Lecture 15

Facts about groups, and examples of groups, I: Additive groups, units in a ring

15.1 Goals

1. Understand that every ring has an underlying additive group.

2. Understand that every ring gives rise to a group of units.

3. Begin to explore matrix groups

Last time we focused a lot on the idea of symmetry. After talking about what a set of symmetries ought to satisfy, we came upon the following definition of a group:

Definition 15.1.1 (See Definition 14.3.1)**.** A group is the data of a set G, together with a binary operation $m : G \times G \to G$ (for brevity, we will write $m(g, h)$ as gh) satisfying the following:

1. There is an element $e \in G$ so that, for every $g \in G$, we have $eg = ge = g$. (This e is unique, and we call it the identity element of G.)

2. Every $g \in G$ has an inverse. That is, there exists an element g^{-1} so that $gg^{-1} = g^{-1}g = e$. (This g^{-1} is unique.)

3. Finally, m is an associative operation. This means for every $g, h, k \in G$, we have $(gh)k = g(hk)$.

Today, we're going to see somewhat "formal" examples of groups. By this, I mean that the algebraic content will be our entry point, and the "symmetry" angle will be more obscure. That the notion of groups can be useful for both languages—the algebraic and the geometric—is a powerful feature of the theory.

15.2 Examples from rings

Let's establish the most concrete ways in which groups and rings are related. This also illustrates the two different roles that groups often play in nature; see Remark 15.2.11.

15.2.1 Groups under addition

Many abelian groups in nature have an "additive" feel about them, perhaps as insinuated by the following:

Proposition 15.2.1. Let R be a (not necessarily commutative) ring. Then R is an abelian group under addition. That is, the pair $(R, +)$ is an abelian group.

Proof. The defining properties 1, 2, and 3 of a group (see Definition 14.3.1) are the properties 1a, 1b, and 1d of a ring (see Definition 2.3.1), respectively. Finally, the requirement that addition be commutative (Property 1c of a ring) shows that R under addition is not only a group, but an abelian group. □

Example 15.2.2 (The additive structure of rings.)**.** All of the following are rings. In particular, all of the following are groups under addition:

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- $\mathbb{R}[x]$
- $M_2(\mathbb{R})$
- $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 0$.

15.2.2 Groups of units

In contrast, $(R, \times)$ is *not* a group. Two of three requirements for being a group are satisfied—$\times$ is associative, and the multiplicative identity 1 of R is an identity element for $\times$—but the element $0 \in R$ has no multiplicative inverse.

Even if we remove 0 from the situation, $(R \setminus \{0\}, \times)$ is not a group in general. For example, $M_2(\mathbb{R}) \setminus \{0\}$, the set of all non-zero 2-by-2 real matrices, is not a group under multiplication because some elements do not have multiplicative inverses. Consider for example the matrix

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

has no multiplicative inverse because it is a zero divisor (Exercise 15.5.1). This is again due to the fact that some elements do not have multiplicative inverses (due to the presence of zero divisors).

However, let's try restricting ourselves to a subset of R known to have multiplicative inverses:

Definition 15.2.3 (Units)**.** Let R be a (not necessarily commutative) ring. A *unit* of R is an element $x \in R$ for which there exists some $y \in R$ so that $xy = 1$ and $yx = 1$. We let

$$R^\times$$

denote the set of all units in R.

Remark 15.2.4. Be careful: The definition of unit requires that x is invertible "from the left and from the right." (So not just that $xy = 1$, but also that $yx = 1$.)

Sometimes, one needs only for x to be invertible from one side to guarantee that x is invertible from the other side.

If R is commutative, of course $xy = 1 \iff yx = 1$.

More generally: Suppose that x and y are elements of a ring R for which $xy = 1$. If R has no zero divisors, one can then conclude that x is a unit. For we have that

$$xy = 1 \implies yxy = y \implies (yx - 1)y = 0 \implies y = 0 \text{ or } xy = 1$$

(where the last implication follows by the assumption that R has no zero divisors). If $y = 0$, the beginning equality tells us that $0 = 1$ in this ring,

meaning R would be the trivial ring (in which case every element is a unit, because the trivial ring only has one element $0 = 1$). If R is not the trivial ring, then we conclude $xy = 1$, meaning x is a unit.

