Rings

Kian Eghbalnia

December 9, 2020

This runs through the important theorems and intuitions about Rings needed to understand the proofs and theorems in field theory which utilize polynomial rings. The subject of rings is very didactic and there are many ways to get to any given destination.

In Abtract Algebra by Dummit and Foote, the concept of Ideals and quotient groups is considered in large part through the lense of homomorphism ”fibers.” Whereas Judson makes an effort to assert the existence and properties of Ideals and Quotient groups without relying as much on homomorphisms. There are many specialized cases that may not need to be mentioned. For example rings without identity are possible, but not useful in the direction we want to go, that is, from rings on to fields on to field extensions. The purpose of this paper is to attempt to cut out any knowledge not entirely necessary for this path through Ring theory. However, I personally like this topic specifically because of all of the viewpoints from which it can be seen. The fact that so many approaches can be used to get to the same theorems gives the impression that the underlying structure of rings and fields are the true form, and the proofs simply an explanation of this structure, rather than the structure itself being a result of the proofs’ validity.

1 Basic definitions and context

This will be a very brief overview of the vocabulary and basics.

A Ring is an algebraic structure R with two binary operations, called addition $(+)$ and multiplication $(*)$, that satisfy the following qualities:

R is an abelian group under addition

R is a monoid- it is closed and associative- under multiplication

Multiplication distributes over addition from both the left and right, meaning $x_1(x_2 + x_3) = x_1x_2 + x_1x_3$ and $(x_2 + x_3)x_1 = x_2x_1 + x_3x_1$

In the previous equations $a * b$ is shortened to ab

There are different types of Rings, and we will specify what we need as we go. For example, from the definition we know R has an additive identity usually denoted 0, but R may or may not have a multiplicative identity. This element would be denoted 1 and have the property that for all $x \in R$, $1x = x$ and $x1 = x$, and the ring which contains it would be called a Ring with identity. We will define these special rings when we need them. There are also special elements in a ring and special subsets in a ring - of interest are zero divisors, units and subrings.

Zero divisor - an element $r \in R$ and $r \neq 0$ st. the equation $rx = 0$ or $xr = 0$ can be satisfied

Unit - an element in a ring with identity $r \in R$ that has an inverse; there exists an $r^{-1} \in R$ st. $rr^{-1} = r^{-1}r = 1$

Subring - a subset of R that forms a ring under the same operations as R

These are all important vocabulary to know for the following proofs, but to take the next step towards useful theorems about fields we need to look at a very important type of subring called a Ideal.

2 Ideals

An ideal is a very congenial subring of a ring R.

Ideal - A subring $I \subseteq R$ st. $RI \subseteq I$ and $IR \subseteq I$

We could say that an ideal is a subring that is closed under multiplication by any element of the ring R. Consider a ring with identity in which the multiplication operation is also commutative, called a commutative ring with identity. Then any element $r \in R$ will generate an ideal $I :=< r >= rR$. This type of ideal is called a principal ideal. Another example of an ideal is the kernel of a ring homomorphism.

Ring homomorphism - a function from one ring to another $\phi := R_1 \to R_2$ which obeys the laws:

$$\phi(x_1 + x_2) = \phi(x_1) + \phi(x_2)$$
$$\phi(x_1 x_2) = \phi(x_1)\phi(x_2)$$

Kernel (of Ring Homomorphism) - The elements that are sent to the additive identity in the codomain

One can check that these are both Ideals of a ring R, additionally, we have two more examples, the entire ring R, and the subring containing only the additive identity $0 \in R$, but these are referred to as the trivial Ideals, for obvious reasons. Ideals are useful because their cosets form form a Ring, similarly to how the cosets of a normal subgroup formed a group.

