My Solutions to Old Algebra Quals

Jacob S Townson

May-July 2017

# Prelude

This document is written in reference to qualifying exams given at the University of Louisville in past years. These solutions are not given from the University, but of my work alone as a way to study for my own qualifying exam. If any tips or recommendations come up and you feel you should share, feel free to raise an issue on GitHub where I have this document saved and open to the public [here](https://github.com/obewanjacobi/gradwork/tree/master/Classes/Old%20Qualifying%20Exams/My%20Solutions). To see the qualifying exams for yourself, [visit this link](http://www.math.louisville.edu/GraduateFAQ/qualifiers/QualifierStudyGuides/). Thank you.

Jacob Townson

## January 2016 Qual

### Let be a group and its center. Suppose that the group is cyclic. Show that is Abelian.

#### My Solution:

Let be cyclic with generator . Every element in can be written as where and . We want to show first for all that can be written in the form for some and . We know that is cyclic, so there exists some such that for some . Well, this is true iff . So there exists a such that .

Now let . Then

and

for and .

Thus

because . THus which implies that G is Abelian. QED

### Prove that every prime ideal is maximal in a PID.

#### My Solution:

Let be a prime ideal in the PID . So iff or . But is a PID, so where . So we want to show is maximal using this information, ie. if is an ideal that contains , then or . So let be an ideal containing such that . Let where because is a PID. Now, which implies that there exists such that . Since , we know either or is in because it's prime.

If , then which implies . On the other hand, if , then there exists such that . So

Because is an integral domain (because it'e a PID), we can reduce the above formula to

Thus is a unit which implies that .

Thus either or for all containing , so is maximal in . QED

### Let be a commutative ring with . For any two ideals and of , let be the ideal generated by all products where and . Suppose , prove that .

#### My Solution:

We will prove this using set containment.

Because and are ideals in , for all and all , and . Moreover, and . Thus

which implies

Thus

Now we just need to show that . To do this we will use the fact that . Let . We know . So for some and . Then since is commutative,

However since and and for similar reasons as our previous argument. By the definition of , this shows us . Thus .

Thus we've proven that in this circumstance. QED

### Prove that any finite group is isomorphic to a subgroup of for some , where is the alternating group on elements.

#### My Solution:

To do this proof, we will use the broader proof of Cayley's Theorem. This theorem states that if is a group of order , then is isomorphic to a subgroup of .

Let be the set of all elements of . Now consider the action of on ,

This action defines a homomorphism . It is fairly easy to see that this homomorphism is one-to-one and onto. Thus, it follows that is isomorphic to a subgroup of . And finally, since we have that This tells us that .

Thus we just need to show that . Let such that if is even, or if is odd where . We just need to show that is an isomorphism. Let . If are even, then

If are both odd, then

This is true because is the identity permutation, and is even. Finally WLOG let be even and be odd. Then

Thus is a homomorphism. It is also obvious that for all there exists a , so we know that is onto. And finally, it is obvious that if , then . Thus is an isomorphism.

Using this fact and Cayley's Theorem, we then know that which proves that any finite group is isomorphic to a subgroup of . QED

### Determine if the field extension is Galois.

#### My Solution:

In order to prove that is or is not Galois, we will use the fundamental theorem of Galois theory. Thus, we know if we prove that is a splitting field over some function in , then we know the extension is Galois. Consider the polynomial . This polynomial has no roots in , but has root . Unfortunately, this is not enough for us to factor into linear factors, as we will need some to further factor the polynomial. Thus we know that is not a splitting field, and thus it must not be Galois by the fundamental theorem of Galois theory. QED

### Let be a group. Consider the commutator subgroup of , the subgroup generated by all commutators, where . It is known that is a normal subgroup of . Prove that a) is Abelian, and b) if such that is Abelian, then .

#### My Solution:

1. First off, to save time let . So we want to show that for all that
2. Well, generates . So, , which implies that through cancellation. Thus is Abelian. QED
3. So here we want to show that for all and , . Well, because and is Abelian, we know that for all that . Using this, we know that . Thus we can say that because is a cummutator. Thus . QED

### Let be a commutative ring. Prove that the following are equivalent: (a) is a field; and (b) and the only ideals of are and .

#### My Solution:

()

Suppose is a nonzero ideal of a field . So contains some . Then since is a field, exists and , so contains and hence . The trivial ideal also exists, and is trivial to show.

