

ALGEBRA HANDOUT 1: RINGS, FIELDS AND GROUPS

PETE L. CLARK

1. RINGS

Recall that a binary operation on a set S is just a function $* : S \times S \rightarrow S$: in other words, given any two elements s_1, s_2 of S , there is a well-defined element $s_1 * s_2$ of S .

A **ring** is a set R endowed with two binary operations $+$ and \cdot , called addition and multiplication, respectively, which are required to satisfy a rather long list of familiar-looking conditions – in all the conditions below, a, b, c denote arbitrary elements of R –

- (A1) $a + b = b + a$ (commutativity of addition);
- (A2) $(a + b) + c = a + (b + c)$ (associativity of addition);
- (A3) There exists an element, called 0, such that $0 + a = a$. (additive identity)
- (A4) For $x \in R$, there is a $y \in R$ such that $x + y = 0$ (existence of additive inverses).
- (M1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associativity of multiplication).
- (M2) There exists an element, called 1, such that $1 \cdot a = a \cdot 1 = a$.
- (D) $a \cdot (b + c) = a \cdot b + a \cdot c$; $(a + b) \cdot c = a \cdot c + b \cdot c$.

Comments:

(i) The additive inverse required to exist in (A4) is unique, and the additive inverse of a is typically denoted $-a$. (It is easy to check that $-a = (-1) \cdot a$.)

(ii) Note that we require the existence of a multiplicative identity (or a “unity”). Every once in a while one meets a structure which satisfies all the axioms except does not have a multiplicative identity, and one does not eject it from the club just because of this. But all of our rings will have a multiplicative identity.

(iii) There are two further reasonable axioms on the multiplication operation that we have *not* required; our rings will sometimes satisfy them and sometimes not:

- (M') $a \cdot b = b \cdot a$ (commutativity of multiplication).
- (M'') For all $a \neq 0$, there exists $b \in R$ such that $ab = 1$.

A ring which satisfies (M') is called – sensibly enough – a **commutative ring**.

Example 1.0: The integers \mathbb{Z} form a ring under addition and multiplication. Indeed they are “the universal ring” in a sense to be made precise later.

Thanks to Kelly W. Edenfield and Laura Nunley (x3) for pointing out typos in these notes.

Example 1.1: There is a unique ring in which $1 = 0$. Indeed, if r is any element of such a ring, then

$$r = 1 \cdot r = 0 \cdot r = (0 + 0) \cdot r = 0 \cdot r + 0 \cdot r = 1 \cdot r + 1 \cdot r = r + r;$$

subtracting r from both sides, we get $r = 0$. In other words, the only element of the ring is 0 and the addition laws are just $0 + 0 = 0 = 0 \cdot 0$; this satisfies all the axioms for a commutative ring. We call this the **zero ring**. Truth be told, it is a bit of annoyance: often in statements of theorems one encounters “except for the zero ring.”

Example 1.n: For any positive integer, let Z_n denote the set $\{0, 1, \dots, n - 1\}$. There is a function mod_n from the positive integers to Z_n : given any integer m , $\text{mod}_n(m)$ returns the remainder of m upon division by n , i.e., the unique integer r satisfying $m = qn + r$, $0 \leq r < n$. We then define operations of $+$ and \cdot on Z_n by viewing it as a subset of the positive integers, employing the standard operations of $+$ and \cdot , and then applying the function mod_n to force the answer back in the range $0 \leq r < n$. That is, we define

$$a +_n b := \text{mod}_n(a + b),$$

$$a \cdot_n b := \text{mod}_n(a \cdot b).$$

The addition operation is familiar from “clock arithmetic”: with $n = 12$ this is how we tell time, except that we use $1, 2, \dots, 12$ instead of $0, \dots, 11$. (However, military time does indeed go from 0 to 23.)

The (commutative!) rings Z_n are basic and important in all of mathematics, especially number theory. The definition we have given – the most “naive” possible one – is not quite satisfactory: how do we know that $+_n$ and \cdot_n satisfy the axioms for a ring? Intuitively, we want to say that the integers \mathbb{Z} form a ring, and the Z_n ’s are constructed from \mathbb{Z} in some way so that the ring axioms become automatic. This leads us to the *quotient construction*, which we will present later.

