Math 313/623 Notes 5

David L. Meretzky

Thursday March 14th, 2019

> ...it's really more intelligent to be able to simplify things than to complicate them. Even if some people think it makes you look stupid.
>
> Eugenia Cheng

We will discuss the material of chapter 2 of Ireland and Rosen as well as some results of chapter 3. You should have notes 3 in front of you while reading notes 5. We will also develop the notion of a group and the notion of the group of units of a ring.

Applications of Unique Factorization

Infinitely Many Primes in $\mathbb{Z}$

Theorem 1. (Euclid) In the ring $\mathbb{Z}$ there are infinitely many primes.

Proof. Let us consider positive primes. List them increasingly,

$$p_1 = 2, p_2 = 3, ...$$

and for any $n \in \mathbb{Z}+$ we may define $N = (p_1 p_2 ... p_n) + 1$. Clearly, for i in the range from 1 to n, p_i does not divide N, for if $p_i | N$ we must have that $p_i | ((p_1 p_2 ... p_n) + 1)$ and since $p_i | (p_1 p_2 ... p_n)$ we must also have that $p_i | 1$, which is false. So none of the p_i divide N. On the other hand, every number N has a prime factorization and therefore, N is divisible by some new prime which is not in the list $p_1, ..., p_n$. In summary, given any prime p_n we can always show that there must exist a greater prime. Thus the set of primes must be infinite. □

Definition of a group

Before continuing we will require some new definitions. In the next few sections we will focus only on the multiplicative structure of rings. Recall that a ring is a set together with two operations (usually called multiplication and division) on that set which satisfy some axioms. Since we will only be interested in one operation we will define the notion of a group. A group is just like a ring except it has one operation only, and we require every element to have an inverse.

Definition 1. A group is a set, G together with a single operation $\circ$ (sometimes the operation will be written $+$ or $*$)[1] which satisfies the following axioms:

1. For all $g, h, k \in G$ we have $g \circ (h \circ k) = (g \circ h) \circ k$ (associativity)
2. There exists an element $e \in G$ such that for all $g \in G$, $e \circ g = g \circ e = g$ (identity)
3. For all $g \in G$, there exists an element $b \in G$ such that $g \circ b = b \circ g = e$ (inverses)[2]

Proposition 1. A ring R with addition $+$ and multiplication $*$ is also a group if we only consider the operation of addition.

Proof. Look back at the definition of a ring in notes 3. Note that the first three additive axioms, which the addition of R must statisfy, are exactly the group axioms. □

For example, $\mathbb{Z}$ with the usual operation of addition is a group.

The group of units, $U(G)$

Note however, that the addition of every ring is commutative by the fourth ring axiom. This requirement is not neccesary for groups, however if the operation of a group is commutative, then we call the group abelian. Hence, the set of ring elements together with the operation of addition of that ring is always an abelian group.
Let us now consider the multiplicative operation of a ring. This is a good time to review the definition of a unit from notes 3, reproduced below:

Definition 2. A non-zero element of a ring, $x \in R$, is called a unit if there exists an element $y \in R$ such that $x * y = 1$.

The final axiom of a group is the axiom of inverses. If we consider the set of ring elements together with multiplication, they fail to consititute a group because the multiplication need not satisfy the axiom of inverses. (Note that we require the multiplication to be associative and have a multiplicative identity, usually written 1.) In fact, 0, the additive identity of the ring, can never have a multiplicative inverse.

Proposition 2. The additive identity $0 \in R$ is not a unit.

[1] Recall that the definition of an operation give us that for all $f, g \in G$, $f \circ g$ must again be in G.

[2] if $\circ$ is written as addition then we usually write b as $-g$ and if $\circ$ is written as multiplication, then we usually write b as g^{-1}

Proof. We have $0 = 0 + 0$. Suppose there existed an element 0^{-1} such that $0 * 0^{-1} = 1$. Then

$$1 = 0 * 0^{-1} = (0 + 0) * 0^{-1} = 0 * 0^{-1} + 0 * 0^{-1} = 1 + 1$$

which is absurd. Thus there cannot be an element such that $0 * 0^{-1} = 1$. □

It follows that a ring R together with its multiplication never form a group. However, if we take just the collection of units in R and consider them with the operation of multiplication we obtain a group. However we need to make sure that the product of two units is again a unit. Multiplication will still be associative and will have an identity element since the multiplicative identity is itself a unit.

Proposition 3. Let R be a ring. Given two units $x, y \in R$, their product $x * y$ is again a unit of R.

Proof. Since x and y are units, they have inverses x^{-1} and y^{-1}. Note that

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

and therefore $y^{-1} * x^{-1}$ is an inverse for $x * y$. Thus $x * y$ is again a unit. □

Definition 3. Given a ring R we denote the collection of units in R, $U(R)$ and consider it with the operation of multiplication. We call $U(R)$ the group of units of R.

Proposition 4. Given a ring R, the group of units, $U(R)$, together with the multiplication of R actually form a group.

Proof. By the previous proposition given $x, y \in U(R)$, their product $x * y \in U(R)$. Thus the multiplication of R is an operation on $U(R)$. This multiplication will still be associative and will have an identity element since the multiplicative identity is itself a unit. Since every element of $U(R)$ is a unit, it has an inverse with respect to the group operation, multiplication. Thus we have verified that $*$ is an operation on $U(R)$ satisfying the group axioms. □

Example 1. Let $\mathbb{F}$ be a field. Since every field is a ring we may ask what is $U(\mathbb{F})$? Since every non-zero element of F is a unit we have $U(\mathbb{F}) = \mathbb{F} - \{0\}$, all elements of $\mathbb{F}$ except 0, viewed as a group with the operation being the multiplication of $\mathbb{F}$. The group of units of a field is sometimes denoted $\mathbb{F}^{\times}$.