()

Let have only two ideals, the trivial and . Suppose is not a field. Then some nonzero element does not have an inverse. If we set . This is a proper nonzero ideal, which gives us a contradiction to our original statement. Thus must be a field for to only contain 2 ideals, the trivial and itself.

Thus the two statements are equivalent, is a field and contains only two ideals, those being the trivial ideal and itself. QED

### (a) Find the degree of the extension over . Find a basis of the vector space over . (b) Find a primitive element of the extension of .

#### My Solution:

1. Here we can use what I like to call the *double extension lemma* to find the degree of the extension. So we know that . Thus because the minimum polynomials for the extensions are and respectively, we know that the degree of the extension is . A basis for this extension is . QED
2. The primitive element of this extension is as this element makes the simple extension . This can be shown through the following containment arguments:

First let . It is obvious that , so we're good there. Thus we just need to show that . So we need to show that . Well, let . We know . , which implies that . Then we can look at which implies that , which implies that . Thus . So finally we have proven both directions of containment, implying that the primitive element makes into a simple extension of which we call . QED

## August 2015 Qual

### Prove that a group of order cannot be simple.

#### My Solution:

To begin, we must understand what it means for a group to be simple. A simple group is a group of whose only normal subgroups are the trivial group and the entire group itself. Thus we want to show there are no proper normal subgroups other than the trivial group.

To do this we will use Sylow's Theorem and a proof by contradiction.

Let be a group of order such that is simple. Well, . We will denote the number of Sylow-p subgroups as . Notice then that and . This implies that or . However, because is simple there cannot only be one Sylow-5 subgroup, otherwise we would have a proper nontrivial normal subgroup. Thus . Because of this, and because is simple, we can say that embeds into if we let act on the Sylow-5 subgroups by conjugation. But then by Lagrange's Theorem, should divide , which it does not. Thus we have a contradiction, which implies that is not simple, thus a group of order cannot be simple. QED

### Let where is imaginary. Find the degree of the extension and a basis of over . Justify.

#### My Solution:

1. Here we can use what I like to call the *double extension lemma* to find the degree of the extension. So we know that . Thus because the minimum polynomials for the extensions are and respectively, we know that the degree of the extension is . A basis for this extension is . QED
2. The primitive element of this extension is as this element makes the simple extension . This can be shown through the following containment arguments:

First let . It is obvious that , so we're good there. Thus we just need to show that . So we need to show that . Well, let . We know . , which implies that . Then we can look at which implies that , which implies that . Thus . So finally we have proven both directions of containment, implying that the primitive element makes into a simple extension of which we call . QED

### Let and be ideals of a ring with . Show that is an ideal of the ring .

#### My Solution:

Recall for this problem the definition of an ideal for rings. is an ideal of the ring if for all and , then .

We will use this definition to show is an ideal of . Notice . So let's consider two elements, and such that and . We want to show that and . Well,

because is an ideal of . But is also an ideal of so , which implies that . Looking at the other direction, we find that

and for similar reasons, we then know that . Thus is an ideal of . QED

* Note: This statement also follows directly from the third isomorphism threorem for rings.

### Let and be ideals of a ring with . Show that the map given by for every , is well-defined, onto, and a homomorphism.

#### My Solution:

We will need to separate this problem into three parts.

* First we must prove that is well-defined. So we want to show that if , then . Well, if , then
* Thus is well-defined by definition.
* Next we will show that is an onto function. So we need to show that for all , and , then . Well, by definition this is obvious, because for all and , . Thus the function must be onto.
* Finally we must show that is a homomorphism. First note that by definition, so the identity maps to the respective identity. Now we must prove that addition and multiplication are preserved. First, let's look at where . So,
* Thus addition is preserved. So now we must only prove that multiplication is preserved. Assume a similar situation as above, but let's look at . Well,
* because is an ideal. Now we can further this manipulation using that is an ideal to see that
* Thus because identities, addition, and multiplication are preserved, we know then that is a homomorphism.

Thus is a well-defined, onto, homomorphism. QED

* Note, this could have been simplified with the first Isomorphism Theorem for Rings.

### Let and be ideals of a ring with . Show that is isomorphic to .

#### My Solution:

This statement follows directly from the third Isomorphism Theorem for rings. QED

### Determine the splitting field and its degree over for the polynomial . Justify.

#### My Solution:

First note that . The roots of this polynomial are . We can then see that the splitting field of over is . This is the splitting field because in this extension can be factored into linear factors. QED

### A ring (not necessarily commutative) with identity in which every nonzero element is a unit is called a *division ring* . Prove that a ring with identity is a division ring iff has no proper left ideal.