3 Quotient Rings

Consider the Left Cosets of the additive group of R, the sets of the form $x + I$. Since the additive group in a ring is abelian we know the Left coset is equal to the Right coset. For our first proof, let us prove that these cosets form a ring under the natural operations:

$(x + I) + (y + I) = (x + y + I)$

$(x + I)(y + I) = (xy + I)$

Theorem 1. *The cosets of an Ideal I form a subring under the given set operations.*

Proof. First we must prove that the operations are well defined, given two cosets, the operations have the same result independent of which representative element we choose. This can be stated as,

$$\text{If } (a + I) = (b + I) \text{ then } (ax + I) = (bx + I) \text{ and } (a + x + I) = (b + x + I)$$

We already know the truth of the well defined addition, as our ring is additively an abelian group, so our ideal is additively a normal subgroup. For the well defined multiplication let $(a + I) = (b + I)$, and consider any element in the coset, $a + i_1 = b + i_2$, then $a = b + i_2 - i_1 = b + i_3$.So we have

$$(ax + I) = (bx + i_3x + I) = (bx + I)$$

because i_3x is some element in the ideal, and given the structure of an ideal as a subring, adding by a constant will give back every element in the subring. We have only proven this property for multiplication on the left, but the proof is the same for multiplication on the right.

The remaining properties of a ring can be confirmed by the corresponding properties in the original ring R following the example:

Let us show that our cosets are closed under addition

$$(x_1 + I) + (x_2 + I) = x_2 + x_1 + I$$

$x_1 + x_2$ is an element of our ring R by the additive closure property of rings, so $x_1 + x_2 + R$ is a coset.

Thus we have two well defined operations that follow the ring axioms.

□

The ring formed by the cosets of an Ideal I in some ring R is called a Quotient Group, and is denoted R/I. Intuitively, our proof relies on the fact that if I is an ideal, coset operations behave like the operations in the encompassing ring, with the exceptions that elements in the same coset are interchangeable. This suggests that a function which sends any element of an ideal to its corresponding coset maintains some of the structure of the original ring. This is correct, as such a function is a homomorphism.

4 Fields

A field is a highly structured ring. We will construct an example of a field with a ring and a maximal ideal.

An ideal is Maximal if there is no larger ideal that contains it besides the full ring R. Consider such an ideal in a commutative ring with identity, we see from our previous proof that any Quotient ring R/I is also commutative with identity $(1+I)$. For any element in our Quotient group, $(x+I)$, the problem of finding a multiplicative inverse for out coset reduces to finding some element in $y \in R$ st $xy \in (1+I)$. In other words. Is there a solution to

$$1 = xy - i,\ \ y \in R, i \in I$$

since $-i \in I$ iff $i \in I$ this becomes

$$1 = xy + i,\ \ y \in R, i \in I$$

So we need to know if 1 is in the set $xR + I$.

It can be proved through straightforward algebraic manipulation $xR + I$ is also an Ideal, and furthermore that it contains I, if $x \notin I$, since $xR + I$ will contain x, then this ideal must be larger that I itself. Therefore, given that I is maximal, $xR + I$ must be the entire ring R and thus must contain 1. Hence $x + I$ has an inverse. Since this was done for an arbitrary coset other than I, we know that every coset other than the additive identity I has a multiplicative Inverse. Thus R/I is a commutative ring with identity in which every element is a unit. Such a ring has a special name; it is called a field.

Theorem 2. *If R is a commutative ring with identity, and I is a maximal ideal, then the Quotient Ring R/I is a field.*

This is actually a two way implication, and proving the converse is also simple.

Theorem 3. *If R is a commutative ring with identity, and the Quotient Ring R/I is a field, then I is a maximal ideal.*

Proof. let us assume that R is a commutative ring with identity, and that R/I is a field. Then we know that for any element $x \in R$, if $x \notin I$ then $x + I$ is not the additive identity in the field R/I, so it has an inverse, thus there exists an element $y \in R$ st. $(x + I)(y + I) = (1 + I)$ and this implies $(xy + I) = (1 + I)$, which implies that there exists an $i \in I$ st.

$$xy + -i = 1$$

by the properties of ideals if both x and i are in some ideal K, then $xy + -i = 1$ is also in the ideal, and finally since 1 is in the ideal, $1R$ is contained in the ideal, and this is all of R. So if $K \supseteq I$ then containing any additional element x would mean $K = R$, and this is our definition of a maximal ideal. □

So if we begin with a ring and a maximal ideal we can generate a field, but we can also go the other way, that is, we can generate a ring from a field. The polynomials with coefficients in a field, F, form a ring, $F[x]$.

