Math 103A Lecture Notes

1.1 Lecture 1 (1/5/2009)

Notation 1.1 *Introduce* $\mathbb{N} := \{0, 1, 2, \dots\}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, *and* $\mathbb{C}$. *Also let* $\mathbb{Z}_+ := \mathbb{N} \setminus \{0\}$.

- Set notations.
- Recalled basic notions of a function being one to one, onto, and invertible. Think of functions in terms of a bunch of arrows from the domain set to the range set. To find the inverse function you should reverse the arrows.
- Some example of groups without the definition of a group:
  1. $GL_2(\mathbb{R}) = \left\{ g := \begin{bmatrix} a & b \\ c & d \end{bmatrix} : \det g = ad - bc \neq 0 \right\}$.
  2. Vector space with "group" operation being addition.
  3. The permutation group of invertible functions on a set S like $S = \{1, 2, \dots, n\}$.

1.1.1 A Little Number Theory

Axiom 1.2 (Well Ordering Principle) *Every non-empty subset,* S, *of* $\mathbb{N}$ *contains a smallest element.*

We say that a subset $S \subset \mathbb{Z}$ is **bounded below** if $S \subset [k, \infty)$ for some $k \in \mathbb{Z}$ and **bounded above** if $S \subset (-\infty, k]$ for some $k \in \mathbb{Z}$.

Remark 1.3 (Well ordering variations). The well ordering principle may also be stated equivalently as:

1. any subset $S \subset \mathbb{Z}$ which is bounded from below contains a smallest element or
2. any subset $S \subset \mathbb{Z}$ which is bounded from above contains a largest element.

To see this, suppose that $S \subset [k, \infty)$ and then apply the well ordering principle to $S - k$ to find a smallest element, $n \in S - k$. That is $n \in S - k$ and $n \leq s - k$ for all $s \in S$. Thus it follows that $n + k \in S$ and $n + k \leq s$ for all $s \in S$ so that $n + k$ is the desired smallest element in S.

For the second equivalence, suppose that $S \subset (-\infty, k]$ in which case $-S \subset [-k, \infty)$ and therefore there exist a smallest element $n \in -S$, i.e. $n \leq -s$ for all $s \in S$. From this we learn that $-n \in S$ and $-n \geq s$ for all $s \in S$ so that $-n$ is the desired largest element of S.

Theorem 1.4 (Division Algorithm). *Let* $a \in \mathbb{Z}$ *and* $b \in \mathbb{Z}_+$, *then there exists unique integers* $q \in \mathbb{Z}$ *and* $r \in \mathbb{N}$ *with* $r < b$ *such that*

$$a = bq + r.$$

(For example,

$$5 \overline{)\begin{matrix} 2 \\ 12 \\ \underline{10} \\ 2 \end{matrix}} \text{ so that } 12 = 2 \cdot 5 + 2.)$$

Proof. Let

$$S := \{k \in \mathbb{Z} : a - bk \geq 0\}$$

which is bounded from above. Therefore we may define,

$$q := \max \{k : a - bk \geq 0\}.$$

As q is the largest element of S we must have,

$$r := a - bq \geq 0 \text{ and } a - b(q + 1) < 0.$$

The second inequality is equivalent to $r - b < 0$ which is equivalent to $r < b$. This completes the existence proof.

To prove uniqueness, suppose that $a = bq' + r'$ in which case, $bq' + r' = bq + r$ and hence,

$$b > |r' - r| = |b(q - q')| = b|q - q'|. \tag{1.1}$$

Since $|q - q'| \geq 1$ if $q \neq q'$, the only way Eq. (1.1) can hold is if $q = q'$ and $r = r'$. ∎

Axiom 1.5 (Strong form of mathematical induction) *Suppose that* $S \subset \mathbb{Z}$ *is a non-empty set containing an element* a *with the property that; if* $[a, n) \cap \mathbb{Z} \subset S$ *then* $n \in \mathbb{Z}$, *then* $[a, \infty) \cap \mathbb{Z} \subset S$.

Axiom 1.6 (Weak form of mathematical induction) *Suppose that* $S \subset \mathbb{Z}$ *is a non-empty set containing an element* a *with the property that for every* $n \in S$ *with* $n \geq a$, $n + 1 \in S$, *then* $[a, \infty) \cap \mathbb{Z} \subset S$.

Remark 1.7. In Axioms 1.5 and 1.6 it suffices to assume that $a = 0$. For if $a \neq 0$ we may replace S by $S - a := \{s - a : s \in S\}$. Then applying the axioms with $a = 0$ to $S - a$ shows that $[0, \infty) \cap \mathbb{Z} \subset S - a$ and therefore,

$$[a, \infty) \cap \mathbb{Z} = [0, \infty) \cap \mathbb{Z} + a \subset S.$$

Theorem 1.8 (Equivalence of Axioms). *Axioms 1.2 – 1.6 are equivalent. (Only partially covered in class.)*

Proof. We will prove 1.2 $\iff$ 1.5 $\iff$ 1.6 $\implies$1.2.

1.2$\implies$1.5 Suppose $0 \in S \subset \mathbb{Z}$ satisfies the assumption in Axiom 1.5. If $\mathbb{N}_0$ is not contained in S, then $\mathbb{N}_0 \setminus S$ is a non empty subset of $\mathbb{N}$ and therefore has a smallest element, n. It then follows by the definition of n that $[0, n) \cap \mathbb{Z} \subset S$ and therefore by the assumed property on S, $n \in S$. This is a contradiction since n can not be in both S and $\mathbb{N}_0 \setminus S$.

1.5 $\implies$1.2 Suppose that $S \subset \mathbb{N}$ does not have a smallest element and let $Q := \mathbb{N} \setminus S$. Then $0 \in Q$ since otherwise $0 \in S$ would be the minimal element of S. Moreover if $[1, n) \cap \mathbb{Z} \subset Q$, then $n \in Q$ for otherwise n would be a minimal element of S. Hence by the strong form of mathematical induction, it follows that $Q = \mathbb{N}$ and hence that $S = \emptyset$.

1.5 $\implies$1.6 Any set, $S \subset \mathbb{Z}$ satisfying the assumption in Axiom 1.6 will also satisfy the assumption in Axiom 1.5 and therefore by Axiom 1.5 we will have $[a, \infty) \cap \mathbb{Z} \subset S$.

1.6 $\implies$1.5 Suppose that $0 \in S \subset \mathbb{Z}$ satisfies the assumptions in Axiom 1.5. Let $Q := \{n \in \mathbb{N} : [0, n) \subset S\}$. By assumption, $0 \in Q$ since $0 \in S$. Moreover, if $n \in Q$, then $[0, n) \subset S$ by definition of Q and hence $n + 1 \in Q$. Thus Q satisfies the restrictions on the set, S, in Axiom 1.6 and therefore $Q = \mathbb{N}$. So if $n \in \mathbb{N}$, then $n + 1 \in \mathbb{N} = Q$ and thus $n \in [0, n + 1) \subset S$ which shows that $\mathbb{N} \subset S$. As $0 \in S$ by assumption, it follows that $\mathbb{N}_0 \subset S$ as desired.