#### My Solution:

First, recall if , is a left ideal if for all and , .

Assume has no proper left ideal, thus the only left ideals are the trivial and the entire ring. So if is nonzero and has no proper left ideals, then we can define and there exists such that . Also note

Because , must be a division ring.

Now we must prove the other direction. Assume is a division ring and is a left ideal of . Then for all ,

Thus has no proper left ideals. QED.

### Let be an arbitrary group. For any two subgroups and of , define . Assume and . (a) Prove that . (b) Prove that and . (c) Prove that .

#### My Solution:

**Note: This is the proof of the 2nd Isomorphism Theorem for Groups**

1. Recall that can only be a subgroup if . Thus if , and we let and , by assumption . Thus
2. This proves that . Similarly, which proves the reverse containment. Thus . QED
3. Since normalizes and normalizes itself trivially, this implies that normalizes . Thus . Since , the quotient group is well defined. Define the map by . Since the group operation in is well defined, it's easy to see that is a homomorphism:
4. Alternatively, the map is just the restriction to the subgroup of the natural progression homomorphism , so it's also a homomorphism. It is clear then from the definition of that is onto. The identity of is simply , so the kernel of consists of the elements with , or where . Thus . So by the first isomorphism theorem, . QED
5. Following the proof of part (b), by the First Isomorphism Theorem, QED

### Let be a field and let . (a) What is the definition of the *splitting field* of the polynomial over the field . (b) Let . Show that and have the same splitting field over .

#### My Solution:

1. The extension field of is a splitting field for the polynomial if factors completely into linear factors in and does not factor completely into linear factors over any proper subfield of containing .
2. Let . Let be the splitting field of over . And finally, this all means that . Since is the splitting field of over , we then know that has roots . Also note that some of these values could be duplicates or even zeroes. So by definition, in , . This means that in , . From here it is easy to see that the roots of are simply . All of these values are in as well because for all , and . So because we can factor into linear factors in , must also be the splitting field of . Note, the situation in which we switch assumptions such that is the splitting field over to prove that must also be the splitting field of over is similar, so we leave this out. QED

## January 2015 Qual

### If is a normal subgroup of and is any subgroup of , prove that is a subgroup of .

#### My Solution:

Let and be a normal subgroup of . Let be defined as above. So we want to show for all , . Well, . First note because is a normal subgroup of and , and . Also note because is normal in , for all , , ie. for all , . Thus in ,

Thus is a subgroup of . QED

### Show that a group of order is not simple

#### My Solution:

Let be a group of order . We will denote the number of Sylow- subgroups by . So where and . Also where and . So and .

If either or are , then we're done as this means that there exists a normal proper nontrivial Sylow- subgroup in our group . Consider . Because $&$ is prime and the subgroups are cyclic, and because we know the subgroups intersect trivially, there exists non identity elements in all of the Sylow -subgroups. Notice, . But if , then there are distinct elements in each of the Sylow- subgroups. But we run into a problem, because , so then there must be only 1 Sylow- subgroup in order to have elements. Thus either or , thus could not be simple as it has a normal proper nontrivial subgroup. QED

### A ring is *Boolean* if every element is idempotent, that is for all . Prove that every Boolean ring is commutative.

#### My Solution:

Recall that a ring is commutative if the multiplication operation in the ring is commutative. Thus we want to show that for every Boolean ring, if then .

To begin this problem, consider . Well,

When cancelling and from both sides, we find that , but because is Boolean, we can easily see that for all . Thus we have proven that all Boolean rings are indeed commutative. QED.

### Show that every prime element in an integral domain is irreducible.

#### My Solution:

Recall an integral domain is a commutative ring with no zero divisors. Also an element in an integral domain is irreducible if it is not equal to the product of two non-units. Also recall that if is our integral domain, is a unit if for some , where is the identity in . Lastly, recall that is prime if or .

Let be a prime element where is an integral domain. Assume where . Obviously , so because is prime, or . WLOG, assume such that for some . If is the identity of , then

Because is an integral domain, can be cancelled out implying that , thus is a unit. This proves that is also irreducible in an integral domain. QED.

### Prove or provide a counterexample: Galois extensions of Galois extensions are Galois extensions. That is, if is Galois and is Galois, then is Galois.