Example 2. What is $U(\mathbb{Z}/p\mathbb{Z})$? In the case where the modulus is a prime p we have already shown in proposition 4 of notes 3 that $\mathbb{Z}/p\mathbb{Z}$ is a field. Thus by the previous exercise,

$$U(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} - \{0\}$$

with the operation of multiplication. Since $\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, 3, ..., p-1\}$ has p elements, $U(\mathbb{Z}/p\mathbb{Z})$ which has the same underlying set except it does not include 0, has $p - 1$ elements.

Example 3. We may also ask what is $U(\mathbb{Z}/n\mathbb{Z})$? The answer is contained in the following proposition

Proposition 5. If $a \in \mathbb{Z}/n\mathbb{Z}$ and $(a, n) = 1$, a and n are relatively prime, then a is a unit. Similarly, if $a \in \mathbb{Z}/n\mathbb{Z}$ and $(a, n) > 1$, a and n are not relatively prime, then a is a zero divisor.

The proof of this proposition is left as an exercise. Hint: examine the proof of proposition 4 of notes 3.

Associates, Primality, and Irreducibility

Definition 4. Let R be a ring, we say that two elements $r, s \in R$ are associates if there exists some unit $u \in R$ such that $r = us$.

Example 4. In $\mathbb{Z}$ the associates of a prime p are simply p and $-p$. In fact for any $n \in \mathbb{Z}$, since 1 and -1 are the only units, the only associates of n are n and $-n$.

Example 5. In $\mathbb{F}$, a field, every non-zero element is an associate of every other non-zero element. Let $x, y \in \mathbb{F}$, then we see that letting $u = x^{-1}y$, $xu = x(x^{-1}y) = y$. Furthermore since x^{-1} and y are units, their product u is a unit.

Now we need to sharpen our definition of *prime* and *irreducible*, and give general definitions for any ring.

Definition 5. Let R be a ring. A non-unit $p \in R$ is said to be prime if $p \neq 0$ and $p|ab$ implies that $p|a$ or $p|b$.

Definition 6. A element $p \in R$ is said to be irreducible if $a|p$ implies that either a is a unit or a is an associate of p.

Note: These definitions coincide for an aribitrary ring R, that is, every prime is irreducible and every irreducible element is prime if every ideal of R is generated by a single element. You should try to show this. For instance, these definitions coincide in $\mathbb{Z}$ and $k[x]$.

To conclude, we will see an example of a ring with where all primes are associates. In this case, there is essentially only one prime.

Definition 7. Let $p \in \mathbb{Z}$ be a prime number. Let $\mathbb{Z}_p$ be the set of all rational numbers a/b where p does not divide b.

Proposition 6. This is a ring with the usual addition and multiplication of $\mathbb{Q}$, the set of rationals.

Proof. This is an exercise. Recall the useful result that if p does not divide a and p does not divide b then p does not divide ab. □

Proposition 7. The units of $\mathbb{Z}_p$ are exactly the rationals a/b such that p does not divide both a and b.

Proof. This is an exercise. □

If $a/b \in \mathbb{Z}_p$ we can always express $a = p^l a'$ where p does not divide a'. Thus every element of $\mathbb{Z}_p$ can be expressed as a power of p times a unit, $a/b = p^l a'/b$.

Proposition 8. The only primes of $\mathbb{Z}_p$ are of the form pc/d where c/d is a unit. Conclude that all primes of $\mathbb{Z}_p$ are associate.

Proof. Suppose that a/b is a prime, that is, it has the property that if a/b divides $(c/d)(e/f)$, where $(c/d), (e/f) \in \mathbb{Z}_p$ then a/b divides (c/d) or (e/f) additionally a/b cannot be a unit. Suppose $a/b = p^j a'/b$ where a'/b is a unit and $j > 1$. Then a/b divides $(p^{j-1}a'/b)(p/1) = a/b$. Which implies that a/b divides either $(p^{j-1}a'/b)$ or $(p/1)$. Since the power of p appearing in both of these terms is less than j, this is impossible. Thus $j = 1$ or 0. Since a/b is prime, it is not a unit and therefore j cannot be 0. So $j = 1$.

Suppose now that $a/b = pa'/b$ where a'/b is a unit. We must show that a/b is prime. Clearly, a/b is not a unit since p divides pa'. Now suppose a/b divides a product

$$(c/d)(e/f) = (p^l c'/d)(p^k e'/f) = p^{k+l} c'e'/df$$

where c'/d, e'/f, and $c'e'/df$ are units. We must have that $k+l > 1$ thus either k or l is greater than 1 since k and l are positive integers. If $l > 1$ then a/b divides (c/d) and if $k > 1$ then a/b divides (e/f). □

So why does Euclid's proof fail for this ring $\mathbb{Z}_p$ which has only one prime up to associates?

Proposition 9. If $a/b \in \mathbb{Z}_p$ is not a unit, prove that $a/b + 1$ is a unit.

Proof. This is an exercise. □

Exercises

Find the number of elements of each of the following. Find the inverse of each element.

1. $U(\mathbb{Z})$
2. $U(\mathbb{Z}/2\mathbb{Z})$
3. $U(\mathbb{Z}/3\mathbb{Z})$
4. $U(\mathbb{Z}/4\mathbb{Z})$
5. $U(\mathbb{Z}/5\mathbb{Z})$

6. $U(\mathbb{Z}/6\mathbb{Z})$
7. $U(\mathbb{Z}/12\mathbb{Z})$
8. $U(k[x])$
9. Prove proposition 5.
10. Prove proposition 6.
11. Prove proposition 7.
12. Prove proposition 9.