Modern mathematics has tended to explore the theory of commutative rings much more deeply and systematically than the theory of (arbitrary) non-commutative rings. Nevertheless noncommutative rings are important and fundamental: the basic example is the ring of $n \times n$ matrices (say, with real entries) for any $n \geq 2$.

A ring (except the zero ring!) which satisfies (M'') is called a **division ring** (or division algebra). Best of all is a ring which satisfies (M') and (M'') : a **field**.¹

I hope you have some passing familiarity with the fields \mathbb{Q} (of rational numbers), \mathbb{R} (of real numbers) and \mathbb{C} (of complex numbers), and perhaps also with the existence of finite fields of prime order (more on these later). In some sense a field is the richest possible purely algebraic structure, and it is tempting to think of the elements

¹A very long time ago, some people used the term “field” as a synonym for “division ring” and therefore spoke of “commutative fields” when necessary. The analogous practice in French took longer to die out, and in relatively recent literature it was not standardized whether “corps” meant any division ring or a commutative division ring. (One has to keep this in mind when reading certain books written by Francophone authors and less-than-carefully translated into English, e.g. Serre’s *Corps Locaux*.) However, the Bourbakistic linguistic philosophy that the more widely used terminology should get the simpler name seems to have at last persuaded the French that “corps” means “(commutative!) field.”

of field as “numbers” in some suitably generalized sense. Conversely, elements of arbitrary rings can have some strange properties that we would, at least initially, not want “numbers” to have.

2. RING HOMOMORPHISMS

Generally speaking, a **homomorphism** between two algebraic objects is a map f between the underlying sets which preserves all the relevant algebraic structure.

So a **ring homomorphism** $f : R \rightarrow S$ is a map such that $f(0) = 0$, $f(1) = 1$ and for all $r_1, r_2 \in R$, $f(r_1 + r_2) = f(r_1) + f(r_2)$, $f(r_1 r_2) = f(r_1) f(r_2)$.

In fact it follows from the preservation of addition that $f(0) = 0$. Indeed, $0 = 0 + 0$, so $f(0) = f(0 + 0) = f(0) + f(0)$; now subtract $f(0)$ from both sides. But in general it seems better to postulate that a homomorphism preserve every structure “in sight” and then worry later about whether any of the preservation properties are redundant. Note well that the property $f(1) = 1$ – “unitality” – is *not* redundant. Otherwise every ring R would admit a homomorphism to the zero ring, which would turn out to be a bit of a pain.

Example 2.1: For any ring R , there exists a unique homomorphism $c : \mathbb{Z} \rightarrow R$. Namely, any homomorphism must send 1 to 1_R , 2 to $1_R + 1_R$, 3 to $1_R + 1_R + 1_R$, -1 to -1_R , -2 to $-1_R + -1_R$ and so forth. (And it is not hard to see that this necessarily gives a homomorphism.)

Recall that a function $f : X \rightarrow Y$ is an **injection** if $x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$. To see whether a homomorphism of rings $f : R \rightarrow S$ is an injection, it suffices to look at the set $K(f) = \{x \in R \mid f(x) = 0\}$, the **kernel** of f . This set contains 0, and if it contains any other element then f is certainly not injective. The converse is also true: suppose $K(f) = 0$ and $f(x_1) = f(x_2)$. Then $0 = f(x_2) - f(x_1) = f(x_2 - x_1)$, so $x_2 - x_1 \in K(f)$, so by our assumption $x_2 - x_1 = 0$, and $x_1 = x_2$.

An important case is when R is a ring and S is a subset of R containing 0 and 1 and which is itself a ring under the operations of $+$ and \cdot – it inherits from R . (In this case what needs to be checked are the *closure* of S under $+$, $-$ and \cdot : i.e., for all $s_1, s_2 \in S$, $s_1 + s_2$, $s_1 - s_2$, $s_1 \cdot s_2 \in S$.) We say that S is a **subring** of R .

