2. Orders of Group Elements

2.1. Elementary number theory. Let us begin by recalling a few notions and ideas that have to do with divisibility of integers. If \( m, n \) are integers, we say that \( m \) divides \( n \) and write \( m \mid n \) if there exists an integer \( k \) such that \( n = mk \). (For example, every integer divides 0; and if \( n \) is an integer, then \( 0 \mid n \) if and only if \( n = 0 \).) Given integers \( m, n \), not both zero, the greatest common divisor of \( m \) and \( n \) is the largest integer \( d \) such that \( d \) divides both \( m \) and \( n \) (it clearly exists because 1 divides \( m \) and \( n \), and the set of all integers between 1 and \( m \) or \( n \) is finite). We write \( d = \gcd(m, n) \).

Example 2.1. We have \( \gcd(-4, -26) = 2 \) (note that the g.c.d. is always positive!).

Two integers, \( m \) and \( n \) (not both 0), are said to be relatively prime if \( \gcd(m, n) = 1 \). In general, the most important property of the g.c.d. is the following one. Let \( m, n \) be integers, not both 0, put \( d = \gcd(m, n) \), and let \( k \) be an arbitrary integer. Then \( k \) divides \( d \) if and only if \( k \) divides both \( m \) and \( n \). The next result is also very useful.

Lemma 2.2. If \( m, n \) are nonzero integers and \( d = \gcd(m, n) \), then there exist \( a, b \in \mathbb{Z} \) such that \( d = am + bn \).

Sketch of a proof. We give a proof of the existence of \( a, b \) that is constructive, i.e., it yields an explicit algorithm for finding \( a \) and \( b \) in practice. That algorithm is called the Euclidean algorithm. Without loss of generality, we may assume that \( m, n > 0 \) (if, for instance, \( m < 0 \), we can replace \( m \) with \(-m\) without changing \( d \) and without affecting the conclusion of the lemma). Further, switching \( m \) and \( n \) if necessary, we may assume that \( n \geq m \). Now use division with remainder to write \( n = mq + r \) where \( q, r \) are integers such that \( q \geq 1 \) and \( 0 \leq r \leq m - 1 \). Consider two cases. If \( r = 0 \), this means that \( m \) divides \( n \), so \( d = m \) and the proof of the lemma is complete (take \( a = 1 \) and \( b = 0 \)). So from now on we assume that \( 1 \leq r \leq m - 1 \).

Observe that \( \gcd(m, n) = \gcd(m, r) \). To see this, it suffices to note that if \( k \) is an integer, then \( k \) divides both \( m \) and \( n \) if and only if \( k \) divides both \( m \) and \( r \). Indeed, if \( k \) divides \( m \) and \( n \), then \( k \) also divides \( r \) because \( r = n - mq \), and conversely, if \( k \) divides \( m \) and \( r \), then \( k \) also divides \( n \) because \( n = mq + r \).

But by construction, \( r < m \). So if we replace the original pair of integers \((m, n)\) with the pair \((r, m)\), we may assume by induction\(^1\) that the lemma holds for the pair \((r, m)\). This means that we can write \( d = a'r + b'm \) for some \( a', b' \in \mathbb{Z} \), so that \( d = a'(n - mq) + b'm = a'n + (b' - a'q)m \), which proves the lemma by taking \( a = b' - a'q \) and \( b = a' \). □

\(^1\)If you want to extract an actual algorithm out of this proof, you have to keep going in the same way: use division with remainder to write \( n = rq_2 + r_2 \), where \( q_2 \geq 1 \) and \( 0 \leq r_2 \leq r - 1 \), then apply the same process to \((r, r_2)\), and so on, until at some stage you reach a remainder that is equal to 0. I also recommend [http://en.wikipedia.org/wiki/Euclidean_algorithm](http://en.wikipedia.org/wiki/Euclidean_algorithm) for additional information.
2.2. Definitions and basic properties. Let \( G \) be a group. An element \( g \in G \) is said to have finite order if there exists an integer \( d \geq 1 \) for which \( g^d = e \) (as always, \( e \) denotes the identity element of \( G \) unless explicitly indicated otherwise). In this case the smallest such \( d \) is called the order of \( g \). If no such \( d \) exists, we say that \( g \) has infinite order.

Lemma 2.3. If \( G \) is a finite group, then every element \( g \in G \) has finite order.

Remark 2.4. Later we will see that if \( G \) is finite, then the order of every element of \( G \) divides \( |G| \) (the number of elements of \( G \)); we don’t quite know enough to prove that yet.

Lemma 2.5. Let \( G \) be any group (not necessarily finite), let \( g \in G \) be an element of finite order and write \( d \) for the order of \( g \). Given an integer \( n \), we have \( g^n = e \iff d \mid n \).