■

1.2 Lecture 2 (1/7/2009)

Definition 1.9. *Given $a, b \in \mathbb{Z}$ with $a \neq 0$ we say that a **divides** b or a is a **divisor** of b (write $a|b$) provided $b = ak$ for some $k \in \mathbb{Z}$.*

Definition 1.10. *Given $a, b \in \mathbb{Z}$ with $|a| + |b| > 0$, we let*

$$\gcd(a, b) := \max\{m : m|a \text{ and } m|b\}$$

*be the **greatest common divisor** of a and b. (We do not define $\gcd(0, 0)$ and we have $\gcd(0, b) = |b|$ for all $b \in \mathbb{Z} \setminus \{0\}$.) If $\gcd(a, b) = 1$, we say that a and b are **relatively prime**.*

Remark 1.11. Notice that $\gcd(a, b) = \gcd(|a|, |b|) \geq 0$ and $\gcd(a, 0) = 0$ for all $a \neq 0$.

Lemma 1.12 (Euclidean Algorithm). *Suppose that a, b are positive integers with $a < b$ and let $b = ka + r$ with $0 \leq r < a$ by the division algorithm. If $r = 0$, then $\gcd(a, b) = \gcd(a, r)$. In particular if $r = 0$, we have*

$$\gcd(a, b) = \gcd(a, 0) = a.$$

Proof. Since $b = ka + r$ if d is a divisor of both a and r it is a divisor of b. Similarly, $r = b - ka$ so that if d is a divisor of both a and b then d is also a divisor of r. Thus the common divisors of a and r and a and b are the same and therefore $\gcd(a, b) = \gcd(a, r)$. ■

Example 1.13. Suppose that $a = 15 = 3 \cdot 5$ and $b = 28 = 2^2 \cdot 7$. In this case it is easy to see that $\gcd(15, 28) = 1$. Nevertheless, lets use Lemma 1.12 repeatedly as follows;

$$28 = 1 \cdot 15 + 13 \text{ so } \gcd(15, 28) = \gcd(13, 15), \tag{1.2}$$
$$15 = 1 \cdot 13 + 2 \text{ so } \gcd(13, 15) = \gcd(2, 13), \tag{1.3}$$
$$13 = 6 \cdot 2 + 1 \text{ so } G\gcd(2, 13) = \gcd(1, 2), \tag{1.4}$$
$$2 = 2 \cdot 1 + 0 \text{ so } \gcd(1, 2) = \gcd(0, 1) = 1. \tag{1.5}$$

Moreover making use of Eqs. (1.2–1.4) in reverse order we learn that,

$$\begin{aligned} 1 &= 13 - 6 \cdot 2 \\ &= 13 - 6 \cdot (15 - 1 \cdot 13) = 7 \cdot 13 - 6 \cdot 15 \\ &= 7 \cdot (28 - 1 \cdot 15) - 6 \cdot 15 = 7 \cdot 28 - 13 \cdot 15. \end{aligned}$$

Thus we have also shown that

$$1 = s \cdot 28 + t \cdot 15 \text{ where } s = 7 \text{ and } t = -13.$$

The choices for s and t used above are certainly not unique. For example we have,

$$0 = 15 \cdot 28 - 28 \cdot 15$$

which added to

$$1 = 7 \cdot 28 - 13 \cdot 15$$

implies,

$$\begin{aligned} 1 &= (7 + 15) \cdot 28 - (13 + 28) \cdot 15 \\ &= 22 \cdot 28 - 41 \cdot 15 \end{aligned}$$

as well.

Example 1.14. Suppose that $a = 40 = 2^3 \cdot 5$ and $b = 52 = 2^2 \cdot 13$. In this case we have $\gcd(40, 52) = 4$. Working as above we find,

$$\begin{aligned} 52 &= 1 \cdot 40 + 12 \\ 40 &= 3 \cdot 12 + 4 \\ 12 &= 3 \cdot 4 + 0 \end{aligned}$$

so that we again see $\gcd(40, 52) = 4$. Moreover,

$$4 = 40 - 3 \cdot 12 = 40 - 3 \cdot (52 - 1 \cdot 40) = 4 \cdot 40 - 3 \cdot 52.$$

So again we have shown $\gcd(a, b) = sa + tb$ for some $s, t \in \mathbb{Z}$, in this case $s = 4$ and $t = 3$.

Example 1.15. Suppose that $a = 333 = 3^2 \cdot 37$ and $b = 459 = 3^3 \cdot 17$ so that $\gcd(333, 459) = 3^2 = 9$. Repeated use of Lemma 1.12 gives,

$$459 = 1 \cdot 333 + 126 \text{ so } \gcd(333, 459) = \gcd(126, 333), \tag{1.6}$$
$$333 = 2 \cdot 126 + 81 \text{ so } \gcd(126, 333) = \gcd(81, 126), \tag{1.7}$$
$$126 = 81 + 45 \text{ so } \gcd(81, 126) = \gcd(45, 81), \tag{1.8}$$
$$81 = 45 + 36 \text{ so } \gcd(45, 81) = \gcd(36, 45), \tag{1.9}$$
$$45 = 36 + 9 \text{ so } \gcd(36, 45) = \gcd(9, 36), \text{ and} \tag{1.10}$$
$$36 = 4 \cdot 9 + 0 \text{ so } \gcd(9, 36) = \gcd(0, 9) = 9. \tag{1.11}$$

Thus we have shown that

$$\gcd(333, 459) = 9.$$

We can even say more. From Eq. (1.11) we have, $9 = 45 - 36$ and then from Eq. (1.11),

$$9 = 45 - 36 = 45 - (81 - 45) = 2 \cdot 45 - 81.$$

Continuing up the chain this way we learn,

$$\begin{aligned} 9 &= 2 \cdot (126 - 81) - 81 = 2 \cdot 126 - 3 \cdot 81 \\ &= 2 \cdot 126 - 3 \cdot (333 - 2 \cdot 126) = 8 \cdot 126 - 3 \cdot 333 \\ &= 8 \cdot (459 - 1 \cdot 333) - 3 \cdot 333 = 8 \cdot 459 - 11 \cdot 333 \end{aligned}$$

so that

$$9 = 8 \cdot 459 - 11 \cdot 333.$$

The methods of the previous two examples can be used to prove Theorem 1.16 below. However, we will two different variants of the proof.

Theorem 1.16. *If $a, b \in \mathbb{Z} \setminus \{0\}$, then there exists (not unique) numbers, $s, t \in \mathbb{Z}$ such that*

$$\gcd(a, b) = sa + tb. \tag{1.12}$$

Moreover if $m \neq 0$ is any common divisor of both a and b then $m | \gcd(a, b)$.

