs above. However, this is contradictory to our establishment that $0 < a, b < m$. Therefore $\mathbb{Z}_m$, where m is non-prime is not a field. If gcd(a,m)= 1, then it is true that there exists a b such that $ab = ba = 1 \pmod{m}$, indicating that the inverse property holds. If m is prime, then for all $a \in \mathbb{Z}_m \;\; (a \neq 0)$, the gcd($a$,$m$)= 1, and $\mathbb{Z}_m$ is a field (Knudsen).

3.3 Fields and Polynomials

If F is a field, then $F[x]$ represents all polynomials of the variable x with coefficients in F. Let

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_mx^m$$

for $a_i \in F \;\; (i = 0, \ldots, m)$ and where $a_m \neq e_1$. The function f is then considered a polynomial over F of degree m.

If $F = 0, 1$, the coefficients of the polynomials in $F[x]$ are restricted to 0 and 1. Take $a(x), b(x) \in F[x]$ for the following examples.

Consider $a(x) = x^2+1$ and $b(x) = x^2+x+1$, then $a(x)+b(x) = x$. Adding the polynomials normally, we find that $a(x) + b(x) = 2x^2 + x + 2$. In the field $\{0, 1\}$, however, $1 + 1 = 0$, not 2, so the $2x^2$ and 2 terms drop out to leave a solitary x. Likewise, if $a(x) = x^3 + x^2$ and $b(x) = x^2 + 1$, then $a(x) + b(x) = x^3 + 1$.

Division of polynomials is possible as well. For instance, let $f(x), g(x), q(x), r(x)$ be polynomials over a field. We can say that $f(x)$ divides $g(x)$, if there is a $q(x)$ such that $g(x) = f(x)q(x)$. We can also say that $g(x) \equiv r(x) \pmod{f(x)}$ if and only if $f(x) \mid g(x) - r(x)$ (see modulus arithmetic). Furthermore, for every $f(x)$ and $g(x) \neq 0$, there are $q(x)$ and $r(x)$ such that $g(x) = f(x)q(x) + r(x)$, where the degree of r is less than the degree of f.

We previously defined $\mathbb{Z}_m$ to be the set of all natural numbers less than m. There is a similar definition for polynomials over a finite field. It is as follows: Let F be a finite field with $f(x) \in F[x]$. $F[x]/(f(x))$ is then defined as all polynomials over F with degrees less than the degree of f (Knudsen). We can thus prove the following theorem.

3.3.1 If F is a finite field with $f(x) \in F[x]$, then $|F[x]/(f(x))| = |F|^{deg(f)}$

Understand that $|F[x]/(f(x))|$ is notation for the number of polynomials over F with degrees less than the degree of f.

Proof Suppose f has degree m. It would then be of the form $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_mx^m$. Polynomials of degree less than that of f would be of the form $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_{m-1}x^{m-1}$. There are $|F|$ possible values, the number of elements in the field F, that b_i for $0 < i < m - 1$ can take on. The number of possible polynomials $g(x)$ would thus be $|F|^m$, because there are m number of terms that $g(x)$ has. This number, m, also happens to be the degree of f, so we can write the number of polynomials over F with degree less than f as being $|F|^{deg(f)}$.

A polynomial $a(x) \in F[x]$ is considered reducible if there exist polynomials $b(x)$ and $c(x)$

such that $a(x) = b(x)c(x)$.

3.4 Constructing Finite Fields

We previously proved that $\mathbb{Z}_m$ was a field only when m was prime. This, however, does not necessarily mean that fields of composite numbers of elements do not exist. We can form fields of other numbers of elements by extending existing fields (Cherowitzo).

For example, a field of 4 is an extension of the prime field of 2, because $4 = 2^2$. First we must find an irreducible polynomial in the field $F = \{0, 1\}$. One such polynomial is $f(x) = x^2 + x + 1$. The polynomials in $F[x]/(f(x))$ would yield $0, 1, x, x + 1$, which, in fact, constitute a field of four elements. These are the addition and multiplication tables for them:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Likewise, to find a field of 9 elements, one would take an extension of the field of 3 elements, by finding an irreducible polynomial in that field, and finding all polynomials of degrees less than that polynomial (Cherowitzo).

4 Applications

Although groups and fields and the theory that intertwines them is seemingly abstract and unrelated to the modern world, there are in fact an astounding number of applications for them. One area in which group theory prevails is music, particularly in musical set theory. It helps to explain and prove various musical phenomena via mathematics.

Furthermore, field theory can be used to conduct primality tests and serves as the basis for cryptography. The company RSA, which has set the world standard for public key encryption devotes a large amount of its revenue towards group and field theory research and offers prizes of tens of thousands of dollars to those able to utilize mathematics to break its codes.

However complex group and field theory may be, it is merely a small stepping stone into the vast realm of number theory, and then mathematics, and the world itself.

References

[1] Cherowitzo, William. 18 Aug. 2001. University of Colorado at Denver. 2 Jan. 2005. http://www-math.cudenver.edu/∼wcherowi/courses/finflds.html.

[2] RSA Laboratories. Cryptography Mathematical Concepts. 2004. RSA Security. 2 Jan. 2005.
http://www.rsasecurity.com/rsalabs/node.asp?id=2365.

[3] Dogfrey, Arfur. Introduction to Group Theory. 1998. The Dog School of Mathematics. 2 Jan. 2005.
http://members.tripod.com/∼dogschool/index.html.

[4] Group Theory. 1 Jan. 2005. Wikipedia. 2 Jan. 2005.
http://en.wikipedia.org/wiki/Group_theory.

[5] Knudsen, Lars R. Groups, Rings, Fields. 13 Sept. 2004. Technical University of Denmark. 2 Jan. 2005.
www.mat.dtu.dk/education/01425/files/note2.ps.

[6] Modular Arithmetic. 30 Dec. 2004. Wikipedia. 2 Jan. 2004.
http://en.wikipedia.org/wiki/Modular_arithmetic.

[7] Weisstein, Eric W. Fields. 2004. MathWorld–A Wolfram Web Resource. 2 Jan. 2005.
http://mathworld.wolfram.com/Field.html.

[8] Weisstein, Eric W. Groups. 2004. MathWorld–A Wolfram Web Resource. 2 Jan. 2005.
http://mathworld.wolfram.com/Group.html.