Consider the Ideals in this ring; a principal ideal generated by $p(x)$ will be denoted $\langle p(x)\rangle$. It is useful to know that there is a euclidean algorithm that works to find the greatest common divisor of two polynomials, and this can be used to prove that we have a similar division algorithm in polynomials as we do in the whole numbers.

Theorem 4. *A principal ideal I generated by $p(x)$ in the ring of polynomials of a field is maximal if and only if $p(x)$ has no nontrivial divisors.*

Proof. If $p(x)$ has non-trivial divisor $q(x)$ then the ideal $\langle q(x)\rangle$ contains $\langle p(x)\rangle$, and since $q(x)$ is non-trivial (it is of not degree 0), then $\langle q(x)\rangle \neq F[x]$. So by definition $\langle p(x)\rangle$ is not maximal.

On the other hand, let $p(x)$ be irreducible. From the division algorithm we can prove that any ideal in a polynomial ring is a principal ideal, thus is generated by one element $k(x)$. Then if $\langle k(x)\rangle$ contains $\langle p(x)\rangle$, it must at least contain $1 * p(x)$, so $k(x)$ must divide $p(x)$.

And so by the irreducibility of $p(x)$, $k(x)$ is either a multiple of $p(x)$ by an element of the field, in which case their principal ideals would be the exact same. Or, $k(x)$ is itself a member of the field, in which case it would generate the entire polynomial ring $F[x]$. Thus by definition $\langle p(x)\rangle$ is maximal. □

And finally we get the following theorem.

Theorem 5. *A quotient ring $F[x]/\langle p(x)\rangle$ on the ring of polynomials over a field is itself a field if and only if $p(x)$ has no nontrivial divisors.*

5 Field extensions

Let us suppose we have a field F, and we take some irreducible polynomial $p(x) \in F[x]$. We know $F[x]$ is a ring, and that $F[x]/p(x)$ is a new field. Our cosets of degree 0 polynomials, cosets of the form : $(f + \langle p(x)\rangle)$ where f is some constant in F, are in this field and behave exactly like the original field F under our operations.

Then if we take only this subset of our field $(F[x]/p(x))' \subset F[x]/p(x)$, the operations addition $(+)$ and multiplication $(*)$ are closed within this subset, this subset also inherits the field axioms from its encompassing field. Thus we have found a smaller field within $F[x]/p(x)$. In this relationship, $(F[x]/p(x))'$ is called a subfield, or we can say that $F[x]/p(x)$ is a field extension of $(F[x]/p(x))'$.

As previously stated, structurally $(F[x]/p(x))'$ and F are the same, thus since $(F[x]/p(x))'$ admits a field extension of the form $F[x]/p(x)$, F must admit a field extension E with the same structure as $F[x]/p(x)$. So we may just call $F[x]/p(x)$ a field extension of F, even though symbolically the first is made of cosets and the second of elements of F.

We have mentioned that a function which preserves structure between two rings is called a Homomorphism. If this function is one-to-one it is called an isomorphism, and we write $R_1 \cong R_2$. So the previous statements can be written as:

$$(F[x]/p(x))' \cong F \text{ and } F[x]/p(x) \cong E$$

The field extansion E may be completely contrived. If it doesn't already exist, the symbols for the extra field elements might need to be created, but the important thing is that it would contain F as a subfield and would have the same structure as $F[x]/p(x)$. For example, our isomorphism might send the coset $(x + \langle p(x)\rangle) \in F[x]/\langle p(x)\rangle$ to an element in E which we will call α. Then x^2 must be sent to α^2, x^3 sent to α^3 and so on...

