Part II

Math 103A Lecture Notes

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 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,

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

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.

■

Lecture 2 (1/7/2009)

Definition 2.1. *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 2.2. *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 2.3. Notice that $\gcd(a, b) = \gcd(|a|, |b|) \geq 0$ and $\gcd(a, 0) = 0$ for all $a \neq 0$.

Lemma 2.4. *Suppose that $a, b \in \mathbb{Z}$ with $b \neq 0$. Then $\gcd(a + kb, b) = \gcd(a, b)$ for all $k \in \mathbb{Z}$.*

Proof. Let S_k denote the set of common divisors of $a + kb$ and b. If $d \in S_k$, then $d|b$ and $d|(a + kb)$ and therefore $d|a$ so that $d \in S_0$. Conversely if $d \in S_0$, then $d|b$ and $d|a$ and therefore $d|b$ and $d|(a + kb)$, i.e. $d \in S_k$. This shows that $S_k = S_0$, i.e. $a + kb$ and b and a and b have the same common divisors and hence the same greatest common divisors. ■

This lemma has a very useful corollary.

Lemma 2.5 (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. Then $\gcd(a, b) = \gcd(a, r)$ and in particular if $r = 0$, we have*

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

Example 2.6. 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 2.5 repeatedly as follows;

$$28 = 1 \cdot 15 + 13 \text{ so } \gcd(15, 28) = \gcd(13, 15), \tag{2.1}$$
$$15 = 1 \cdot 13 + 2 \text{ so } \gcd(13, 15) = \gcd(2, 13), \tag{2.2}$$
$$13 = 6 \cdot 2 + 1 \text{ so } G\gcd(2, 13) = \gcd(1, 2), \tag{2.3}$$
$$2 = 2 \cdot 1 + 0 \text{ so } \gcd(1, 2) = \gcd(0, 1) = 1. \tag{2.4}$$

Moreover making use of Eqs. (2.1–2.3) 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 2.7. 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 2.8. 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 2.5 gives,

$$\begin{aligned}
459 &= 1 \cdot 333 + 126 \text{ so } \gcd(333, 459) = \gcd(126, 333), && (2.5)\\
333 &= 2 \cdot 126 + 81 \text{ so } \gcd(126, 333) = \gcd(81, 126), && (2.6)\\
126 &= 81 + 45 \text{ so } \gcd(81, 126) = \gcd(45, 81), && (2.7)\\
81 &= 45 + 36 \text{ so } \gcd(45, 81) = \gcd(36, 45), && (2.8)\\
45 &= 36 + 9 \text{ so } \gcd(36, 45) = \gcd(9, 36), \text{ and} && (2.9)\\
36 &= 4 \cdot 9 + 0 \text{ so } \gcd(9, 36) = \gcd(0, 9) = 9. && (2.10)
\end{aligned}$$

Thus we have shown that

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

We can even say more. From Eq. (2.10) we have, $9 = 45 - 36$ and then from Eq. (2.10),

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

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 2.9 below. However, we will two different variants of the proof.

Theorem 2.9. *If $a, b \in \mathbb{Z} \setminus \{0\}$, then there exists (not unique) numbers, $s, t \in \mathbb{Z}$ such that*

$$\gcd(a, b) = sa + tb. \tag{2.11}$$

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. (2.11).) 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

$$d := \min(S \cap \mathbb{Z}_+) = sa + tb \text{ for some } s, t \in \mathbb{Z}. \tag{2.12}$$

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,

$$a = kd + r \text{ with } 0 \leq r < d. \tag{2.13}$$

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. (2.12) which would contradict Eq. (2.13). Hence it follows that $r = 0$ and $d|a$. Similarly, one shows that $d|b$. ■

Lemma 2.10 (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 2.11. *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 $\gcd(a, b) = 1$. ■

2.1 Ideals (Not covered in class.)

Definition 2.12. *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 2.13. 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 2.14 (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 2.15. Notice that $a|b$ iff $b = ak$ for some $k \in \mathbb{Z}$ which happens iff $b \in (a)$.

