Math 417 – Seventeenth Day

Bruce Reznick
University of Illinois at Urbana-Champaign

October 2, 2020

I'll begin with some review for the test, which will be in a week. I will repeat these frames in class on Friday, to give you a chance to ask questions, remind me of something I missed, etc.

Number theory topics: $\mathbb{Z}, \mathbb{Q}$, divisibility, $m \mid n$, congruence mod n, $a \equiv b \mod n$, $[a]_n$, prime numbers, gcd, $gcd(m, n)$, relatively prime integers, the existence of prime factorization, Euclidean Algorithm. Know what the Euler phi function $\phi(n)$ means, but you won't have to calculate it. Know that $gcd(m, n) = g$ implies that there exist integers r, s so that $g = mr + ns$ (findable through the EA) and if $gcd(m, n) = 1$ and $n \mid mr$, then $n \mid r$.

Group Theory Vocabulary: commutative, associative, binary operations, the definition of a group, and an identity and inverses in a group, abelian groups, cyclic groups ($C_n = \langle a \rangle, a^n = e$ or $(\mathbb{Z}/n\mathbb{Z}, \oplus)$, the symmetric group S_n in general, and in more detail S_3, the Klein group V and the dihedral group D_4.

More Group Theory: subgroups, $H \leq G$, the order of a group $|G|$, the order of an element in a group, isomorphisms, homomorphisms (plus kernel $Ker(\phi)$ and image $Im(\phi)$), left and right cosets of a subgroup, normal subgroup $H \trianglelefteq G$ and what that means, direct product of two groups $G \times H$, factor groups as a result of a normal subgroup, G/H consisting of the cosets of H. If $\phi : G \to H$ is a homomorphism, then $K = Ker(\phi) \trianglelefteq G$ and G/K is isomorphic to $Im(\phi)$.

More things to be able to do: Read a group multiplication table. If you know G and H, you should be able to work with $G \times H$ and if $gcd(m, n) = 1$, you should know that $C_m \times C_n \approx C_{mn}$. How to decide if a subset H of G is a subgroup, how to find the subgroups of cyclic groups and the connection with gcd, Lagrange's Theorem. How to compute the orders of elements in cyclic groups and in direct products.

With permutations, know cycles and transpositions. Write permutations in multiple ways, for example if $\pi : \{1,2,3,4\} \to \{1,2,3,4\}$ and $\pi(1) = 2, \pi(2) = 4, \pi(3) = 3, \pi(4) = 1$, then we might write this as:

$$\pi : 1 \mapsto 2 \mapsto 4 \mapsto 1, 3 \mapsto 3,$$

$$\pi = (124)(3), \quad \pi = (124), \qquad \pi = \begin{pmatrix} 1234 \\ 2431 \end{pmatrix}$$

Know how to multiply permutations in the right order.

Not on this test $\phi(n)$ (except incidentally as $|((\mathbb{Z}/n\mathbb{Z})^*, \odot)|$), repeating decimals as such, Cayley's Theorem, odd/even permutations, the book's theorem on the classification of finite abelian groups. What we've done this week on $Aut(G)$, i_g, etc.

Send me an email if there's something I missed.

Now we move on to the second main topic of this course, rings. This is an overview, and since we won't have homework due on this for two weeks, I'll just give mostly definitions. There are a lot of them.

A *ring* R is a set which has two binary operations ($+$ and $\cdot$) which fulfill the following rules:

The rings, under $+$, are an abelian group, so:

(i) $a, b \in R \implies a + b = b + a \in R$;

(ii) There exists an additive identity element, called 0_R, so that for all $a \in R$, $a + 0_R = 0_R + a = a$;

(iii) Every $a \in R$ has an inverse, called $-a$ so that $a \in R$, $a + (-a) = (-a) + a = 0_R$;

(iv) Associativity: $a, b, c \in R \implies (a + b) + c = a + (b + c) \in R$;

The rings, under $\cdot$, have very few rules:

(v) $a, b \in R \implies a \cdot b \in R$;

(vi) Associativity: $a, b, c \in R \implies (a \cdot b) \cdot c = a \cdot (b \cdot c)$;

The two operations are linked by the distributive law, both on the left and the right.

(vii) Distributivity: $a, b, c \in R \implies$

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad (a + b) \cdot c = a \cdot c + b \cdot c.$$

What isn't spoken of is not necessarily there.
We do not assume that multiplication is commutative.
We do not assume that there is a multiplicative identity.

If the ring R satisfies the additional condition

(viii) $a, b \in R \implies a \cdot b = b \cdot a \in R$

Then it is called a *commutative ring*.