Suppose R and S are division rings and $f : R \rightarrow S$ is a homomorphism between them. Suppose that r is in the kernel of f , i.e., $f(r) = 0$. If $r \neq 0$, then it has a (left and right) multiplicative inverse, denoted r^{-1} , i.e., an element such that $rr^{-1} = r^{-1}r = 1$. But then

$$1 = f(1) = f(rr^{-1}) = f(r)f(r^{-1}) = 0 \cdot f(r^{-1}) = 0,$$

a contradiction. So any homomorphism of division rings is an injection: it is especially common to speak of **field extensions**. For example, the natural inclusions $\mathbb{Q} \hookrightarrow \mathbb{R}$ and $\mathbb{R} \hookrightarrow \mathbb{C}$ are both field extensions.

Example 2.1, continued: recall we have a unique homomorphism $c : \mathbb{Z} \rightarrow R$. If c is injective, then we find a copy of the integers naturally as a subring of R . E.g. this is the case when $R = \mathbb{Q}$. If not, there exists a least positive integer n such that

$c(n) = 0$, and one can check that $\text{Ker}(c)$ consists of all integer multiples of n , a set which we will denote by $n\mathbb{Z}$ or by (n) . This integer n is called the **characteristic** of R , and if no such n exists we say that R is of characteristic 0 (yes, it would seem to make more sense to say that n has infinite characteristic). As an important example, the homomorphism $c: \mathbb{Z} \rightarrow Z_n$ is an extension of the map mod_n to all of \mathbb{Z} ; in particular the characteristic of Z_n is n .

3. INTEGRAL DOMAINS

A commutative ring R (which is not the zero ring!) is said to be an **integral domain** if it satisfies either of the following *equivalent* properties:²

(ID1) If $x, y \in R$ and $xy = 0$ then $x = 0$ or $y = 0$.

(ID2) If $a, b, c \in R$, $ab = ac$ and $a \neq 0$, then $b = c$.

(Suppose R satisfies (ID1) and $ab = ac$ with $a \neq 0$. Then $a(b - c) = 0$, so $b - c = 0$ and $b = c$; so R satisfies (ID2). The converse is similar.)

(ID2) is often called the “cancellation” property and it is extremely useful when solving equations. Indeed, when dealing with equations in a ring which is not an integral domain, one must remember *not* to apply cancellation without further justification! (ID1) expresses the nonexistence of **zero divisors**: a nonzero element x of a ring R is called a zero divisor if there exists y in R such that $xy = 0$.

An especially distressing kind of zero divisor is an element $0 \neq a \in R$ such that $a^n = 0$ for some positive integer n . (If N is the least positive integer N such that $a^N = 0$ we have $a, a^{N-1} \neq 0$ and $a \cdot a^{N-1} = 0$, so a is a zero divisor.) Such an element is called **nilpotent**, and a ring is **reduced** if it has no nilpotent elements.

One of the difficulties in learning ring theory is that the examples have to run very fast to keep up with all the definitions and implications among definitions. But, look, here come some now:

Example 3.1: Let us consider the rings Z_n for the first few n .

The rings Z_2 and Z_3 are easily seen to be fields: indeed, in Z_2 the only nonzero element, 1 is its own multiplicative inverse, and in Z_3 $1 = 1^{-1}$ and $2 = (2)^{-1}$.

In the ring Z_4 $2^2 = 0$, so 2 is nilpotent and Z_4 is nonreduced.

In Z_5 one finds – after some trial and error – that $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$ so that Z_5 is a field.

In Z_6 we have $2 \cdot 3 = 0$ so there are zero-divisors, but a bit of calculation shows there are no nilpotent elements. (We take enough powers of every element until we get the same element twice; if we never get zero then no power of that element will be zero. For instance $2^1 = 2$, $2^2 = 4$, $2^3 = 2$, so 2^n will equal either 2 or 4 in Z_6 : never 0.)

²The terminology “integral domain” is completely standardized but a bit awkward: on the one hand, the term “domain” has no meaning by itself. On the other hand there is also a notion of an “integral extension of rings” – which we will meet in Handout A3 – and, alas, it may well be the case that an extension of integral domains is not an integral extension! But there is no clear remedy here, and proposed changes in the terminology – e.g. Lang’s attempted use of “entire” for “integral domain” – have not been well received.