Proposition 15.2.5. Let R be a (not necessarily commutative ring).

(a) If x is a unit and x' is a unit, the xx' is a unit.

(b) $(R^\times, \times)$ is a group. (That is, the units of R are a group under multiplication.)

(c) In particular, if R is a field, then $(R \setminus \{0\}, \times)$ is a group. In fact, it is an abelian group.[1]

Proof. (a) Suppose x and x' are units. That means there exist elements y and y' for which $xy = yx = 1$ and $y'x' = x'y' = 1$. I claim that $y'y$ is a multiplicative inverse to xx'. Behold:

$$(y'y)(xx') = y'(yx)x' = y'1x' = y'x' = 1$$

where the first equality is associativity, the next is the fact that $yx = 1$, and the last equality again uses that $y'x' = 1$. One can likewise prove that $(xx')(y'y) = 1$, so proving the claim.

(b) By the previous paragraph, we see that the set of units is closed under multiplication. So multiplication indeed defines a binary operation on the set of units. 1 is obviously a unit, and serves as a multiplicative identity of $(R^\times, \times)$. $R^\times$ has inverses because if x is a unit, its inverse y is also a unit (you should think through this if this isn't clear to you yet; it's a worthwhile exercise to clear confusion). Finally, multiplication is associative by the assumption that R is a ring. This shows $(R^\times, \times)$ satisfies all the properties of being a group (Definition 14.3.1).

(c) By definition, if R is a field, every non-zero element is a unit. Hence the set of units $R^\times$ is equal to $R \setminus \{0\}$. Again by definition of field, multiplication is commutative, so $R \setminus \{0\}$ is an abelian group, as claimed. □

To summarize: Any ring R naturally gives rise to two groups. An abelian group given by $(R, +)$, and a not-necessarily abelian group given by the group of units $(R^\times, \times)$.

So, let's talk about specific examples of the above.

[1] This is a rare example of an abelian group that does not have an "additive feel."

Example 15.2.6 (Units of $\mathbb{Z}/n\mathbb{Z}$ for small values of n)**.** We refer to the multiplication tables in (12.2.3.1) for verification of the claims below. (If you want to know whether an element a has a multiplicative inverse, you simply need to check whether the row containing a contains 1.)

Let's consider the ring $\mathbb{Z}/2\mathbb{Z}$. It groups of units consists of one element called 1.

In the ring $\mathbb{Z}/4\mathbb{Z}$, we see that only the elements 1 and 3 have multiplicative inverses. (3 is its own inverse!) So $(\mathbb{Z}/4\mathbb{Z})^\times$ is a group with two elements.

In the ring $\mathbb{Z}/5\mathbb{Z}$, every non-zero element has a multiplicative inverse. So the group of units $(\mathbb{Z}/5\mathbb{Z})^\times$ is a group with 4 elements.

Remark 15.2.7. We have now seen two groups with four elements: The units of $\mathbb{Z}/5\mathbb{Z}$, and the symmetries of a (non-square) mattress. We will later see that the size of a group only says so much—two groups of the same size might be inequivalent. We will soon define the notion of a *group isomorphism* to articulate ways in which two groups are equivalent. For now, you could wonder: Are these two groups with four elements equivalent in some way? How would you articulate that?

Example 15.2.8 (Units of some polynomial rings)**.** Let R be an integral domain (so R is commutative and has no zero divisors; our favorite example of $R = \mathbb{R}$ is in fact a field).

What are the units of the polynomial ring $R[x]$?

By definition of unit, a polynomial p is a unit if and only if there's another polynomial q for which $pq = 1$. You have seen that when you multiply polynomials, degrees add in $R[x]$ so long as R is an integral domain (Proposition 7.3.26). So the fact that p is a unit means there is some polynomial q for which

$$\deg(p) + \deg(q) = \deg(1) = 0.$$

But for this equality to hold, we must have that $\deg(p) = \deg(q) = 0$. In other words, if p is a unit, it must be a degree 0 polynomial—i.e., a constant polynomial.