#### My Solution:

This statement is false! Consider , , and . In this case, is Galois because is a splitting field over , and it is similar for . However, is not Galois, as does not make a splitting field over . This can be seen from the polynomial . Not all of the roots of are contained in , as does not contain any imaginary numbers. QED

### Let be a finite extension of field . Prove that is algebraic over .

#### My Solution:

Assume is finite. Let . We have then that . We know

Consider . So there exists such that , where at least one . Let , so . Thus if is finite, then is algebraic over . QED

### Find the degree of the extension , where . Is this a simple extension? Why or why not?

#### My Solution:

1. Here we can use what I like to call the *double extension lemma* to find the degree of the extension. So we know that . Thus because the minimum polynomials for the extensions are and respectively, we know that the degree of the extension is . A basis for this extension is . QED
2. The primitive element of this extension is as this element makes the simple extension . This can be shown through the following containment arguments:

First let . It is obvious that , so we're good there. Thus we just need to show that . So we need to show that . Well, let . We know . , which implies that . Then we can look at which implies that , which implies that . Thus . So finally we have proven both directions of containment, implying that the primitive element makes into a simple extension of which we call . QED

### Let be an arbitrary group with a center . Prove that the inner automorphism group is isomorphic to . (Recall by definition is the group of all automorphisms of the form , for all .)

#### My Solution:

Consider the map defined as , where is the automorphism of defined by .

**Lemma 1**: is a homomorphism.

*Proof*: We have , and

**Lemma 2**: .

*Proof*: We have

Finally, by the first isomorphism theorem, we have , as desired. QED.

### Let be a finite group and let . Prove that for any Sylow -subgroup of , is a Sylow -subgroup of .

#### My Solution:

Since is a -group, as it is contained , we only need to show that has maximal -power order in . By the Sylow Theorem, is contained in a conjugate of , which we'll call such that . Thus . Also , so . Since , we get that , so is a -Sylow subgroup of . QED

### Let be a commutative ring with unity and let be an ideal of . Prove that the following are equivalent: (i) is prime, and (ii) For any ideals , if then or .

#### My Solution:

1. ii

Let and suppose WLOG that . Then there is some such that . But then for all , so by (i), for all .

1. i

Let so that or . Then if we let and , if , then , so by (ii), or which implies by definition that is prime.

### Determine the Galois group of over .

#### My Solution:

Recall that the Galois group of a separable polynomial is defined to be the Galois group of the splitting field of over .

Well, . We cannot factor any futher in but in , can be factored into linear factors. So the plitting field over is . So the automorphisms in the Galois group map , , the identity map, and interchanging the and . Thus the Galois group has order and is not cyclic, implying that the Galois group must be . QED

## August 2014 Qual

### Let . Prove that is isomorphic to a subgroup of . Recall the normalizer and the centralizer

#### My Solution:

For , it is clear that defines an automorphism of . Define a map:

where . Since for all , we have that . Then is a group homomorphism from to . Note that

From the first isomorphism theorem we then have that is isomorphic to a subgroup of . QED

### An integral domain is said to be **Artinian** if for any descending chain of ideals of , there is an integer such that for all . Prove that an integral domain is Artinian if and only if it is a field.

#### My Solution:

Assume is Artinian, and has a unit that is a multiplicative identity element. For any , consider the principle ideal generated by , . Since for any , we have that . Thus we have our descending chain of ideals

which will stabilize because is Artinian. Thus for some positive integer ,

Then since , there exists such that or . Using the properties of an integral domain, this implies that . Thus we have shown that every has a multiplicative inverse thus is also a field.

Assume is an integral domain and a field. Then has only two ideals, the trivial and itself. Thus every strictly descending chain of ideals is of finite length, implying that is Artinian. QED

### A *principal ideal ring* is a ring in which every ideal has a single generator. (a) Prove that an element of a principal ideal domain is prime iff it is irreducible. (b) Provide an example of a principal ideal ring containing an element which is prime but not irreducible.

#### My Solution:

1. Recall that a PID is also an integral domain. Also recall that an integral domain is a commutative ring with no zero divisors. Also an element in an integral domain is irreducible if it is not equal to the product of two non-units. Also recall that if is our integral domain, is a unit if for some , where is the identity in . Lastly, recall that is prime if or .

Let be a prime element where is an integral domain. Assume where . Obviously , so because is prime, or . WLOG, assume such that for some . If is the identity of , then

Because is an integral domain, can be cancelled out implying that , thus is a unit. This proves that is also irreducible in an integral domain.