Similarly we find that Z_7 is a field, 2 is a nilpotent in Z_8 , 3 is a nilpotent in Z_9 , Z_{10} is reduced but not an integral domain, and so forth. Eventually it will strike us that it appears to be the case that Z_n is a field exactly when n is prime. This realization makes us pay closer attention to the prime factorization of n , and given this clue, one soon guesses that Z_n is reduced iff n is **squarefree**, i.e., not divisible by the square of any prime. Moreover, it seems that whenever Z_n is an integral domain, it is also a field. All of these observations are true in general but nontrivial to prove. The last fact is the easiest:

Proposition 1. *Any integral domain R with finitely many elements is a field.*

Proof: Consider any $0 \neq a \in R$; we want to find a multiplicative inverse. Consider the various powers a^1, a^2, \dots of a . They are, obviously, elements of R , and since R is finite we must eventually get the same element via distinct powers: there exist positive integers i and j such that $a^{i+j} = a^i \neq 0$. But then $a^i = a^{i+j} = a^i \cdot a^j$, and applying (ID2) we get $a^j = 1$, so that a^{j-1} is the multiplicative inverse to a .

Theorem 2. *a) The ring Z_n is a field iff n is a prime.
b) The ring Z_n is reduced iff n is squarefree.*

Proof: In each case one direction is rather easy. Namely, if n is not prime, then $n = ab$ for integers $1 < a, b < n$, and then $a \cdot b = 0$ in Z_n . If n is not squarefree, then for some prime p we can write $n = p^2 \cdot m$, and then the element mp is nilpotent: $(mp)^2 = mp^2m = mn = 0$ in Z_n .

However, in both cases the other direction requires Euclid's Lemma: if a prime p divides ab then $p|a$ or $p|b$. (We will encounter and prove this result early on in the course.) Indeed, this says precisely that if $ab = 0$ in Z_n then either $a = 0$ or $b = 0$, so Z_p is an integral domain, and, being finite, by Proposition 1 it is then necessarily a field. Finally, if $n = p_1 \cdots p_n$ is squarefree, and $m < n$, then m is not divisible by some prime divisor of n , say p_i , and by the Euclid Lemma neither is any power m^a of m , so for no positive integer a is $m^a = 0$ in Z_n .

Example 3.2: Of course, the integers \mathbb{Z} form an integral domain. How do we know? Well, if $a \neq 0$ and $ab = ac$, we can multiply both sides by a^{-1} to get $b = c$. This may at first seem like cheating since a^{-1} is generally not an integer: however it exists as a rational number and the "computation" makes perfect sense in \mathbb{Q} . Since $\mathbb{Z} \subset \mathbb{Q}$, having $b = c$ in \mathbb{Q} means that $b = c$ in \mathbb{Z} .

It turns out that for *any* commutative ring R , if R is an integral domain we can prove it by the above argument of exhibiting a field that contains it:

Theorem 3. *A ring R is an integral domain iff it is a subring of some field.*

Proof: The above argument (i.e., just multiply by a^{-1} in the ambient field) shows that any subring of a field is an integral domain. The converse uses the observation that given an integral domain R , one can formally build a field $F(R)$ whose elements are represented by formal fractions of the form $\frac{a}{b}$ with $a \in R, b \in R \setminus \{0\}$, subject to the rule that $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$ in R . There are many little checks to make to see that this construction actually works. On the other hand, this is a direct generalization of the construction of the field \mathbb{Q} from the integral domain \mathbb{Z} , so we feel relatively sanguine about omitting the details here.

Remark: The field $F(R)$ is called the **field of fractions**³ of the integral domain R .