So when does a constant polynomial p have a multiplicative inverse? Precisely when p (considered as an element of R) has a multiplicative inverse. What we have proven is

$$(R[x])^\times = R^\times$$

when R is an integral domain. (This equality is made precise if one thinks of R as a subset of $R[x]$.)

So when R is an integral domain, the polynomial ring doesn't really give us any new group of units—the group of units of $R[x]$ is equivalent to the group of units of R.

Remark 15.2.9. When R is not an integral domain, $R[x]$ can have some interesting units. For example, if there is a non-zero element a of R which squares to zero, then

$$(1 + ax)(1 - ax) = 1 - a^2x^2 = 1$$

so that linear polynomials can be units. An example is when $R = \mathbb{Z}/8\mathbb{Z}$ and $a = 4$.

Example 15.2.10. Consider the ring $M_2(\mathbb{R})$. Then the group of units $M_2(\mathbb{R})^\times$ is the set of all 2-by-2 matrices that admit a multiplicative inverse—that is, the collection of all invertible linear transformations. This group is written

$$GL_2(\mathbb{R}).$$

More generally, for any $n \geq 0$, the set of n-by-n invertible matrices forms a group (under matrix multiplication), and this group is denoted

$$GL_n(\mathbb{R}).$$

Each of these is called the *(real) general linear group*.

Remark 15.2.11. Groups often play two different roles in mathematical practice.

First, they might be the object of study themselves. A question like "What is the group of symmetries of a square mattress?" or "Can we understand $GL_n(\mathbb{R})$" are questions that can draw the curiosity of many mathematicians.

Second, they are often tools of computation. This is most obvious for groups like $\mathbb{Z}$ and $\mathbb{R}$, where "numbers" feel like a very useful tool for quantifying things. But groups like $\mathbb{Z}/n\mathbb{Z}$—even without considering their ring structure, and only remembering their additive structure—are used all the time in computation.

15.2.3 $GL_2(\mathbb{Z}/2\mathbb{Z})$

Recall that for any ring R, we could define $M_n(R)$, the ring of n-by-n matrices with entries in R (Theorem 3.5.2).

Definition 15.2.12. For any ring R, we let $GL_n(R)$ denote the group of units of $M_n(R)$.

In words, $GL_n(R)$ is the group of invertible n-by-n matrices with entries in a ring R. We saw the case $R = \mathbb{R}$ in Example 15.2.10.

Remark 15.2.13. This remark will assume some linear algebra knowledge.

For any commutative ring R, one can define the determinant of an n-by-n matrix with entries in R using the usual formula from linear algebra. One can further prove that $\det(AB) = \det(A)\det(B)$. You can verify this for yourself for the case of 2-by-2 matrices; for higher rank matrices, you can see a proof in a linear algebra class.

Because the determinant respects multiplication, and knowing that the determinant of the identity matrix is always 1, we see that for A to be invertible (i.e., for A to be a unit in $M_n(R)$) it must have a unit determinant (i.e., $\det(A)$ must be in $R^\times$). Conversely, by Cramer's rule (which works for matrices with entries in any commutative ring) any matrix with a determinant in $R^\times$ admits an inverse.

The upshot: $GL_n(R)$ can be identified exactly with those matrices for which the determinant is a unit of R.

Let's work out the example of $n = 2$ with the ring $R = \mathbb{Z}/2\mathbb{Z}$.

First, note that $M_2(\mathbb{Z}/2\mathbb{Z})$ has exactly $2^4 = 16$ elements. This is because there are four entries in a 2-by-2 matrix (so there are four choices to be made) while there are only 2 elements in $\mathbb{Z}/2\mathbb{Z}$ (so there are 2 options for each choice).

By Remark 15.2.13, $GL_2(\mathbb{Z}/2\mathbb{Z})$ consists exactly of those matrices whose determinants are non-zero.