Corollary 2.6. Let \( f : G \to H \) be a homomorphism of groups and let \( g \in G \).
(a) If \( g \) has finite order in \( G \), then \( f(g) \) has finite order as an element of \( H \), and the order of \( f(g) \) divides the order of \( g \).
(b) If \( f \) is injective, then \( g \) has finite order in \( G \) if and only if \( f(g) \) has finite order as an element of \( H \), in which case the orders of \( g \) and \( f(g) \) are equal.

Proof. As we saw in class, for any integer \( n \), we have \( f(g)^n = f(g^n) \). In particular, if \( g^n = e_G \), then \( f(g)^n = e_H \). Moreover, if \( f \) is injective, then the converse is also true: if \( f(g)^n = e_H \), then \( g^n = e_G \). So both (a) and (b) easily follow from the last lemma.

Lemma 2.7. Suppose that \( G \) is a group, \( g \in G \) is an element of finite order and \( d \) is the order of \( g \). For any integer \( k \), the element \( g^k \) also has finite order, equal to \( d/\gcd(k,d) \).

Proof. First, \( g^k \) has finite order because \( (g^k)^d = (g^d)^k = e^k = e \). Next, let \( m \geq 1 \) be an integer. Then \( (g^k)^m = e \iff g^{mk} = e \iff d \mid mk \) by the previous lemma. Now it is easy to check that the smallest positive integer \( m \) such that \( d \mid mk \) is equal to \( d/\gcd(k,d) \), which implies the assertion of the lemma.

2.3. Simple examples.
(1) If \( G \) is one of the groups \((\mathbb{Z},+)\) or \((\mathbb{Q},+\)) or \((\mathbb{R},+\)) or \((\mathbb{C},+)\), then \( 0 \) (which is the identity element of \( G \)) is the only element of finite order in \( G \). The reason is that in these examples, the \( n \)-th power of an element \( x \in G \) is equal to \( n \cdot x \) (the usual product of two numbers). If \( n \neq 0 \), then \( n \cdot x \) can only be 0 if \( x = 0 \).

(2) If \( G = (\mathbb{R}^\times,\cdot) \) is the group of nonzero real numbers under multiplication, its only elements of finite order are 1 and \(-1\). Note that 1 has order 1 and \(-1\) has order 2.

(3) If \( G = (\mathbb{C}^\times,\cdot) \) is the group of nonzero complex numbers under multiplication, then \( G \) has infinitely many elements of finite order, and we can describe all of them. Namely, if \( n \geq 1 \) and \( k \) are integers, then \( z(n,k) := \exp(2\pi ik/n) \) is an element of finite order in \( \mathbb{C}^\times \), and every element of finite order in \( \mathbb{C}^\times \) has this form for some choice of \( n \) and \( k \). The order of \( z(n,k) \) is equal to \( n/\gcd(k,n) \).
(4) If \( n \geq 3 \) is an integer and \( G = D_n \) is the dihedral group of rigid motions of a regular \( n \)-gon (as usual, the group operation is composition of motions in this case), we recall that there are two types of elements in \( G \): rotations and reflections. Each reflection has order 2. Rotation by \( 2\pi k/n \) radians around the center of the polygon has order \( n/\gcd(k,n) \).

(5) Let \( N \geq 1 \) be an integer and consider the group \( G = \mathbb{Z}/N\mathbb{Z} \) of remainders modulo \( N \), the group operation being addition of remainders. It is clear (why?) that the order of \( \bar{1} \in G \) is equal to \( N \). The last lemma implies that for any integer \( k \), the order of \( \bar{k} \) in \( \mathbb{Z}/N\mathbb{Z} \) is equal to \( N/\gcd(k,N) \), because \( \bar{k} \) is the \( k \)-th power of \( \bar{1} \).

2.4. Another example. Here is a variation of the last example, which shows that the problem of computing orders of elements of a finite group could be pretty difficult even for commutative groups. (The example we will construct also plays an important role in many other situations, including the RSA algorithm in cryptography.)

Let \( N \geq 1 \) be an integer and consider again the set \( \mathbb{Z}/N\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \bar{N-1}\} \) of remainders modulo \( N \). Aside from addition, this set has another natural operation, namely, multiplication of remainders: we can define \( \bar{k} \cdot \bar{m} \) to be the remainder of dividing \( km \) by \( N \). This operation is associative, and it also has an identity, namely, \( \bar{1} \). However, we don’t get a group yet, because not every element has an inverse. It is clear that to get a group, we have to at least throw away \( \bar{0} \), but we may also have to throw away other elements: for instance, \( \bar{2} \) does not have an inverse under multiplication modulo 4.