Example 3.3 (Subrings of \mathbb{Q}): There are in general many different integral domains with a given quotient field. For instance, let us consider the integral domains with quotient field \mathbb{Q} , i.e., the subrings of \mathbb{Q} . The two obvious ones are \mathbb{Z} and \mathbb{Q} , and it is easy to see that they are the extremes: i.e., for any subring R of \mathbb{Q} we have $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$. But there are many others: for instance, let p be any prime number, and consider the subset R_p of \mathbb{Q} consisting of rational numbers of the form $\frac{a}{b}$ where b is not divisible by any prime except p (so, taking the convention that $b > 0$, we are saying that $b = p^k$ for some k). A little checking reveals that R_p is a subring of \mathbb{Q} . In fact, this construction can be vastly generalized: let S be any subset of the prime numbers (possibly infinite!), and let R_S be the rational numbers $\frac{a}{b}$ such that b is divisible only by primes in S . It is not too hard to check that: (i) R_S is a subring of \mathbb{Q} , (ii) if $S \neq S'$, $R_S \neq R_{S'}$, and (iii) every subring of \mathbb{Q} is of the form R_S for some set of primes S . Thus there are uncountably many subrings in all!

4. POLYNOMIAL RINGS

Let R be a commutative ring. One can consider the ring $R[T]$ of polynomials with coefficients in T : that is, the union over all natural numbers n of the set of all formal expressions $\sum_{i=0}^n a_i T^i$ ($T^0 = 1$). (If $a_n \neq 0$, this polynomial is said to have degree n . By convention, we take the zero polynomial to have degree $-\infty$.) There are natural addition and multiplication laws which reduce to addition in R , the law $T^i \cdot T^j = T^{i+j}$ and distributivity. (Formally speaking we should write down these laws precisely and verify the axioms, but this is not very enlightening.) One gets a commutative ring $R[T]$.

One can also consider polynomial rings in more than one variable: $R[T_1, \dots, T_n]$. These are what they sound like; among various possible formal definitions, the most technically convenient is an inductive one: $R[T_1, \dots, T_n] := R[T_1, \dots, T_{n-1}][T_n]$, so e.g. the polynomial ring $R[X, Y]$ is just a polynomial ring in one variable (called Y) over the polynomial ring $R[X]$.

Proposition 4. $R[T]$ is an integral domain iff R is an integral domain.

Proof: R is naturally a subring of $R[T]$ – the polynomials rT^0 for $r \in R$ and any subring of an integral domain is a domain; this shows necessity. Conversely, suppose R is an integral domain; then any two nonzero polynomials have the form $a_n T^n + a_{n-1} T^{n-1} + \dots + a_0$ and $b_m T^m + \dots + b_0$ with $a_n, b_m \neq 0$. When we multiply these two polynomials, the leading term is $a_n b_m T^{n+m}$; since R is a domain, $a_n b_m \neq 0$, so the product polynomial has nonzero leading term and is therefore nonzero.

Corollary 5. A polynomial ring in any number of variables over an integral domain is an integral domain.

This construction gives us many “new” integral domains and hence many new fields. For instance, starting with a field F , the fraction field of $F[T]$ is the set of all formal

³The term “quotient field” is also used, even by me until rather recently. But since there is already a quotient construction in ring theory, it seems best to use a different term for the fraction construction.

quotients $\frac{P(T)}{Q(T)}$ of polynomials; this is denoted $F(T)$ and called the field of rational functions over F . (One can equally well consider fields of rational functions in several variables, but we shall not do so here.)

The polynomial ring $F[T]$, where F is a field, has many nice properties; in some ways it is strongly reminiscent of the ring \mathbb{Z} of integers. The most important common property is the ability to divide:

Theorem 6. (*Division theorem for polynomials*) Given any two polynomials $a(T)$, $b(T)$ in $F[T]$, there exist unique polynomials $q(T)$ and $r(T)$ such that

$$b(T) = q(T)a(T) + r(T)$$

and $\deg(r(T)) < \deg(a(T))$.

A more concrete form of this result should be familiar from high school algebra: instead of formally proving that such polynomials exist, one learns an algorithm for actually finding $q(T)$ and $r(T)$. Of course this is as good or better: all one needs to do is to give a rigorous proof that the algorithm works, a task we leave to the reader. (Hint: induct on the degree of b .)

Corollary 7. (*Factor theorem*) For $a(T) \in F[T]$ and $c \in F$, the following are equivalent:

- a) $a(c) = 0$.
- b) $a(T) = q(T) \cdot (T - c)$.