Now assume that is irrecucible. To complete the proof, we want to show that is prime. If is irreducible, then is maximal in the set of all proper principal ideals of . Since is a principal ideal domain then every ideal is principal, so in fact is maximal in itself. Since is an integral domain (because it's a PID), then has an identity. So then must be prime which implies must then be prime. QED

1. In is prime but not irreducible because and neither nor are units.

### Prove that is a simple group if it's order is .

#### My Solution:

Let be a group of order . We will denote the number of Sylow- subgroups by . So where and . Also where and . So and .

If either or are , then we're done as this means that there exists a normal proper nontrivial Sylow- subgroup in our group . Consider . Because $&$ is prime and the subgroups are cyclic, and because we know the subgroups intersect trivially, there exists non identity elements in all of the Sylow -subgroups. Notice, . But if , then there are distinct elements in each of the Sylow- subgroups. But we run into a problem, because , so then there must be only 1 Sylow- subgroup in order to have elements. Thus either or , thus could not be simple as it has a normal proper nontrivial subgroup. QED

### Let be a finite extension of the field . Prove that is algebraic over .

#### My Solution:

Assume is finite. Let . We have then that . We know

Consider . So there exists such that , where at least one . Let , so . Thus if is finite, then is algebraic over . QED

### Let and put . (a) Find the minimal polynomial of over . (b) Find . (c) Identify the group , the set of all automorphisms of which fix .

#### My Solution:

1. We will denote the minimal polynomial here as . Consider . First we can see that . We can also see from Eisenstein's Criteria that is irreducible in . Thus is indeed the minimal polynomial of over .
2. We know that . Thus .
3. Well, fixes all , so to find the automorphisms we just need to observe the roots. Well, there are possible automorphism maps for the roots:
4. Notice first off that these automorphisms do not make a cyclic group, so our Galois group is not , and our Galois group turns out to be . QED

## January 2014

### Let . (a) Show that is irreducible over . (b) Determine the four roots of . (c) Let be the splitting field of over . Determine . Justify. (d) Determine the Galois group of over . Justify.

#### My Solution:

1. This is obviously irreducible by Eisenstein's Criteria.
2. Let be the primitive root of unity. Then are the roots of .
3. Let . Since is irreducible in , and can be reduced into linear factors in , must be the splitting field of over . Thus, with as the minimal polynomial, .
4. We know by the fundamental theorem of Galois Theory that . Thus where maps to all possible powers of .

## August 2011

### Let be an Artinian ring. (a) For every ideal in show that is Artinian. (b) Show that every prime ideal in is also a maximal ideal.

#### My Solution:

We will skip part (b) as it is a repeat of an earlier problem because if is Artinian, then it is an integral domain.

1. So for all descending chains of ideals in
2. the descending chain stabilizes such that for some , . Well, note that . We will now prove a lemma stating that is an ideal of if and are ideals of .

For all , . So then for all , . So is an ideal of .

Now consider a descending chain of ideals

where all 's are ideals in . Then

is a descending chain of ideals in . Let because is Artinian. Then because . So is Artinian. QED

## August 2008

### Let be the set of all continuous real-valued functions on . Define addition and multiplication on as follows. For and , and . (a) Show that with these operations is a commutative ring with identity. (b) Find the units of . (c) If and , then show that or .

#### My Solution:

1. The identity function here is obvious, it is .

Let and be in . Then . So is Abelian. Also for all there exists a such that . Hence because of this and because is a continuous function from to , so is an Abelian group.

Let . Consider

Thus multiplication is associative.

Let . Consider

Thus follows the distributive property. Thus is a ring. It is also easy to see that because all of the functions are continuous on . Thus is a commutative ring with identity .

1. The units of are just the inverse functions of . ie. iff .
2. Let . Then . Then by cancellation, or . QED

### Prove that a group of order cannot be simple.

#### My Solution:

Assume is simple and denote the number of Sylow- subgroups as . Then where and . Also, where and . So . Since is not simple by assumption, then .

Thus because is smple and , there exists such that . This implies that can be embedded in if we let act on by conjugation. But then by Lagrange's theorem should divide which it does not. Thus we have a contradiction, so cannot be simple. QED

## Important proofs (not specific to Qualifiers)

### Prove the First Isomorphism Theorem for Groups

#### My Solution

First we will state the theorem itself:

Let be a homomorphism of groups, then and .