Most of the rings we will deal with in the class are commutative rings. The most natural example of a non-commutative ring is

$$M_n(\mathbb{R}) := \{\text{the set of all } n \times n \text{ matrices with real entries}\}.$$

For matrices with integer coefficients, we'd have $M_n(\mathbb{Z})$, etc. Matrix rings are important, but 416 isn't a prerequisite for this section. I may mention 2×2 matrices occasionally as examples. The multiplication is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}.$$

This is not commutative. For example,

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$$

A ring R is called a *ring with unity* if it satisfies the additional condition

(ix) There exists a multiplicative identity element, written 1_R, so that, for all $a \in R$, $a \cdot 1_R = 1_R \cdot a = a$.

(Fraleigh calls the element 1_R a "unity".) If both (viii) and (ix) are satisfied, then R is called a *commutative ring with unity*.

There are more definitions coming, but you need some familiar examples.

The real numbers $\mathbb{R}$ with the usual operations are a commutative ring with unity $1_R = 1$ and $0_R = 0$. (These are the usual one and zero.) Addition is an abelian group, multiplication is associative and the distributive laws hold. All non-zero elements of $\mathbb{R}$ have the usual multiplicative inverse x^{-1}.

The rational numbers $\mathbb{Q}$ with the usual operations are a commutative ring with unity for the same reason. All non-zero elements of $\mathbb{Q}$ have the usual multiplicative inverse $(p/q)^{-1} = q/p$.

The integers $\mathbb{Z}$ with the usual operations are a commutative ring with unity. The only elements of $\mathbb{Z}$ which have a multiplicative inverse *in* $\mathbb{Z}$ are $\{-1, 1\}$. (For example $\frac{1}{2} \cdot 2 = 1$, but $\frac{1}{2} \notin \mathbb{Z}$.)

Consider $2\mathbb{Z}$, under the usual operations. We've already looked at this under addition and persuaded ourselves that it's an abelian group. The associative and distributive laws are "inherited" from $\mathbb{R}$, so this is a ring. It is commutative, but it doesn't have an identity! We have

$$2\mathbb{Z} = \{\ldots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\},$$

and the only possible multiplicative identity is 1, but $1 \notin 2\mathbb{Z}$, so $1_{2\mathbb{Z}}$ does not exist. This is true for $n\mathbb{Z}$ for every integer $n \geq 2$.

Another friend from our group days is a candidate for a ring, and this combines $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ and $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$ into one object.

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\},$$
$$[a]_n + [b]_n = [a+b]_n, \ [a]_n \cdot [b]_n = [ab]_n$$

The difference here is that we now do not limit multiplication to those $[k]_n$ with $gcd(k, n) = 1$.

For example, cut and pasting from the first week, with $n = 4$,

$\oplus$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

$\odot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$.

This is a commutative ring with unity $[1]_4$ and additive identity $[0]_4$. But notice $[2]_4 \cdot [2]_4 = [0]_4$. The product of two non-zero elements equal to zero. This leads to an important definition.

If $a, b \in R$ and $a \neq 0, b \neq 0$, but $ab = 0$, then a and b are called *zero divisors*. It is not very hard to show that with the definitions given so far, $\mathbb{Z}/n\mathbb{Z}$ has no zero divisors if and only if n is prime.

The ring of matrices has zero divisors. For example,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

An *integral domain* is a commutative ring with unity $1_R \neq 0_R$ which has no zero divisors. Think of $\mathbb{Z}$ as the natural example. (The condition $1_R \neq 0_R$ is a technicality we'll deal with later.)

Another example is coming up: polynomials.

Another familiar ring is the *ring of polynomials* over a ring R, which is written $R[x]$. So, for example $\mathbb{Z}[x]$ is the ring of polynomials with integer coefficients and $\mathbb{R}[x]$ is the ring of polynomials with real coefficients. One fun thing is that if we look at polynomials with coefficients in $\mathbb{Z}/n\mathbb{Z}$, then it is possible that we no longer have unique factorization: for example

$$x^2 + 7 = (x+1)(x+7) = (x+3)(x+5)$$

if we are only looking mod 8, because $(x+1)(x+7) = x^2 + 8x + 7$ and $(x+3)(x+5) = x^2 + 8x + 15$, and both of these reduce to $x^2 + 7$ mod 8. To be precise, the equation above is really

$$\begin{aligned} &[1]_8 x^2 + [0]_8 x + [7]_8 \\ &= ([1]_8 x + [1]_8)([1]_8 x + [7]_8) \\ &= ([1]_8 x + [3]_8)([1]_8 x + [5]_8). \end{aligned}$$

We will spend a fair bit of time on situations like these later in the semester.