Proof: We apply the division theorem with $b(T) = (T - c)$, getting $a(T) = q(T)(T - c) + r(T)$. The degree of r must be less than the degree of $T - c$, i.e., zero – so r is a constant. Now plug in $T = c$: we get that $a(c) = r$. So if $a(c) = 0$, $a(T) = q(T)(T - c)$; the converse is obvious.

Corollary 8. A nonzero polynomial $p(T) \in F[T]$ has at most $\deg(p(T))$ roots.

Remark: The same result holds for polynomials with coefficients in an integral domain R , since every root of p in R is also a root of p in the fraction field $F(R)$.

This may sound innocuous, but do not underestimate its power – a judicious application of this Remark (often in the case $R = \mathbb{Z}/p\mathbb{Z}$) can and will lead to substantial simplifications of “classical” arguments in elementary number theory.

Example 4.1: Corollary 8 does *not* hold for polynomials with coefficients in an arbitrary commutative ring: for instance, the polynomial $T^2 - 1 \in \mathbb{Z}_8[T]$ has degree 2 and 4 roots: 1, 3, 5, 7.

5. COMMUTATIVE GROUPS

A **group** is a set G endowed with a single binary operation $*$: $G \times G \rightarrow G$, required to satisfy the following axioms:

- (G1) for all $a, b, c \in G$, $(a * b) * c = a * (b * c)$ (associativity)
- (G2) There exists $e \in G$ such that for all $a \in G$, $e * a = a * e = a$.
- (G3) For all $a \in G$, there exists $b \in G$ such that $ab = ba = e$.

Example: Take an arbitrary set S and put $G = \text{Sym}(S)$, the set of all bijections

$f : S \rightarrow S$. When $S = \{1, \dots, n\}$, this is called the **symmetric group** of order n , otherwise known as the group of all permutations on n elements: it has order $n!$.

We have notions of **subgroups** and **group homomorphisms** that are completely analogous to the corresponding ones for rings: a subgroup $H \subset G$ is a subset which is nonempty, and is closed under the group law and inversion: i.e., if $g, h \in H$ then also $g * h$ and g^{-1} are in H . (Since there exists some $h \in H$, also h^{-1} and $e = h * h^{-1} \in H$; so subgroups necessarily contain the identity.)⁴ And a homomorphism $f : G_1 \rightarrow G_2$ is a map of groups which satisfies $f(g_1 * g_2) = f(g_1) * f(g_2)$ (as mentioned above, that $f(e_{G_1}) = e_{G_2}$ is then automatic). Again we get many examples just by taking a homomorphism of rings and forgetting about multiplication.

Example 5.1: Let F be a field. Recall that for any positive integer n , the $n \times n$ matrices with coefficients in F form a ring under the operations of matrix addition and matrix multiplication, denoted $M_n(F)$. Consider the subset of invertible matrices, $GL_n(F)$. It is easy to check that the invertible matrices form a group under matrix multiplication (the “unit group” of the ring $M_n(F)$, coming up soon). No matter what F is, this is an interesting and important group, and is not commutative if $n \geq 2$ (when $n = 1$ it is just the group of nonzero elements of F under multiplication). The determinant is a map

$$\det : GL_n(F) \rightarrow F \setminus \{0\};$$

a well-known property of the determinant is that $\det(AB) = \det(A)\det(B)$. In other words, the determinant is a homomorphism of groups. Moreover, just as for a homomorphism of rings, for any group homomorphism $f : G_1 \rightarrow G_2$ we can consider the subset $K_f = \{g \in G_1 \mid f(g) = e_{G_2}\}$ of elements mapping to the identity element of G_2 , again called the **kernel** of f . It is easy to check that K_f is always a subgroup of G_1 , and that f is injective iff $K_f = 1$. The kernel of the determinant map is denoted $SL_n(F)$; by definition, it is the collection of all $n \times n$ matrices with determinant 1.⁵ For instance, the rotation matrices $\begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix}$ form a subset (indeed, a subgroup) of the group $SL_2(\mathbb{R})$.

Theorem 9. (*Lagrange*) *For a subgroup H of the finite group G , we have $\#H \mid \#G$.*

The proof⁶ is combinatorial: we exhibit a partition of G into a union of subsets H_i , such that $\#H_i = \#H$ for all i . Then, the order of G is $\#H \cdot n$, where n is the number of subsets.