To shorten things, let . Define the homomorphism by . We claim that is an isomorphism. So we need to check that it's a well-defined homomorphism, and a bijection. First, to check that it's well-defined, we will check to see that if , then . If we let then for some , then

Now we will show that is a homomorphism. Consider . Then for any we have that

This proves that is a well-defined homomorphism. To prove that is one-to-one, we must prove that . Well, observe that

So . Finally we just need that is onto, which is somewhat obvious from the fact that so that has preimage . Thus we have proven the First Isomorphism Theorem for Groups. QED

### Prove the 2nd Isomorphism Theorem for Groups

#### My Solution:

First we must state it. Let be an arbitrary group. For any two subgroups and of , define . Assume and . Then: (a) . (b) and . (c) .

1. Recall that can only be a subgroup if . Thus if , and we let and , by assumption . Thus
2. This proves that . Similarly, which proves the reverse containment. Thus . QED
3. Since normalizes and normalizes itself trivially, this implies that normalizes . Thus . Since , the quotient group is well defined. Define the map by . Since the group operation in is well defined, it's easy to see that is a homomorphism:
4. Alternatively, the map is just the restriction to the subgroup of the natural progression homomorphism , so it's also a homomorphism. It is clear then from the definition of that is onto. The identity of is simply , so the kernel of consists of the elements with , or where . Thus . So by the first isomorphism theorem, . QED
5. Following the proof of part (b), by the First Isomorphism Theorem, QED

### State and Prove the 3rd Isomorphism Theorem for Groups

#### My Solution:

First (once again) we must state it first. Let with . Then and .

The proof that is easy and follows from the 4th Isomorphism Theorem for Groups, so we will leave this aside. Now, define

by . By the First Isomorphism Theroem, . It is clear that is onto, so . Now

Thus by the First Isomorphism Theorem, . QED

### State and Prove the 1st Isomorphism Theorem for Rings

#### My Solution:

If is a homomorphism of rings, then the kernel of is an ideal of , the image of is a subring of , and

Proof:

If is the kernel of , then the cosets of are precisely the fibers of . In particular, the cosets and are the fibers of over and respectively. Since is a ring homomorphism, , hence . Multiplication of cosets is well defined and so is an ideal and is a ring. The correspondence is a bijection between rings and which respects addition and multiplication, hence is a ring isomorphism. Proving that the image of is a subring of is trivial. QED

### State and Prove the 2nd Isomorphism Theorem for Rings

#### My Solution:

Let be a subgring and let be an ideal of . Then is a subring of , is an ideal of and

Proof:

1. is a subring and is an ideal, so . Let and be elements of . Then
2. and
3. Hence is a subring of .
4. The intersection is nonempty since is contained in and . Let and let . Then sinc and are both closed under addition. Furthermore and are in since is closed under multiplication from and is closed under multiplication. Thus is an ideal of .
5. Consider the map which sends an element to . THis is a ring homomorphism by definition of addition and multiplication in quotient rings (easy to prove). We claim that it is onto with kernel whcih would complete the proof by the first isomorphism theorem for rings. Consider the elements and . Then since , so and hence is onto. Let be an element of . THen which holds iff or equivalently if . Thus and by the first isomorphism theorem we have our result. QED

### State and Prove the 3rd Isomorphism Theroem for Rings

#### My Solution:

Let and be ideals of with . Then is an ideal of and .

Proof:

Since and are ideals, they are nonempty and so is also nonempty. Let and let . By definition of addition and multiplication of cosets, we have

and

Since is an ideal, and are contained in so is an ideal of . Consider the map that sends to . We claim that this is a well-defined onto homomorphism with kernel equal to . This is fairly obvious to see as every input has an image in . As for the kernel, take any where . Well, as well, and maps to because . Thus is the kernel. Thus we have proven the desired result by the first isomorphism theorem for rings. QED