Proof. If m is any common divisor of a and b then m is also a divisor of $sa + tb$ for any $s, t \in \mathbb{Z}$. (In particular this proves the second assertion given the truth of Eq. (1.12).) In particular, $\gcd(a, b)$ is a divisor of $sa + tb$ for all $s, t \in \mathbb{Z}$. Let $S := \{sa + tb : s, t \in \mathbb{Z}\}$ and then define

$$d := \min(S \cap \mathbb{Z}_+) = sa + tb \text{ for some } s, t \in \mathbb{Z}. \tag{1.13}$$

By what we have just said if follows that $\gcd(a, b) | d$ and in particular $d \geq \gcd(a, b)$. If we can snow d is a common divisor of a and b we must then have $d = \gcd(a, b)$. However, using the division algorithm,

$$a = kd + r \text{ with } 0 \leq r < d. \tag{1.14}$$

As

$$r = a - kd = a - k(sa + tb) = (1 - ks)a - ktb \in S \cap \mathbb{N},$$

if r were greater than 0 then $r \geq d$ (from the definition of d in Eq. (1.13) which would contradict Eq. (1.14). Hence it follows that $r = 0$ and $d | a$. Similarly, one shows that $d | b$. ∎

Lemma 1.17 (Euclid's Lemma). *If $\gcd(c, a) = 1$, i.e. c and a are relatively prime, and $c | ab$ then $c | b$.*

Proof. We know that there exists $s, t \in \mathbb{Z}$ such that $sa + tc = 1$. Multiplying this equation by b implies,

$$sab + tcb = b.$$

Since $c | ab$ and $c | cb$, it follows from this equation that $c | b$. ∎

Corollary 1.18. *Suppose that $a, b \in \mathbb{Z}$ such that there exists $s, t \in \mathbb{Z}$ with $1 = sa + tb$. Then a and b are relatively prime, i.e. $\gcd(a, b) = 1$.*

Proof. If $m > 0$ is a divisor of a and b, then $m | (sa + tb)$, i.e. $m | 1$ which implies $m = 1$. Thus the only positive common divisor of a and b is 1 and hence $\gcd(a, b) = 1$. ∎

1.2.1 Ideals (Not covered in class.)

Definition 1.19. *As non-empty subset $S \subset \mathbb{Z}$ is called an **ideal** if S is closed under addition (i.e. $S+S \subset S$) and under multiplication by **any** element of $\mathbb{Z}$, i.e. $\mathbb{Z} \cdot S \subset S$.*

Example 1.20. For any $n \in \mathbb{Z}$, let

$$(n) := \mathbb{Z} \cdot n = n\mathbb{Z} := \{kn : k \in \mathbb{Z}\}.$$

I is easily checked that (n) is an ideal. The next theorem states that this is a listing of all the ideals of $\mathbb{Z}$.

Theorem 1.21 (Ideals of $\mathbb{Z}$). *If $S \subset \mathbb{Z}$ is an ideal then $S = (n)$ for some $n \in \mathbb{Z}$. Moreover either $S = \{0\}$ in which case $n = 0$ for $S \neq \{0\}$ in which case $n = \min(S \cap \mathbb{Z}_+)$.*

Proof. If $S = \{0\}$ we may take $n = 0$. So we may assume that S contains a non-zero element a. By assumption that $\mathbb{Z} \cdot S \subset S$ it follows that $-a \in S$ as well and therefore $S \cap \mathbb{Z}_+$ is not empty as either a or $-a$ is positive. By the well ordering principle, we may define n as, $n := \min S \cap \mathbb{Z}_+$.

Since $\mathbb{Z} \cdot n \subset \mathbb{Z} \cdot S \subset S$, it follows that $(n) \subset S$. Conversely, suppose that $s \in S \cap \mathbb{Z}_+$. By the division algorithm, $s = kn + r$ where $k \in \mathbb{N}$ and $0 \leq r < n$. It now follows that $r = s - kn \in S$. If $r > 0$, we would have to have $r \geq n = \min S \cap \mathbb{Z}_+$ and hence we see that $r = 0$. This shows that $s = kn$ for some $k \in \mathbb{N}$ and therefore $s \in (n)$. If $s \in S$ is negative we apply what we have just proved to $-s$ to learn that $-s \in (n)$ and therefore $s \in (n)$. ∎

Remark 1.22. Notice that $a|b$ iff $b = ak$ for some $k \in \mathbb{Z}$ which happens iff $b \in (a)$.

Proof. Second Proof of Theorem 1.16. Let $S := \{sa + tb : s, t \in \mathbb{Z}\}$. One easily checks that $S \subset \mathbb{Z}$ is an ideal and therefore $S = (d)$ where $d := \min S \cap \mathbb{Z}_+$. Notice that $d = sa + tb$ for some $s, t \in \mathbb{Z}$ as $d \in S$. We now claim that $d = \gcd(a, b)$. To prove this we must show that d is a divisor of a and b and that it is the maximal such divisor.

Taking $s = 1$ and $t = 0$ or $s = 0$ and $t = 1$ we learn that both $a, b \in S = (d)$, i.e. $d|a$ and $d|b$. If $m \in \mathbb{Z}_+$ and $m|a$ and $m|b$, then

$$\frac{d}{m} = s\frac{a}{m} + t\frac{b}{m} \in \mathbb{Z}$$

from which it follows that so that $m|d$. This shows that $d = \gcd(a, b)$ and also proves the last assertion of the theorem.

Alternate proof of last statement. If $m|a$ and $m|b$ there exists $k, l \in \mathbb{Z}$ such that $a = km$ and $b = lm$ and therefore,

$$d = sa + tb = (sk + tl)\, m$$

which again shows that $m|d$. ∎

Remark 1.23. As a second proof of Corollary 1.18, if $1 \in S$ (where S is as in the second proof of Theorem 1.16)), then $\gcd(a, b) = \min(S \cap \mathbb{Z}_+) = 1$.

1.3 Lecture 3 (1/9/2009)

1.3.1 Prime Numbers

Definition 1.24. *A number, $p \in \mathbb{Z}$, is **prime** iff $p \geq 2$ and p has no divisors other than 1 and p. Alternatively put, $p \geq 2$ and $\gcd(a, p)$ is either 1 or p for all $a \in \mathbb{Z}$.*

Example 1.25. The first few prime numbers are $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$.

Lemma 1.26 (Euclid's Lemma again). *Suppose that p is a prime number and $p|ab$ for some $a, b \in \mathbb{Z}$ then $p|a$ or $p|b$.*

Proof. We know that $\gcd(a, p) = 1$ or $\gcd(a, p) = p$. In the latter case $p|a$ and we are done. In the former case we may apply Euclid's Lemma 1.17 to conclude that $p|b$ and so again we are done. ∎

Theorem 1.27 (The fundamental theorem of arithmetic). *Every $n \in \mathbb{Z}$ with $n \geq 2$ is a prime or a product of primes. The product is unique except for the order of the primes appearing the product. Thus if $n \geq 2$ and $n = p_1 \ldots p_n = q_1 \ldots q_m$ where the p's and q's are prime, then $m = n$ and after renumbering the q's we have $p_i = q_i$.*

Proof. Existence: This clearly holds for $n = 2$. Now suppose for every $2 \leq k \leq n$ may be written as a product of primes. Then either $n+1$ is prime in which case we are done or $n + 1 = a \cdot b$ with $1 < a, b < n + 1$. By the induction hypothesis, we know that both a and b are a product of primes and therefore so is $n + 1$. This completes the inductive step.