The H_i 's will be the **left cosets** of H , namely the subsets of the form

$$gH = \{gh \mid h \in H\}.$$

Here g ranges over all elements of G ; the key is that for $g_1, g_2 \in G$, the two cosets g_1H and g_2H are either equal or disjoint – i.e., what is not possible is for them to

⁴Indeed there is something called the “one step subgroup test”: a nonempty subset $H \subset G$ is a subgroup iff whenever g and h are in H , then $g * h^{-1} \in H$. But this is a bit like saying you can put on your pants in “one step” if you hold them steady and jump into them: it’s true but not really much of a time saver.

⁵The “GL” stands for “general linear” and the “SL” stands for “special linear.”

⁶This proof may be too brief if you have not seen the material before; feel free to look in any algebra text for more detail, or just accept the result on faith for now.

share some but not all elements. To see this: suppose $x \in g_1H$ and is also in g_2H . This means that there exist $h_1, h_2 \in H$ such that $x = g_1h_1$ and also $x = g_2h_2$, so $g_1h_1 = g_2h_2$. But then $g_2 = g_1h_1h_2^{-1}$, and since $h_1, h_2 \in H$, $h_3 := h_1h_2^{-1}$ is also an element of H , meaning that $g_2 = g_1h_3$ is in the coset g_1H . Moreover, for any $h \in H$, this implies that $g_2h = g_1h_3h = g_1h_4 \in g_1H$, so that $g_2H \subset g_1H$. Interchanging the roles of g_2 and g_1 , we can equally well show that $g_1H \subset g_2H$, so that $g_1H = g_2H$. Thus overlapping cosets are equal, which was to be shown.

Remark: In the proof that G is partitioned into cosets of H , we did not use the finiteness anywhere; this is true for all groups. Indeed, for any subgroup H of any group G , we showed that there is a set S – namely the set of distinct left cosets $\{gH\}$ such that the elements of G can be put in bijection with $S \times H$. If you know about such things (no matter if you don't), this means precisely that $\#H$ divides $\#G$ even if one or more of these cardinalities is *infinite*.

Corollary 10. *If G has order n , and $g \in G$, then the order of g – i.e., the least positive integer k such that $g^k = 1$ – divides n .*

Proof: The set of all positive powers of an element of a finite group forms a subgroup, denoted $\langle g \rangle$, and it is easily checked that the distinct elements of this group are $1, g, g^2, \dots, g^{k-1}$, so the order of g is also $\#\langle g \rangle$. Thus the order of g divides the order of G by Lagrange's Theorem.

Example 5.2: For any ring R , $(R, +)$ is a commutative group. Indeed, there is nothing to check: a ring is simply more structure than a group. For instance, we get for each n a commutative group Z_n just by taking the ring Z_n and forgetting about the multiplicative structure.

A group G is called **cyclic** if it has an element g such that every element x in G is of the form $1 = g^0, g^n := g \cdot g \cdot \dots \cdot g$ or $g^{-n} = g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}$ for some positive integer n . The group $(\mathbb{Z}, +)$ forms an infinite cyclic group; for every positive integer n , the group $(Z_n, +)$ is cyclic of order n . It is not hard to show that these are the only cyclic groups, up to isomorphism.

An element u of a ring R is a **unit** if there exists $v \in R$ such that $uv = vu = 1$.

Example 5.3: 1 is always a unit; 0 is never a unit (except in the zero ring, in which $0 = 1$). The units in \mathbb{Z} are ± 1 .

A nonzero ring is a division ring iff every nonzero element is a unit.

The set of all units in a ring is denoted R^\times . It is not hard to see that the units form a group under multiplication: for instance, if u and v are units, then they have two-sided inverses denoted u^{-1} and v^{-1} , and then

$$uv \cdot (v^{-1}u^{-1}) = (v^{-1}u^{-1})uv = 1,$$

so uv is also a unit. Similarly, the (unique) inverse u^{-1} of a unit is a unit. In general, R^\times is not commutative, but of course it will be if R is commutative.