## Definitions and Important Theorems (without proofs)

### Group Theory

* Hard to define in words, but remember what the dihedral group is (, where is the number of sides of the geometric representation).
* A map is a *homomorphism* if it maps a group to a group such that if and
* An *isomorphism* is a homomorphism that is a bijection
* The homomorphism given from to where is the permutation of the set is called the *permutation representation* associated to the given action.
* (One-Step-Subgroup Test) A subset of a group is a subgroup iff is nonempty and for all .
* Define . This subset of is called the *centralizer* of in .
* Define . This subset of is the *center*
* Define . Define the *normalizer* of in to be the set .
* The *kernel* of an action of on is defined as .
* A group is *cyclic* if can be generated by a single element, in other words, there exists some such that .
* If is a homomorphism of to , the *kernel* of is the set where is the identity of .
* Let be any subgroup of the group . The set of left cosets of in form a partition of . Furthermore, for all , iff .
* The element is called the *conjugate* of by . The set is called the *conjugate* of by . THe element is said to *normalize* if . A subgroup of is called *normal* if every element of cormalizes .
* (Lagrange's Theorem) If is a finite group and is a subgroup of , then the order of divides the order of , and the number of left cosets of in equals .
* If is a group and , the number of left cosets of in is called the *index* of in , denoted .
* If is a group of prime order , then is cyclic, hence .
* If is a finite group and , then the order of divides the order of . In particular for all .
* (Cauchy's Theorem) If is a finite group and is a prime dividing , then has an element of order .
* If and are finite subgroupd of a group then
* If and are subgroups of a group, is a subgroup iff .
* IF is a finite abelian group and is a prime dividing , then contains an element of order .
* A group is called *simple* if and the only normal subgroups of are and .
* In a group a sequence of subgroups is called a *composition series* if and is a simple group.
* If is a simple group of odd order, then for some prime .
* A group is *solvable* if there is a chain of subgroups such that is abelian for all .
* The permutation is odd iff the number of cycles of even length in its cycle decomposition is odd.
* A group action is *faithful* if its kernel is the identity.
* (Cayley's Theorem) Every group is isomorphic to a subgroup of some symmetric group. If is a group of order , then is isomorphic to a subgroup of .
* If is a finite group of order and is the smallest prime dividing , then any subgroup of index is normal.
* Two elements and of are said to be *conjugate* in is there is some such that . The orbits of acting on itself by conjugation are called the *conjugacy classes* of .
* (The Class Equation) .
* Let be a group. An isomorphism from onto itself is called an *automorphism* of .
* Let be a group and let . Conjugation by is called an *inner automorphism* of and the subgroup of consisting of all inner automorphisms is denoted by .
* A subgroup of a group is called *characteristic* in if every automorphism of maps to itself.
* (Sylow's Theorem) Let be a group of order where is a prime not dividing . Then: (i) Sylow -subgroups of exist, (ii) If is a Sylow -subgroup of and is any -subgroup of , then there exists such that , in particular two Sylow -subgroups of are conjugate in , and (iii) The number of Sylow -subgroups of is of the form , or .
* If is a Sylow -subgroup of , then the following are equivalent: is characteristic in ; is the unique Sylow -subgroup of (); is normal in .
* A *maximal subgroup* of a group is a proper subgroup of such that there are no subgroups of with .

### Ring Theory

* A *ring* is a set together with two binary operations and satisfying the following properties:

-- is an abelian group

-- is associative

-- The distributive law holds for

* A ring is commutative if multiplication is commutative.
* The ring is said to have an *identity* if there is an element such that for all .
* A ring with is called a *division ring* if every nonzero element has a multiplicative inverse. A commutative division ring is called a *field*.
* Let be a ring. A nonzero element of is called a *zero divisor* if there is a nonzero element such that either or .
* Assume has an identity . An element of is called a *unit* in if there is some in such that .
* A commutative ring with identity is called an *integral domain* if it has no zero divisors.
* A subring of the ring is a subgroup of that is closed under multiplication.
* Let and be rings. A *ring homomorphism* is a map satisfying:

1. for all
2. for all .