Uniqueness: You are asked to prove the uniqueness assertion in 0.#25. Here is the solution. Observe that $p_1|q_1 \ldots q_m$. If p_1 does not divide q_1 then $\gcd(p_1, q_1) = 1$ and therefore by Euclid's Lemma 1.17, $p_1|(q_2 \ldots q_m)$. It now follows by induction that p_1 must divide one of the q_i, by relabeling we may assume that $q_1 = p_1$. The result now follows by induction on $n \vee m$. ∎

Definition 1.28. *The least common multiple of two non-zero integers, a, b, is the smallest positive number which is both a multiple of a and b and this number will be denoted by $\operatorname{lcm}(a, b)$. Notice that $m = \min((a) \cap (b) \cap \mathbb{Z}_+)$.*

Example 1.29. Suppose that $a = 12 = 2^2 \cdot 3$ and $b = 15 = 3 \cdot 5$. Then $\gcd(12,15) = 3$ while

$$\operatorname{lcm}(12,15) = \left(2^2 \cdot 3\right) \cdot 5 = 2^2 \cdot (3 \cdot 5) = \left(2^2 \cdot 3 \cdot 5\right) = 60.$$

Observe that

$$\gcd(12,15) \cdot \operatorname{lcm}(12,15) = 3 \cdot \left(2^2 \cdot 3 \cdot 5\right) = \left(2^2 \cdot 3\right) \cdot (3 \cdot 5) = 12 \cdot 15.$$

This is a special case of Chapter 0.#12 on p. 23 which can be proved by similar considerations. In general if

$$a = p_1^{n_1} \cdot \dots \cdot p_k^{n_k} \text{ and } b = p_1^{m_1} \dots p_k^{m_k} \text{ with } n_j, m_l \in \mathbb{N}$$

then

$$\gcd(a,b) = p_1^{n_1 \wedge m_1} \cdot \dots \cdot p_k^{n_k \wedge m_k} \text{ and } \operatorname{lcm}(a,b) = p_1^{n_1 \vee m_1} \cdot \dots \cdot p_k^{n_k \vee m_k}.$$

Therefore,

$$\begin{aligned} \gcd(a,b) \cdot \operatorname{lcm}(a,b) &= p_1^{n_1 \wedge m_1 + n_1 \vee m_1} \cdot \dots \cdot p_k^{n_k \wedge m_k + n_k \vee m_k} \\ &= p_1^{n_1 + m_1} \cdot \dots \cdot p_k^{n_k + m_k} = a \cdot b. \end{aligned}$$

1.3.2 Modular Arithmetic

Definition 1.30. *Let n be a positive integer and let $a = q_a n + r_a$ with $0 \le r_a < n$. Then we define $a \bmod n := r_a$. (Sometimes we might write $a = r_a \bmod n$ – but I will try to stick with the first usage.)*

Lemma 1.31. *Let $n \in \mathbb{Z}_+$ and $a, b, k \in \mathbb{Z}$. Then:*

1. $(a + kn) \bmod n = a \bmod n$.
2. $(a + b) \bmod n = (a \bmod n + b \bmod n) \bmod n$.
3. $(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$.

Proof. Let $r_a = a \bmod n$, $r_b = b \bmod n$ and $q_a, q_b \in \mathbb{Z}$ such that $a = q_a n + r_a$ and $b = q_b n + r_b$.

1. Then $a + kn = (q_a + k) n + r_a$ and therefore,

$$(a + kn) \bmod n = r_a = a \bmod n.$$

2. $a + b = (q_a + q_b) n + r_a + r_b$ and hence by item 1 with $k = q_a + q_b$ we find,

$$(a + b) \bmod n = (r_a + r_b) \bmod n. = (a \bmod n + b \bmod n) \bmod n.$$

3. For the last assertion,

$$a \cdot b = [q_a n + r_a] \cdot [q_b n + r_b] = (q_a q_b n + r_a q_b + r_b q_a) n + r_a \cdot r_b$$

and so again by item 1. with $k = (q_a q_b n + r_a q_b + r_b q_a)$ we have,

$$(a \cdot b) \bmod n = (r_a \cdot r_b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n.$$

■

Example 1.32. Take $n = 4$, $a = 18$ and $b = 7$. Then $18 \bmod 4 = 2$ and $7 \bmod 4 = 3$. On one hand,

$$\begin{aligned} (18 + 7) \bmod 4 = 25 \bmod 4 = 1 \text{ while on the other,} \\ (2 + 3) \bmod 4 = 1. \end{aligned}$$

Similarly, $18 \cdot 7 = 126 = 4 \cdot 31 + 2$ so that

$$\begin{aligned} (18 \cdot 7) \bmod 4 = 2 \text{ while} \\ (2 \cdot 3) \bmod 4 = 6 \bmod 4 = 2. \end{aligned}$$

Remark 1.33 (Error Detection). Companies often add extra digits to identification numbers for the purpose of detecting forgery or errors. For example the United Parcel Service uses a mod 7 check digit. Hence if the identification number were $n = 354691332$ one would append

$$\begin{aligned} n \bmod 7 = 354691332 \bmod 7 = 2 \text{ to the number to get} \\ 354691332\_2 \text{ (say).} \end{aligned}$$

See the book for more on this method and other more elaborate check digit schemes. Note,

$$354691332 = 50\,670\,190 \cdot 7 + 2.$$

Remark 1.34. Suppose that $a, n \in \mathbb{Z}_+$ and $b \in \mathbb{Z}$, then it is easy to show

$$(ab) \bmod (an) = a \cdot (b \bmod n).$$

Example 1.35 (Computing $\bmod 10$). We have,

$$\begin{aligned} 123456 \bmod 10 &= 6 \\ 123456 \bmod 100 &= 56 \\ 123456 \bmod 1000 &= 456 \\ 123456 \bmod 10000 &= 3456 \\ 123456 \bmod 100000 &= 23456 \\ 123456 \bmod 1000000 &= 123456 \end{aligned}$$

so that

$$a_n \ \dots a_2 \ a_1 \bmod 10^k = a_k \ \dots a_2 \ a_1 \text{ for all } k \le n.$$

Solution to Exercise (0.52). As an example, here is a solution to Problem 0.52 of the book which states that $\overbrace{111\ldots1}^{k \text{ times}}$ is not the square of an integer except when $k = 1$.

As 11 is prime we may assume that $k \geq 3$. By Example 1.35, $111\ldots1 \bmod 10 = 1$ and $111\ldots1 \bmod 100 = 11$. Hence $1111\ldots1 = n^2$ for some integer n, we must have

$$n^2 \bmod 10 = 1 \text{ and } \left(n^2-1\right) \bmod 100 = 10.$$

The first condition implies that $n \bmod 10 = 1$ or 9 as $1^2 = 1$ and $9^2 \bmod 10 = 81 \bmod 10 = 1$. In the first case we have, $n = k \cdot 10 + 1$ and therefore we must require,

$$10 = \left(n^2-1\right) \bmod 100 = \left[(k\cdot 10+1)^2 - 1\right] \bmod 100 = \left(k^2 \cdot 100 + 2k \cdot 10\right) \bmod 100$$
$$= (2k \cdot 10) \bmod 100 = 10 \cdot (2k \bmod 10)$$

which implies $1 = (2k \bmod 10)$ which is impossible since $2k \bmod 10$ is even.