Given a 2-by-2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the determinant is computed by $ad - bc$. So we see that for a matrix to have non-zero determinant, the first column must therefor not identically be zero. So any $A \in GL_2(\mathbb{Z}/2\mathbb{Z})$ must have one of the following three possible first-columns:

$$\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \qquad \begin{pmatrix} 1 & b \\ 1 & d \end{pmatrix} \qquad \begin{pmatrix} 0 & b \\ 1 & d \end{pmatrix}$$

Now, for the determinant to be non-zero, the column given by entries b and d must simply not equal the first column and not equal 0. For each of the above three first-column possibilities, this leaves exactly 2 options for the second column. So $GL_2(\mathbb{Z}/2\mathbb{Z})$ has six elements, listed as follows:

$$\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix} \quad \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix} \quad \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$$

$$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} \quad \begin{pmatrix}1 & 0\\1 & 1\end{pmatrix} \quad \begin{pmatrix}0 & 1\\1 & 1\end{pmatrix}$$

This groups is not abelian. Behold:

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

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

So this is our first explicit example of a non-abelian group of order six.

Remark 15.2.14. It turns out that this is the *smallest* non-abelian group possible.

15.3 Some useful facts about computations in a group

We have so far seen examples of geometry (symmetries of mattresses) and of algebra (the additive group of a ring, and the units of a ring). It is *powerful* that such different examples fit under the same umbrella of "group," because general facts about groups will apply in all of these settings. Let's discover some facts that are used all the time.

Proposition 15.3.1 (Cancellation law)**.** Let G be a group. Suppose that g, h, k are three elements for which $gh = gk$. Then $h = k$.

Likewise, if $hg = kg$, then $h = k$.

Remark 15.3.2. The above are sometimes called the left cancellation and right cancellation laws. We will bundle the two and call the proposition a single "cancellation law" for short.

Proof. There exists a (unique) element $g^{-1} \in G$ for which $gg^{-1} = e$ and $g^{-1}g = e$. Thus

$$\begin{aligned} gh = gk &\implies g^{-1}(gh) &&= g^{-1}(gk) \\ &\implies (g^{-1}g)h &&= (g^{-1}g)k \\ &\implies eh &&= ek \\ &\implies h &&= k. \end{aligned}$$

The first implication is by "multiplying both sides by g^{-1}." (We are applying the multiplication function m to the pairs (g^{-1}, gh) and (g^{-1}, gk). That $gk = gh$ means the outputs are identical.) The second implication is the associative property of the group operation, applied to both sides of the equality. The next implication follows by definition of inverse. The last is by definition of the identity element e.

A similar proof shows the right cancellation law:

$$\begin{aligned} hg = hk &\implies (hg)g^{-1} &&= (kg)g^{-1} \\ &\implies h(gg^{-1}) &&= k(gg^{-1}) \\ &\implies he &&= ke \\ &\implies h &&= k. \end{aligned}$$

□

Here is a useful corollary:

Corollary 15.3.3. Let G be a group. If $g \in G$ is an element for which $g^2 = g$, then $g = e$.

Proof. If $g^2 = g$, then we may write

$$gg = ge.$$

By the cancellation law, we conclude $g = e$. □

Remark 15.3.4. In any setting with a binary operation, an element satisfying $x^2 = x$ is called an *idempotent*. (For example, a diagonal matrix whose only diagonal entries are 0s and 1s is an idempotent matrix.) The corollary says that in a group, the only idempotent element is the identity element.

The following says that the process of "taking inverses" reverses the order of multiplication:

Proposition 15.3.5. Let G be a group. For any $g, h \in G$, we have that $(gh)^{-1} = h^{-1}g^{-1}$.