We will show that $p(\alpha) = 0_F$ where 0_F is the additive identity in the field F. If we take $p^*(x)$ to be the polynomial $p(x)$, but with the coefficients in F replaced with their corresponding elements in $(F[x]/\langle p(x)\rangle)' \subset F[x]/\langle p(x)\rangle$, then we can derive the following.

$$p^*((x + \langle p(x)\rangle)) = (p(x) + \langle p(x)\rangle) = \langle p(x)\rangle$$

This is the additive identity in $F[x]/\langle p(x)\rangle$, then by our isomorphism properties, the phrase $p(\alpha)$ must also be sent to the additive identity in its corresponding field. This is a general outline, but it does most of the hard work for the following theorem.

Theorem 6. *Kronecker's theorem. If F is a field, then for any polynomial $p(x) \in F[x]$ there exists a field extension E in which $p(x)$ has a root.*

Proof. Factor $p(x)$ until you find an irreducible factor, then there exist a field extension E in which this factor will have a root. $p(x)$ will also have a root in E. □

We see in the description above that $x + \langle p(x)\rangle$ is a special element in $F[x]/\langle p(x)\rangle$, in that it is a root of the polynomial over $F[x]/\langle p(x)\rangle$ that corresponds to the polynomial $p(x)$ over F.

It is special in another way, as any element in $F[x]/\langle p(x)\rangle$ can be created with only the powers of $x + \langle p(x)\rangle$ and our elements in $(F[x]/\langle p(x)\rangle)'$, and that powers of x greater than or equal to the degree of $p(x)$ are superfluous because we may divide by $p(x)$ and get a polynomial with lesser degree but in the same coset. Thus the powers of $(x + \langle p(x)\rangle)$ less than the degree of $p(x)$ form a basis for $F[x]/\langle p(x)\rangle$ over $(F[x]/\langle p(x)\rangle)'$. Again, by our isomorphism this means that the powers of α less than the degree of $p(x)$ form a basis for E over F.

6 The Characteristic Field

Suppose we have a field F and this field has multiplicative identity 1 and additive identity 0. Then by closure we know $1+1$ is in the field as well, and $1+1+1$ and so on. If our field is infinite this may go on forever and each sum may be a unique element of the field. But if F is finite then eventually one sum must equal another, and we will have

$$1+1+1+....+1+1 = 1+1+1+...+1+1$$

where the number of elements in each sum differs by some constant k. Now my repeatedly adding by the additive inverse of 1 we can obtain $0 = 1+1+1+...+1+1$ where the number of elements in the right sum is k. Then k is called the characteristic of the field. in the aforementioned case where this sum never equals 0 we give the characteristic the value 0.

We also see that if k is composite, $k = a * b$ then a sum of 1 of length a multiplied by a sum of length b will be equal to 0, and since this is impossible in a field, k must be prime.

For our last proof note that for a nonzero characteristic, a sum of length k of any element in the field will also equal 0 as $x + x + ... + x$ can be factored into $(1+1+...+1)x$.

For our last proof we will show that the characteristic of a field gives rise to a homomorphism between the field and itself.

Theorem 7. *Let F be a field with characteristic $k \neq 0$, then the function $\phi : F \to F$ given by $\phi(x) = x^k$ is a homomorphism*

Proof. We must show the following:

$\phi(x_1 + x_2) = \phi(x_1) + \phi(x_2)$

$\phi(x_1 x_2) = \phi(x_1)\phi(x_2)$

The second item follows from the property that a field has commutative multiplication. For the first item we use the binomial theorem

$$(x_1 + x_2)^k = x_1^k + \binom{k}{1} x_1^{k-1} x_2 + ... + \binom{k}{k-1} x_1 x_2^{k-1} + x_2^k$$

where the binomial coefficient is used to indicate that the following product of x_1 and x_2 are added $\binom{k}{j}$ times. For $j \neq 1, k$ and k prime it can be shown that $\binom{k}{j}$ is divisible by k. The the terms in the middle compute to 0 and the expression $x_1^k + \binom{k}{1} x_1^{k-1} x_2 + ... + \binom{k}{k-1} x_1 x_2^{k-1} + x_2^k$ reduces to $x_1^k + x_2^k$. So ϕ is a homomorphism. □

There is still a long way to go to prove Evariste Galois' famous theorem that not all quintic polynomials are solvable by radicals. However, these theorems provide a basis to go down that road, and are interesting and elegant in their own right.