One more piece of notation, if R is a ring with unity 1_R, $a \in R$ is called a *unit* if there exists $b \in R$ so that $ab = 1_R$. The set of units in a ring is written as $U(R)$ or R^*. (This is where I got the notation $(\mathbb{Z}/n\mathbb{Z})^*$.)

LEMMA If R is a ring, then $0_R \cdot x = 0_R$ for every $x \in R$. In particular, 0_R is not a unit.

PROOF. From the distributive law (and $0_R + 0_R = 0_R$), we have

$$0_R \cdot x = (0_R + 0_R) \cdot x = 0_R \cdot x + 0_R \cdot x \implies$$
$$-(0_R \cdot x) + 0_R \cdot x = -(0_R \cdot x) + (0_R \cdot x + 0_R \cdot x) \implies$$
$$-(0_R \cdot x) + 0_R \cdot x = (-(0_R \cdot x) + 0_R \cdot x) + 0_R \cdot x) \implies$$
$$0_R = 0_R + 0_R \cdot x \implies 0_R = 0_R \cdot x \quad \square$$

If $U(R) = R \setminus \{0_R\}$, then R is called a *division ring*. If a division ring is commutative, it is called a *field*. We will see that $\mathbb{C}, \mathbb{R}$ and $\mathbb{Q}$ are fields, as is $\mathbb{Z}/p\mathbb{Z}$ when p is prime.

What are the units in $\mathbb{R}[x]$? Let's talk informally about polynomials, there will be a formal definition later, but it does coincide with what you are familiar with, and both addition and multiplication are what you expect.

Well, when can we have polynomials p, q so that $p(x)q(x) = 1_{\mathbb{R}[x]}$? First of all what is $1_{\mathbb{R}[x]}$? If a polynomial is

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad a_j \in \mathbb{R},$$

and multiplication is what you expect, and $u(x) = 1$ is the constant polynomial, then $p(x)u(x) = u(x)p(x) = p(x)$ for all p, so $u(x) = 1_{\mathbb{R}[x]}$ is the constant polynomial.

Repeating the question, when can we have polynomials p, q so that $p(x)q(x) = 1$, where 1 is the constant polynomial. If you think about degrees (we'll do this formally later), p and q both have to be non-zero constant polynomials (degree zero), so

$$U(\mathbb{R}[x]) = \{a_0 \mid a_0 \neq 0\} = \mathbb{R}^* = \mathbb{R} \setminus \{0\}.$$

Finally, yes, there are ring homomorphisms too. Suppose R and R' are two rings. A map $\phi : R \to R'$ is called a *ring homomorphism* if for all $a, b \in R$, we have

$$\phi(a+b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a)\phi(b),$$

where the operations on a, b are the operations in R and those on $\phi(a), \phi(b)$ are the operations in R'. Yes, we have kernels and images and isomorphisms and automorphisms. All in due time.

I wanted to mention one non-intuitive homomorphism on $\mathbb{R}[x]$. We have polynomials as objects, we can add them and multiply them in the familiar way as objects. But they are also functions, and we can evaluate them.

Suppose $c \in \mathbb{R}$, the *evaluation homomorphism at* c, ϕ_c, which is a homomorphism from $\mathbb{R}[x] \to \mathbb{R}$, is defined by

$$\phi_c(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1 c + \cdots + a_n c^n; \quad \phi_c(p) = p(c).$$

As a small hint of further developments, what ought $Ker(\phi_c)$ be? I haven't given all the formal definitions, but by analogy,

$$Ker(\phi_c) = \{p(x) \ : \ \phi_c(p(x)) = 0_{\mathbb{R}}\} = \{p(x) \ : \ p(c) = 0\},$$

so the kernel is the set of polynomials which vanish at $x = c$. You probably know that, in this case, this condition is equivalent to being able to factor $p(x) = (x - c)q(x)$. We will look at some polynomial rings in which this is not the case.

One more thing, because I have half a frame to fill: if R and S are both rings then we define $R \times S$ in basically the same way we did for groups. The elements are $(r, s), r \in R, s \in S$ and for $r_i \in R$, $s_i \in S$,

$$(r_1, s_1)+(r_2, s_2) = (r_1+r_2, s_1+s_2), \ (r_1, s_1)\cdot(r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2),$$

where the operations in the first component take place in R and those in the second component take place in S.

Lots of fun left in the semester!