Proof. Let $x = h^{-1}g^{-1}$. We must prove that $x(gh) = e$ and $(gh)x = e$ to show that x is the inverse to gh. Observe:

$$\begin{aligned} x(gh) &= (h^{-1}g^{-1})(gh) \\ &= (h^{-1}g^{-1}g)h \\ &= h^{-1}(g^{-1}g)h \\ &= h^{-1}eh \\ &= h^{-1}h \\ &= e. \end{aligned} \tag{15.3.0.1}$$

The first equality is the definition of x, the next two equalities follow from the associative property of the group operation, and the last equalities are by definition of inverse. Likewise we observe:

$$\begin{aligned} (gh)x &= (gh)(h^{-1}g^{-1}) \\ &= g(hh^{-1}g^{-1}) \\ &= g(hh^{-1})g^{-1} \\ &= geg^{-1} \\ &= gg^{-1} \\ &= e. \end{aligned} \tag{15.3.0.2}$$

□

The following says that—even though the definition of an inverse to g required the inverse to be both a left- and right- inverse—it suffices to check that an element inverts g on only one side to conclude that it inverts g from both sides.

Proposition 15.3.6. Let G be a group. For any $g, h \in G$, we have that $gh = e$ if and only if $hg = e$. (In other words, any left inverse to g is automatically a right inverse to g, and hence an inverse to g; and vice versa.)

Proof. Assume that h is an element for which $gh = e$. Then, by multiplying both sides by h on the left, we have that $hgh = h$. By the right cancellation law (multiplying by h^{-1} on the right) we see that$hg = e$. A similar proof shows that $hg = e \implies gh = e$. □

15.4 Comparing groups

When studying rings, a ring homomorphism $f : R \to S$ was a kind of function respecting ring structures (of addition and multiplication and multiplicative unit). A ring isomorphism was a ring homomorphism that was also a bijection—and this articulated a sense in which the ring structure of R can be made to look identical to that of S.

Likewise, we'll want a group homomorphism to respect group operations, and a group isomorphism to exhibit a way in which two groups look identical.

Definition 15.4.1. Let G and H be two groups. A function $f : G \to H$ is called a *group homomorphism* if for every $g, g' \in G$, we have that $f(gg') = f(g)f(g')$.

Recall that for a ring homomorphism, even though we only asked that $+$, $\times$, and 1 be respected, it turned out further structures like additive inverse and 0 are respected. The same is true of group homomorphisms:

Proposition 15.4.2. Suppose $f : G \to H$ is a group homomorphism. Then:

(a) Let $e_g \in G$ and $e_H \in H$ be the identity elements. Then $f(e_G) = e_H$. (So group homomorphisms automatically respect identity elements.)

(b) For any $g \in G$, $f(g)^{-1} = f(g^{-1})$. (So group homomorphisms automatically respect inverses.)

Proof. (a) We observe:

$$f(e_G)f(e_G) = f(e_G e_G) = f(e_G)$$

where the first equality uses the fact that f is a group homomorphism, and the last follows by applying the function f to the equality $e_G e_G = e_G$. Then $f(e_G)$ is an idempotent, but Corollary 15.3.3 tells us that the only idempotent in a group H is the identity element of H. Hence $f(e_G) = e_H$.

(b) We observe the following:

$$f(g^{-1})f(g) = f(g^{-1}g) = f(e_G) = e_H$$

where the first equality is by definition of group homomorphism, the next equality is true by applying f to both sides of the equation $g^{-1}g = e$, and the last equality is the first part of the proposition. This shows that $f(g^{-1})$ is a left inverse to $f(g)$. By proposition 15.3.6 —which shows that any one-sided inverse is in fact a (two-sided) inverse—we see that $f(g^{-1}) = (f(g))^{-1}$. □

Finally, the following notion gives us a way to detect when two groups behave indistinguishably:

Definition 15.4.3. We say that a group homomorphism f is a group *isomorphism* if f is a bijection.

Proposition 15.4.4. Let $f : G \to H$ be a group isomorphism.

1. Then the inverse function to f is a group isomorphism.
2. Let $f' : H \to K$ be another group isomorphism. Then $f' \circ f$ is also a group isomorphism.

Remark 15.4.5. Let G and H be two groups. If there exists a group isomorphism from G to H, we say that G and H are isomorphic. *However*, you should make a habit of remembering your favorite group isomorphisms. Just remembering that G and H are isomorphic tells you there is some way to view the two as equivalent; but without remembering the isomorphism itself, you will not know *how* to view them as equivalent.