* The *kernel* of the ring homomorphism is the set of elements of that map to in .
* A bijective ring homomorphism is a *ring isomorphism*.
* Let and be rings and let be a homomorphism. Then the image of is a subgring of . Also, the kernel of is a subring of .
* Let be a ring and let be a subset of , and let $ r R$. and . A subset of is a *left ideal* of if is a subring and is closed under left multiplication by elements from , ie. for all . A right ideal is identical to this, just replace left with right. Then an *ideal* is a subset of that is both a left and a right ideal.
* Let . is the ideal generated by .
* Let be an ideal of . iff contains a unit. Assume is commutative. Then is a field iff its only ideals are and .
* An ideal in a ring is a *maximal ideal* if and the only ideals containing are and .
* Assume is commutative. The ideal is a maximal ideal iff the quotient ring is a field.
* Assume is commutative. An ideal is called a *prime ideal* if and whenever the product of two elements is an element of , then at least one of and is an element of .
* Any function with is called a *norm* on the integral domain . If for define to be a *positive norm*.
* The integral domain is said to be a *Euclidean Domain* if there is a norm on such that for any two elements and of with there exists elements and in such that
* A *Principle Ideal Domain* or *PID* is an integral domain in which every ideal is principal.
* Every nonzero prime ideal in a PID is a maximal ideal.
* If is any commutative ring such that the polynomial ring is a PID (or a Euclidean Domain), then is necessarily a field.
* Let be an integral domain. Suppose is nonzero and is not a unit. Then is called *irreducible* in if whenever with , at least one of or must be a unit in . Otherwise is \*reducible.
* Let be an integral domain. The nonzero element is called *prime* in if the ideal generated by is a prime ideal. In other words, a nonzero element isa prime if it is not a unit and whenever for any , then either or .
* Let be an integral domain. Two elements and of differing by a unit are said to be *associate* in .
* In an integral domain a prime element is always irreducible.
* In a PID a nonzero element is a prime iff it is irreducible.
* A *Unique Factorization Domain* or *UFD* is an integral domain in which every nonzero element which is not a unit has the following two proporties: (i) can be written as a finite product of irreducibles of (not necessarily distinct), so ; and (ii) the decomposition in (i) is *unique up to associates*, namely, if is another factorization of into irreducibles, then and there is some renumbering of the factors so that is associate to for all .
* In a UFD a nonzero element is a prime iff it's irreducible.
* The integers are a UFD
* finite fields fields Euclidean domains PIDs UFDs integral domains commutative rings
* If is a field, then is a PID and a UFD.
* (Gauss' Lemma) Let be a UFD with field of fractions and let . If is reducible in then is reducible in .
* is a UFD iff is a UFD.
* Let be a field and let . Then has a factor of degree one iff has a root in .
* (Eisenstein's Criterion) Let be a prime ideal of the integral domain and let be a polynomial in . Suppose are all elements of and suppose is not an element of . Then is irreducible in .

### Field and Galois Theory

* Let be fields. Then
* The *characteristic* of a field is defined to be the smallest positive integer such that if such a exists and is defined to be otherwise.
* The *prime subfield* of a field is the subfield of generated by the multiplicative identity of .
* If is a field containing the subfield , then is said to be an *extension field* of , denoted .
* The *degree* of a field extension denoted is the dimension of as a vector space over .
* Let be an extension of the field and let be a collection of elements in . Then the smallest subfield of containing both and the elements , denoted is called the field *generated* by over .
* If the field is generated by a single element over , , then is said to be a *simple* extension of and the element is called a *primitive element* for the extension.
* The element is said to be *algebraic* over if is a root of some nonzero polynomial . If is not algebraic over then is said to be *transcendental* over . The extension is said to be *algebraic* if every element of is algebraic over .
* Let be algebraic over . Then there is a unique monic irreducible polynomial which has as a root. A polynomial has as a root iff divides in .
* The element is algebraic over iff the simple extension is finite.
* If the extension is finite, then it's algebraic.
* Let be an arbitrary extension. Then the collection of elements of that are algebraic over form a subfield of .
* If is algebraic over and is algebraic over , then is algebraic over .
* THe extension field of is called a *splitting field* for the polynomial if factors completely into linear factors in and does not factor completely into linear factors over any proper subfield of containing .
* For any field , if then there exists an extension of which is a splitting field for .
* If is an algebraic extension of which is the splitting field over for a collection of polynomials then is called a *normal* extension of .
* (Uniqueness of Splitting Fields) Any two splitting fields for a polynomial over a field are isomorphic.
* A field is said to be *algebraically closed* if every polynomial with coefficients in has a root in .
* (Fundamental Theorem of Algebra) The field is algebraically closed.
* A polynomial over is called *separable* if it has no multiple roots.
* Let be a field of characteristic . Then for any ,
* Suppose that is a finite field of characteristic . Then every element of is a th power in .
* If is a subgroup of the group of automorphisms of , the subfield of fixed by all the elements of is called the *fixed field* of .
* Let be a finite extension. Then is said to be *Galois* over and is a *Galois* extension if . If is Galois the group of automorphisms is called the *Galois Group* of , denoted .
* If is the splitting field over of a separable polynomial then is Galois.
* If is a separable polynomial over , then the *Galois group of* over is the Galois group of the splitting field of over .
* Let be a subgroup of automorphisms of a field and let be the fixed field. Then .
* The extension is Galois iff is the splitting field of some separable polynomial over .
* (Fundamental Theorem of Galois Theory) Let be a Galois extension and set . Then there is an order reversing bijection between the subfields of containing and the subgroups of . Theorem continues, but this is biggest idea.