For the second case we must have,

$$\begin{aligned} 10 &= \left(n^2-1\right) \bmod 100 \bmod 100 = \left[(k\cdot 10+9)^2 - 1\right] \bmod 100 \\ &= \left(k^2 \cdot 100 + 18k \cdot 10 + 81 - 1\right) \bmod 100 \\ &= \left(\left(10+8\right) k \cdot 10 + 8 \cdot 10\right) \bmod 100 \\ &= \left(8\left(k+1\right) \cdot 10\right) \bmod 100 \\ &= 10 \cdot 8k \bmod 10 \end{aligned}$$

which implies which $1 = (8k \bmod 10)$ which again is impossible since $8k \bmod 10$ is even.

Solution to Exercise (0.52 Second and better solution). Notice that $111\ldots11 = 111\ldots00 + 11$ and therefore,

$$111\ldots11 \bmod 4 = 11 \bmod 4 = 3.$$

On the other hand, if $111\ldots11 = n^2$ we must have,

$$(n \bmod 4)^2 \bmod 4 = 3.$$

There are only four possibilities for $r := n \bmod 4$, namely $r = 0, 1, 2, 3$ and these are not allowed since $0^2 \bmod 4 = 0 \neq 3$, $1^2 \bmod 4 = 1 \neq 3, 2^2 \bmod 4 = 0 \neq 3$, and $3^2 \bmod 4 = 1 \neq 3$.

1.3.3 Equivalence Relations

Definition 1.36. *A **equivalence relation** on a set S is a subset, $R \subset S \times S$ with the following properties:*

1. *R **is reflexive:** $(a,a) \in R$ for all $a \in S$*
2. *R **is symmetric:** If $(a,b) \in R$ then $(b,a) \in R$.*
3. *R **is transitive:** If $(a,b) \in R$ and $(b,c) \in R$ then $(a,c) \in R$.*

*We will usually write $a \sim b$ to mean that $(a,b) \in R$ and pronounce this as a is equivalent to b. With this notation we are assuming $a \sim a$, $a \sim b \implies b \sim a$ and $a \sim b$ and $b \sim c \implies a \sim c$. (**Note well:** the book write aRb rather than $a \sim b$.)*

Example 1.37. If $S = \{1,2,3,4,5\}$ then:

1. $R = \{1,2,3\}^2 \cup \{4,5\}^2$ is an equivalence relation.
2. $R = \{(1,1),(2,2),(3,3),(4,4),(5,5),(1,2),(2,1),(2,3),(3,2)\}$ is not an equivalence relation. For example, $1 \sim 2$ and $2 \sim 3$ but 1 is not equivalent to 3, so R is not transitive.

Example 1.38. Let $n \in \mathbb{Z}_+$, $S = \mathbb{Z}$ and say $a \sim b$ iff $a \bmod n = b \bmod n$. This is an equivalence relation. For example, when $s = 2$ we have $a \sim b$ iff both a and b are odd or even. So in this case $R = \{\text{odd}\}^2 \cup \{even\}^2$.

Example 1.39. Let $S = \mathbb{R}$ and say $a \sim b$ iff $a \geq b$. Again not symmetric so is not an equivalence relation.

Definition 1.40. *A **partition** of a set S is a decomposition, $\{S_\alpha\}_{\alpha \in I}$, by disjoint sets, so S_α is a non-empty subset of S such that $S = \cup_{\alpha \in I} S_\alpha$ and $S_\alpha \cap S_\beta = \emptyset$ if $\alpha \neq \beta$.*

Example 1.41. If $\{S_\alpha\}_{\alpha \in I}$ is a partition of S, then $R = \cup_{\alpha \in I} S_\alpha^2$ is an equivalence relation. The next theorem states this is the general type of equivalence relation.

1.4 Lecture 4 (1/12/2009)

Theorem 1.42. *Let R or $\sim$ be an equivalence relation on S and for each $a \in S$, let*

$$[a] := \{x \in S : a \sim x\}$$

*be the **equivalence class** of a.. Then S is partitioned by its distinct equivalence classes.*

Proof. Because $\sim$ is reflexive, $a \in [a]$ for all a and therefore every element $a \in S$ is a member of its own equivalence class. Thus to finish the proof we must show that distinct equivalence classes are disjoint. To this end we will show that if $[a] \cap [b] \neq \emptyset$ then in fact $[a] = [b]$. So suppose that $c \in [a] \cap [b]$ and $x \in [a]$. Then we know that $a \sim c$, $b \sim c$ and $a \sim x$. By reflexivity and transitivity of $\sim$ we then have,

$$x \sim a \sim c \sim b, \text{ and hence } b \sim x,$$

which shows that $x \in [b]$. Thus we have shown $[a] \subset [b]$. Similarly it follows that $[b] \subset [a]$. ∎

Exercise 1.1. Suppose that $S = \mathbb{Z}$ with $a \sim b$ iff $a \bmod n = b \bmod n$. Identify the equivalence classes of $\sim$. Answer,

$$\{[0], [1], \ldots, [n-1]\}$$

where

$$[i] = i + n\mathbb{Z} = \{i + ns : s \in \mathbb{Z}\}.$$

Exercise 1.2. Suppose that $S = \mathbb{R}^2$ with $\mathbf{a} = (a_1, a_2) \sim \mathbf{b} = (b_1, b_2)$ iff $|\mathbf{a}| = |\mathbf{b}|$ where $|\mathbf{a}| := a_1^2 + a_2^2$. Show that $\sim$ is an equivalence relation and identify the equivalence classes of $\sim$. Answer, the equivalence classes consists of concentric circles centered about the origin $(0,0) \in S$.

1.4.1 Binary Operations and Groups – a first look

Definition 1.43. *A **binary operation** on a set S is a function, $* : S \times S \to S$. We will typically write $a * b$ rather than $*(a, b)$.*

Example 1.44. Here are a number of examples of binary operations.

1. $S = \mathbb{Z}$ and $* =$ " $+$ "
2. $S = \{\text{odd integers}\}$ and $* =$ " $+$ " is **not** an example of a binary operator since $3 * 5 = 3 + 5 = 8 \notin S$.
3. $S = \mathbb{Z}$ and $* =$"$\cdot$"
4. $S = \mathbb{R} \setminus \{0\}$ and $* =$"$\cdot$"
5. $S = \mathbb{R} \setminus \{0\}$ with $* =$ "$\setminus$" = " $\div$ ".
6. Let S be the set of 2×2 real (complex) matrices with $A * B := AB$.