**Lemma 2.8.** If \( k \) is an integer, then \( k \) has an inverse under multiplication modulo \( N \) if and only if \( k \) and \( N \) are relatively prime.

**Proof.** First, here is a more concrete reformulation. Note that \( k \) has an inverse under multiplication modulo \( N \) if and only if there is another integer \( m \) such that \( km - 1 \) is divisible by \( N \). So we are claiming that this happens if and only if \( \gcd(k,N) = 1 \).

For the “only if” direction, suppose that \( m \) is an integer such that \( km - 1 \) is divisible by \( N \). Now if \( d \geq 1 \) is any integer that divides both \( k \) and \( N \), then \( d \) also divides \( km - 1 \) and therefore \( d \mid 1 \), which means that \( d = 1 \). This shows that \( \gcd(k,N) = 1 \).

Conversely, suppose that \( \gcd(k,N) = 1 \). Lemma 2.2 (the Euclidean algorithm) implies that there exist \( a, b \in \mathbb{Z} \) such that \( ak + bN = 1 \). Taking \( m = a \), we find that \( km - 1 = -bN \) is divisible by \( N \), proving the lemma.

**Definition 2.9.** Let \( N \geq 1 \) be an integer and let \((\mathbb{Z}/N\mathbb{Z})^\times \subset \mathbb{Z}/N\mathbb{Z}\) denote the subset consisting of all remainders \( \bar{k} \) for which \( k \) is relatively prime to \( N \).

The last lemma implies that \((\mathbb{Z}/N\mathbb{Z})^\times \) is a group with respect to multiplication of remainders. This is a finite commutative group whose order is usually denoted \( \varphi(N) \); this is called Euler’s phi function or Euler’s totient function of \( N \).
Remark 2.10. For this finite group, there is no “easy” formula for the order of a given element. Just for fun, you can try the following. Let $N = p$ be an odd prime, so that 2 belongs to the group $(\mathbb{Z}/p\mathbb{Z})^\times$, and try to find the order of 2 as a function of $p$.

2.5. **Injective group homomorphisms.** We finish with a useful remark about the notion of an injective group homomorphism, which came up in Corollary 2.6(b).

Suppose that $G, H$ are groups and $f : G \rightarrow H$ is a homomorphism. By definition, $f$ is injective if and only if, given elements $g_1, g_2 \in G$ such that $f(g_1) = f(g_2)$, it necessarily follows that $g_1 = g_2$. However, because $f$ is a homomorphism and not just an arbitrary map of sets, there is a shortcut.

**Definition 2.11.** The kernel of $f$ is the subset $\text{Ker}(f) = \{g \in G \mid f(g) = e_H\}$.

One can easily check that $\text{Ker}(f)$ is a subgroup of $G$.

**Lemma 2.12.** A group homomorphism $f : G \rightarrow H$ is injective if and only if its kernel is trivial, i.e., $\text{Ker}(f) = \{e_G\}$.

**Proof.** We have $f(e_G) = e_H$, so if $f$ is injective, then $f(g) \neq e_H$ for any $g \neq e_G$, which means that $\text{Ker}(f)$ is trivial. Conversely, suppose that $\text{Ker}(f) = \{e_G\}$ and let $g_1, g_2 \in G$ be such that $f(g_1) = f(g_2)$. Then $f(g_1^{-1}g_2) = f(g_1^{-1})f(g_2) = f(g_1)^{-1}f(g_2) = e_H$, so $g_1^{-1}g_2 \in \text{Ker}(f)$. By hypothesis, this means that $g_1^{-1}g_2 = e_G$, whence $g_1 = g_2$. \qed

Remark 2.13. There is no similar shortcut for checking surjectivity. If $f : G \rightarrow H$ is a group homomorphism, we can define the image of $f$ to be the subset

$$\text{Im}(f) := \{f(g) \mid g \in G\} \subset H.$$  

It is easy to check that $\text{Im}(f)$ is a subgroup of $H$. Moreover, $f$ is surjective if and only if $\text{Im}(f) = H$, but this is just the definition of surjectivity: we are not using any special properties of group homomorphisms.

2.6. **Warning.** In general, orders of elements do not behave well under taking products. In particular, there are examples in which a group $G$ has elements $g, h$ of finite order such that $gh$ has infinite order (can you think of such an example for $G = GL_2(\mathbb{R})$?)

If $G$ is a group and $g, h \in G$ are elements of finite order that satisfy $gh = hg$, then $gh$ does have finite order as well; still, there is no general “formula” for the order of $gh$ in terms of the orders of $g$ and $h$ (the best statement one can make is that the order of $gh$ divides the least common multiple of the orders of $g$ and $h$).