Here is a related issue. Every group G is isomorphic to itself, because the function $g \mapsto g$ is a function from G to itself that is a bijection and a homomorphism. But a group G can have many other interesting isomorphisms to itself!

For example, let $G = \mathbb{Z}$ under addition. The operation $n \mapsto -n$ is a group isomorphism to itself.

15.4.1 The power of group isomorphisms

In Section 15.2.3 we saw the group $GL_2(\mathbb{Z}/2\mathbb{Z})$. I told you then that it was the smallest non-abelian group possible.

It turns out that there is another non-abelian group of order 6 (i.e., a non-abelian group with 6 elements), written D_6, defined to be the symmetries of an equilateral triangle. Moreover, it turns out that D_6 is isomorphic to $GL_2(\mathbb{Z}/2\mathbb{Z})$.

What would a group isomorphism $f : D_6 \to GL_2(\mathbb{Z}/2\mathbb{Z})$ do for us?

Well, the way that we would compute the group operation in D_6 woudl be *geometric*. Just as we composed rotations of a mattress to study the group operation of the symmetry group of a mattress, we would futz around with an equilateral triangle to understand how the triangle's symmetries compose.

On the other hand, the way to compute the group operation in $GL_2(\mathbb{Z}/2\mathbb{Z})$ is purely *algebraic*—it's just matrix multiplication involving 0s and 1s.

The power of the group isomorphism f is that it allows you to compute group operations in either of these settings, and be able to make conclusions about the group operation in the other. If you're a geometry guru, you love it because you get to avoid multiplying matrices, and you also get to think of a somewhat abstract 2-by-2 matrix with $\mathbb{Z}/2\mathbb{Z}$ entries as behaving like a geometric object—e.g., behaving like a rotation or reflection of a triangle.

Or, if you're an algebra guru and if you also don't have geometric intuitions about things, you're happy because you can learn about geometry through doing simple computations of matrices.

(Note also how much easier it is to have a computer multiply matrices; it's more involved to try to represent geometric operations without using matrices in some way.)

15.5 Exercises

Exercise 15.5.1. Let R be a ring. Recall that a *zero divisor* of R is a non-zero element $x \in R$ for which there exists some non-zero $y \in R$ satisfying $xy = 0$ or $yx = 0$.

(a) Show that if x is a zero divisor, then x cannot be a unit.

(b) Conversely, suppose that R is a ring for which $0 \neq 1$ (so R has at least two elements). Show that if x is a unit, then x cannot be a zero divisor.

Exercise 15.5.2. (a) Prove Proposition 15.4.4.

(b) Prove the analogous statement for rings.

Exercise 15.5.3. Let G and H be groups, and suppose they are isomorphic. This intuitively means that G and H should look identical, but this intuition is vague. Let's see it play out.

Show the following:

1. G is abelian if and only if H is.
2. G contains an element $g \neq e_G$ for which $g^5 = e_G$ if and only if H contains an element $h \neq e_H$ for which $h^5 = e_H$. (e_G and e_H are the identity elements of G and H, respectively.)

3. Fix a group K. Then G is isomorphic to K if and only if H is isomorphic to K.

Exercise 15.5.4. For the following examples of G and H, write down (i) all group homomorphisms from G to H, and (ii) all group isomorphisms from G to H.

(a) $G = \mathbb{Z}/2\mathbb{Z}$ and $H = \mathbb{Z}/3\mathbb{Z}$ (both under addition).

(b) $G = H = \mathbb{Z}/3\mathbb{Z}$ (under addition).

(c) $G = \mathbb{Z}^\times$ (the group of units of the ring $\mathbb{Z}$) and $H = \mathbb{Z}/2\mathbb{Z}$.

(d) $G = \mathbb{Q}$ and $H = \mathbb{Z}$ (both under addition).

(e) $G = \mathbb{Z}$ and $H = GL_2(\mathbb{R})$.

(f) $G = \mathbb{Z}$ and H is any group.

Exercise 15.5.5. Complete Exercise 14.5.1.