Definition 1.45. *Let $*$ be a binary operation on a set S. Then;*

1. *$*$ is **associative** if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.*
2. *$e \in S$ is an **identity element** if $e * a = a = a * e$ for all $a \in S$.*
3. *Suppose that $e \in S$ is an identity element and $a \in S$. We say that $b \in S$ is an **inverse** to a if $b * a = e = a * b$.*
4. *$*$ is **commutative** if $a * b = b * a$ for all $a, b \in S$.*

Definition 1.46 (Group). *A **group** is a triple, $(G, *, e)$ where $*$ is an associative binary operation on a set, G, $e \in G$ is an identity element, and each $g \in G$ has an inverse in G. (Typically we will simply denote $g * h$ by gh.)*

Definition 1.47 (Commutative Group). *A group, (G, e), is commutative if $gh = hg$ for all $h, g \in G$.*

Example 1.48 ($(\mathbb{Z}, +)$). One easily checks that $(\mathbb{Z}, * = +)$ is **a commutative group** with $e = 0$ and the inverse to $a \in \mathbb{Z}$ is $-a$. Observe that $e * a = e + a = a$ for all a iff $e = 0$.

Example 1.49. $S = \mathbb{Z}$ and $* =$"$\cdot$" is an associative, commutative, binary operation with $e = 1$ being the identity. Indeed $e \cdot a = a$ for all $a \in \mathbb{Z}$ implies $e = e \cdot 1 = 1$. This is **not** a group since there are no inverses for any $a \in \mathbb{Z}$ with $|a| \geq 2$.

Example 1.50 ($(\mathbb{R} \setminus \{0\}, \cdot)$). $G = \mathbb{R} \setminus \{0\} =: \mathbb{R}^*$, and $* =$"$\cdot$" is a commutative group, $e = 1$, an inverse to a is $1/a$.

Example 1.51. $S = \mathbb{R} \setminus \{0\}$ with $* =$ "$\setminus$" = " $\div$ ". In this case $*$ is not associative since

$$a * (b * c) = a / (b/c) = \frac{ac}{b} \text{ while}$$
$$(a * b) * c = (a/b) / c = \frac{a}{bc}.$$

It is also not commutative since $a/b \neq b/a$ in general. There is no identity element $e \in S$. Indeed, $e * a = a = a * e$, we would imply $e = a^2$ for all $a \neq 0$ which is impossible, i.e. $e = 1$ and $e = 4$ at the same time.

Example 1.52. Let S be the set of 2×2 real (complex) matrices with $A * B := AB$. This is a non-commutative binary operation which is associative and has an identity, namely

$$e := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

It is however not a group only those $A \in S$ with $\det A \neq 0$ admit an inverse.

Example 1.53 ($GL_2(\mathbb{R})$). Let $G := GL_2(\mathbb{R})$ be the set of 2×2 real (complex) matrices such that $\det A \neq 0$ with $A * B := AB$ is a group with $e := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and the inverse to A being A^{-1}. This group is non-abeliean for example let

$$A := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

then

$$AB = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \text{ while}$$

$$BA = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} \neq AB.$$

Example 1.54 ($SL_2(\mathbb{R})$). Let $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) : \det A = 1\}$. This is a group since $\det(AB) = \det A \cdot \det B = 1$ if $A, B \in SL_2(\mathbb{R})$.

1.5 Lecture 5 (1/14/2009)

1.5.1 Elementary Properties of Groups and the notion of a subgroup

Let $(G, \cdot)$ be a group.

Lemma 1.55. *The identity element in G is unique.*

Proof. Suppose that e and e' both satisfy $ea = ae = a$ and $e'a = ae' = a$ for all $a \in G$, then $e = e'e = e'$. ∎

Lemma 1.56. *Left and right cancellation holds. Namely, if $ab = ac$ then $b = c$ and $ba = ca$ then $b = c$.*

Proof. Let d be an inverse to a. If $ab = ac$ then $d(ab) = d(ac)$. On the other hand by associativity,

$$d(ab) = (da)b = eb = b \text{ and similarly, } d(ac) = c.$$

Thus it follows that $b = c$. The right cancellation is proved similarly. ∎

Example 1.57 (No cross cancellation in general). Let $G = GL_2(\mathbb{R})$,

$$A := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \; B := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } C := \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}.$$

Then

$$AB = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = CA$$

yet $B \neq C$. In general, all we can say if $AB = CA$ is that $C = ABA^{-1}$.

Lemma 1.58. *Inverses in G are unique.*

Proof. Suppose that b and b' are both inverses to a, then $ba = e = b'a$. Hence by cancellation, it follows that $b = b'$. ∎

Notation 1.59 *If $g \in G$, let g^{-1} denote the unique inverse to g. (If we are in an abelian group and using the symbol, "+" for the binary operation we denote g^{-1} by $-g$ instead.*

Example 1.60. Let G be a group. Because of the associativity law it makes sense to write $a_1a_2a_3$ and $a_1a_2a_3a_4$ where $a_i \in G$. Indeed, we may either interpret $a_1a_2a_3$ as $(a_1a_2)a_3$ or as $a_1(a_2a_3)$ which are equal by the associativity law. While we might interpret $a_1a_2a_3a_4$ as one of the following expressions;

$$\begin{aligned} c_1 &:= (a_1a_2)(a_3a_4) \\ c_2 &:= ((a_1a_2)a_3)a_4 \\ c_3 &:= (a_1(a_2a_3))a_4 \\ c_4 &:= a_1((a_2a_3)a_4) \\ c_5 &:= a_1(a_2(a_3a_4)). \end{aligned}$$

Using the associativity law repeatedly these are all seen to be equal. For example,

$$\begin{aligned} c_1 = (a_1a_2)(a_3a_4) &= ((a_1a_2)a_3)a_4 = c_2, \\ c_3 = (a_1(a_2a_3))a_4 &= a_1((a_2a_3)a_4) = c_4 \\ = a_1(a_2(a_3a_4)) &= (a_1a_2)(a_3a_4) = c_1 \end{aligned}$$

and

$$c_5 := a_1(a_2(a_3a_4)) = (a_1a_2)(a_3a_4) = c_1.$$

More generally we have the following proposition.

Proposition 1.61. *Suppose that G is a group and $g_1, g_2, \dots, g_n \in G$, then it makes sense to write $g_1g_2 \dots g_n \in G$ which is interpreted to mean: do the pairwise multiplications in any of the possible allowed orders without rearranging the orders of the g's.*

Proof. Sketch. The proof is by induction. Let us begin by defining $\{M_n : G^n \to G\}_{n=2}^{\infty}$ inductively by $M_2(a,b) = ab$, $M_3(a,b,c) = (ab)c$, and $M_n(g_1, \dots, g_n) := M_{n-1}(g_1, \dots, g_{n-1}) \cdot g_n$. We wish to show that $M_n(g_1, \dots, g_n)$ may be expressed as one of the products described in the proposition. For the base case, $n = 2$, there is nothing to prove. Now assume that the assertion holds for $2 \leq k \leq n$. Consider an expression for $g_1 \dots g_ng_{n+1}$. We now do another induction on the number of parentheses appearing on the right of this expression, $\dots g_n \overbrace{)\dots)}^{k}$. If $k = 0$, we have

(brackets involving $g_1 \dots g_n) \cdot g_{n+1} = M_n(g_1, \dots, g_n)\, g_{n+1} = M_{n+1}(g_1, \dots, g_{n+1})$,

wherein we used induction in the first equality and the definition of M_{n+1} in the second. Now suppose the assertion holds for some $k \geq 0$ and consider the case where there are $k+1$ parentheses appearing on the right of this expression, i.e. $\ldots g_n \overbrace{)\ldots)}^{k+1}$. Using the associativity law for the last bracket on the right we can transform this expression into one with only k parentheses appearing on the right. It then follows by the induction hypothesis, that $\ldots g_n \overbrace{)\ldots)}^{k+1} = M_{n+1}(g_1, \ldots, g_{n+1})$. ∎

Notation 1.62 *For $n \in \mathbb{Z}$ and $g \in G$, let $g^n := \overbrace{g \ldots g}^{n \text{ times}}$ and $g^{-n} := \overbrace{g^{-1} \ldots g^{-1}}^{n \text{ times}} = \left(g^{-1}\right)^n$ if $n \geq 1$ and $g^0 := e$.*

Observe that with this notation that $g^m g^n = g^{m+n}$ for all $m, n \in \mathbb{Z}$. For example,

$$g^3 g^{-5} = gggg^{-1}g^{-1}g^{-1}g^{-1} = ggg^{-1}g^{-1}g^{-1}g^{-1} = gg^{-1}g^{-1}g^{-1} = g^{-1}g^{-1} = g^{-2}.$$

1.5.2 More Examples of Groups

Example 1.63. Let G be the set of 2×2 real (complex) matrices with $A * B := A + B$. This is a group. In fact any vector space under addition is an abelian group with $e = 0$ and $v^{-1} = -v$.

Example 1.64 ($\mathbb{Z}_n$). For any $n \geq 2$, $G := \mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ with $a * b = (a+b) \bmod n$ is a commutative group with $e = 0$ and the inverse to $a \in \mathbb{Z}_n$ being $n - a$. Notice that $(n - a + a) \bmod n = n \bmod n = 0$.

Example 1.65. Suppose that $S = \{0, 1, 2, \ldots, n-1\}$ with $a * b = ab \bmod n$. In this case $*$ is an associative binary operation which is commutative and $e = 1$ is an identity for S. In general it is not a group since not every element need have an inverse. Indeed if $a, b \in S$, then $a * b = 1$ iff $1 = ab \bmod n$ which we have seen can happen iff $\gcd(a, n) = 1$ by Lemma **??**. For example if $n = 4$, $S = \{0, 1, 2, 3\}$, then

$$2 * 1 = 2, \; 2 * 2 = 0, \quad 2 * 0 = 0, \quad \text{and} \quad 2 * 3 = 2,$$

none of which are 1. Thus, 2 is not invertible for this operation. (Of course 0 is not invertible as well.)

1.6 Lecture 6 (1/16/2009)

Theorem 1.66 (The groups, $U(n)$). *For $n \geq 2$, let*

$$U(n) := \{a \in \{1, 2, \ldots, n-1\} : \gcd(a, n) = 1\}$$

and for $a, b \in U(n)$ let $a * b := (ab) \bmod n$. Then $(U(n), *)$ is a group.

Proof. First off, let $a * b := ab \bmod n$ for all $a, b \in \mathbb{Z}$. Then if $a, b, c \in \mathbb{Z}$ we have

$$\begin{aligned}(abc) \bmod n &= ((ab)c) \bmod n = ((ab) \bmod n \cdot c \bmod n) \bmod n \\ &= ((a * b) \cdot c \bmod n) \bmod n = ((a * b) \cdot c) \bmod n \\ &= (a * b) * c.\end{aligned}$$

Similarly one shows that

$$(abc) \bmod n = a * (b * c)$$

and hence $*$ is associative. It should be clear also that $*$ is commuative.

Claim: an element $a \in \{1, 2, \ldots, n-1\}$ is in $U(n)$ iff there exists $r \in \{1, 2, \ldots, n-1\}$ such that $r * a = 1$.

($\Longrightarrow$) $a \in U(n) \iff \gcd(a, n) = 1 \iff$ there exists $s, t \in \mathbb{Z}$ such that $sa + tn = 1$. Taking this equation $\bmod n$ then shows,

$$(s \bmod n \cdot a) \bmod n = (s \bmod n \cdot a \bmod n) \bmod n = (sa) \bmod n = 1 \bmod n = 1$$

and therefore $r := s \bmod n \in \{1, 2, \ldots, n-1\}$ and $r * a = 1$.

($\Longleftarrow$) If there exists $r \in \{1, 2, \ldots, n-1\}$ such that $1 = r * a = ra \bmod n$, then $n \mid (ra - 1)$, i.e. there exists t such that $ra - 1 = kt$ or $1 = ra - kt$ from which it follows that $\gcd(a, n) = 1$, i.e. $a \in U(n)$.

The claim shows that to each element, $a \in U(n)$, there is an inverse, $a^{-1} \in U(n)$. Finally if $a, b \in U(n)$ let $k := b^{-1} * a^{-1} \in U(n)$, then

$$k * (a * b) = b^{-1} * a^{-1} * a * b = 1$$

and so by the claim, $a * b \in U(n)$, i.e. the binary operation is really a binary operation on $U(n)$. ∎

Example 1.67 ($U(10)$). $U(10) = \{1, 3, 7, 9\}$ with multiplication or Cayley table given by

$$\begin{array}{c|cccc} a \backslash b & 1 & 3 & 7 & 9 \\ \hline 1 & 1 & 3 & 7 & 9 \\ 3 & 3 & 9 & 1 & 7 \\ 7 & 7 & 1 & 9 & 3 \\ 9 & 9 & 7 & 3 & 1 \end{array}$$

where the element of the (a, b) row indexed by $U(10)$ itself is given by $a * b = ab \bmod 10$.

Example 1.68. If p is prime, then $U(p) = \{1, 2, \dots, p\}$. For example $U(5) = \{1, 2, 3, 4\}$ with Cayley table given by,

$$\begin{array}{c} a\backslash b \; 1\; 2\; 3\; 4 \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix} \end{array}.$$

1.6.1 $O(2)$ – reflections and rotations in $\mathbb{R}^2$

Definition 1.69 (Sub-group). *Let $(G, \cdot)$ be a group. A non-empty subset, $H \subset G$, is said to be a subgroup of G if:*

1. *H is **closed** under $\cdot$, i.e. $hk \in H$ for all $h, k \in H$,*
2. *H is **closed** under taking inverses, i.e. $h^{-1} \in H$ if $h \in H$.*

The following lemma is easy to prove upon noticing that $e \in H$ since if $h \in H$, then $e = h^{-1}h \in H$.

Lemma 1.70. *If $H \subset G$ is a sub-group, then $(H, \cdot)$ is a group.*

Notation 1.71 *The **order of a group,** G, is the number of elements in G which we denote by $|G|$.*

In this section, we are interested in describing the subgroup of $GL_2(\mathbb{R})$ which corresponds to reflections and rotations in the plane. We define these operations now.

As in Figure 1.1 let

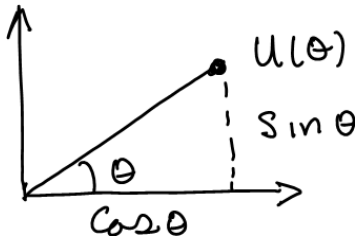

Fig. 1.1. The unit vector, $u(\theta)$, at angle θ to the x – axis.

$$u(\theta) := \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix}.$$

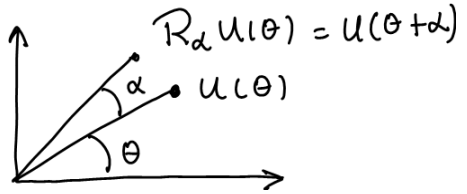

Fig. 1.2. Rotation by α degrees in the counter clockwise direction.

We also let R_α denote rotation by α degrees counter clockwise so that $R_\alpha u(\theta) = u(\theta + \alpha)$ as in Figure 1.2. We may represent R_α as a matrix, namely

$$\begin{aligned} R_\alpha &= [R_\alpha e_1 | R_\alpha e_2] = [R_\alpha u(0) | R_\alpha u(\pi/2)] = [u(\alpha) | u(\alpha + \pi/2)] \\ &= \begin{bmatrix} \cos\alpha & \cos(\alpha + \pi/2) \\ \sin\alpha & \sin(\alpha + \pi/2) \end{bmatrix} = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}. \end{aligned}$$

We also define reflection, S_α, across the line determined by $u(\alpha)$ as in Figure 1.3 so that $S_\alpha u(\theta) := u(2\alpha - \theta)$. We may compute the matrix representing S_α

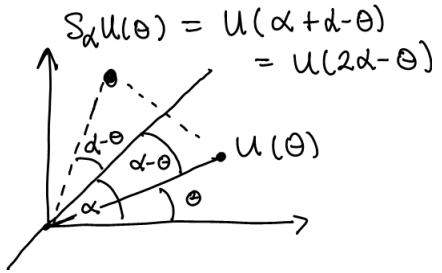

Fig. 1.3. Computing S_α.

as,

$$\begin{aligned} S_\alpha &= [S_\alpha e_1 | S_\alpha e_2] = [S_\alpha u(0) | S_\alpha u(\pi/2)] = [u(2\alpha) | u(2\alpha - \pi/2)] \\ &= \begin{bmatrix} \cos 2\alpha & \cos(2\alpha - \pi/2) \\ \sin 2\alpha & \sin(2\alpha - \pi/2) \end{bmatrix} = \begin{bmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{bmatrix}. \end{aligned}$$

Proposition 1.72. *The elements, $O(2) := \{S_\alpha, R_\alpha : \alpha \in \mathbb{R}\}$ form a subgroup $GL_2(\mathbb{R})$, moreover we have the following multiplication rules:*

$$R_\alpha R_\beta = R_{\alpha+\beta}, \quad S_\alpha S_\beta = R_{2(\alpha-\beta)}, \tag{1.15}$$

$$R_\beta S_\alpha = S_{\alpha+\beta/2}, \quad \text{and } S_\alpha R_\beta = S_{\alpha-\beta/2}. \tag{1.16}$$

for all $\alpha, \beta \in \mathbb{R}$.

Proof. Equations (1.15) and (1.16) may be verified by direct computations using the matrix representations for R_α and S_β. Perhaps a more illuminating way is to notice that all linear transformations on $\mathbb{R}^2$ are determined by there actions on $u(\theta)$ for all θ (actually for two θ is typically enough). Using this remark we find,

$$R_\alpha R_\beta u(\theta) = R_\alpha u(\theta+\beta) = u(\theta+\beta+\alpha) = R_{\alpha+\beta}u(\theta)$$
$$S_\alpha S_\beta u(\theta) = S_\alpha u(2\beta-\theta) = u(2\alpha-(2\beta-\theta)) = u(2(\alpha-\beta)+\theta) = R_{2(\alpha-\beta)}u(\theta),$$
$$R_\beta S_\alpha u(\theta) = R_\beta u(2\alpha-\theta) = u(2\alpha-\theta+\beta) = u(2(\alpha+\beta/2)-\theta) = S_{\alpha+\beta/2}u(\theta),$$

and

$$S_\alpha R_\beta u(\theta) = S_\alpha u(\theta+\beta) = u(2\alpha-(\theta+\beta)) = u(2(\alpha-\beta/2)-\theta) = S_{\alpha-\beta/2}u(\theta)$$

which verifies equations (1.15) and (1.16). From these it is clear that H is a closed under matrix multiplication and since $R_{-\alpha} = R_\alpha^{-1}$ and $S_\alpha^{-1} = S_\alpha$ it follows H is closed under taking inverses. ∎

1.6.2 Dihedral Groups

Definition 1.73 (Dihedral Groups). *For* $n \geq 3$, *the* ***dihedral group***, D_n, *is the symmetry group of a regular* n *– gon. To be explicit this may be realized as the sub-groups* $O(2)$ *defined as*

$$D_n = \left\{ R_{k\frac{2\pi}{n}}, S_{k\frac{\pi}{n}} : k = 0, 1, 2, \ldots, n-1 \right\},$$

see the Figures below. Notice that $|D_n| = 2n$.

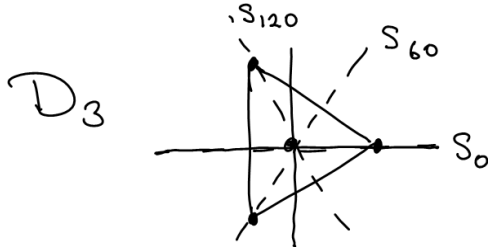

Fig. 1.4. The 3 reflection symmetries axis of a regular 3 – gon,. i.e. a equilateral triangle.

See the book and the demonstration in class for more intuition on these groups. For computational purposes, we may present D_n in terms of generators and relations as follows.

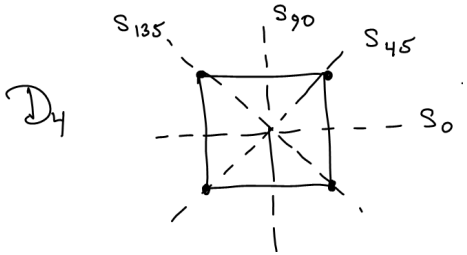

Fig. 1.5. The 4− reflection symmetries axis of a regular 4 – gon,. i.e. a square.

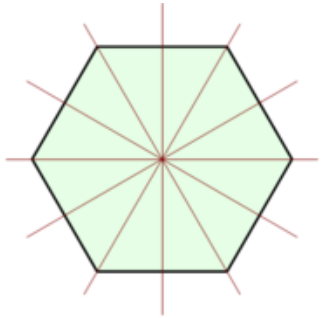

Fig. 1.6. The 6− reflection symmety axis of a regular 6 – gon,. i.e. a heagon. There are also 6 rotation symmetries.