Proof. Second Proof of Theorem 2.9. 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 2.16. As a second proof of Corollary 2.11, if $1 \in S$ (where S is as in the second proof of Theorem 2.9)), then $\gcd(a, b) = \min(S \cap \mathbb{Z}_+) = 1$.

Lecture 3 (1/9/2009)

3.1 Prime Numbers

Definition 3.1. *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 3.2. The first few prime numbers are $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$.

Lemma 3.3 (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 2.10 to conclude that $p|b$ and so again we are done. ■

Theorem 3.4 (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 2.10, $p_1 | (q_2 \ldots q_m)$. 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 3.5. *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 3.6. 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

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

then

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

Therefore,

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

3.2 Modular Arithmetic

Definition 3.7. *Let n be a positive integer and let $a = q_a n + r_a$ with $0 \leq r_a < n$. 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 3.8. *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,
$$a\cdot b=[q_an+r_a]\cdot[q_bn+r_b]=(q_aq_bn+r_aq_b+r_bq_a)\,n+r_a\cdot r_b$$
and so again by item 1. with $k=(q_aq_bn+r_aq_b+r_bq_a)$ we have,
$$(a\cdot b)\bmod n=(r_a\cdot r_b)\bmod n=((a\bmod n)\cdot(b\bmod n))\bmod n.$$

■

Example 3.9. 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 3.10 (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 3.11. Suppose that $a,n\in\mathbb{Z}_+$ and $b\in\mathbb{Z}$, then it is easy to show (you prove)
$$(ab)\bmod(an)=a\cdot(b\bmod n)\,.$$

Example 3.12 (Computing mod 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
$$a_n\ \ldots a_2\ a_1\bmod 10^k=a_k\ \ldots a_2\ a_1\text{ for all }k\le n.$$

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 3.12, $111\ldots1\bmod 10=1$ 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,
$$\begin{aligned}10=\left(n^2-1\right)\bmod 100&=\left[(k\cdot 10+1)^2-1\right]\bmod 100=\left(k^2\cdot 100+2k\cdot 10\right)\bmod 100\\&=(2k\cdot 10)\bmod 100=10\cdot(2k\bmod 10)\end{aligned}$$
which implies $1=(2k\bmod 10)$ which is impossible since $2k\bmod 10$ is even.

For the second case we must have,
$$\begin{aligned}10=\left(n^2-1\right)\bmod 100\bmod 100&=\left[(k\cdot 10+9)^2-1\right]\bmod 100\\&=\left(k^2\cdot 100+18k\cdot 10+81-1\right)\bmod 100\\&=((10+8)\,k\cdot 10+8\cdot 10)\bmod 100\\&=(8\,(k+1)\cdot 10)\bmod 100\\&=10\cdot 8k\bmod 10\end{aligned}$$
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 $111\dots 11 = 111\dots 00 + 11$ and therefore,

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

On the other hand, if $111\dots 11 = n^2$ 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 $3^2 \bmod 4 = 1 \neq 3$.

3.3 Equivalence Relations

Definition 3.13. *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 3.14. 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 3.15. 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 3.16. Let $S = \mathbb{R}$ and say $a \sim b$ iff $a \geq b$. Again not symmetric so is not an equivalence relation.

Definition 3.17. *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 3.18. 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.

4

Lecture 4 (1/12/2009)

Theorem 4.1. *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 4.1. Suppose that $S = \mathbb{Z}$ with $a \sim b$ iff $a \bmod n = b \bmod n$. Identify the equivalence classes of $\sim$. Answer,

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

where

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

Exercise 4.2. 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 $(0,0) \in S$.

4.1 Binary Operations and Groups – a first look

Definition 4.2. *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 4.3. 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 $* =$ “\” = “ $\div$ ”.
6. Let S be the set of 2×2 real (complex) matrices with $A * B := AB$.

Definition 4.4. *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 4.5 (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 4.6 (Commutative Group). *A group, (G, e), is commutative if $gh = hg$ for all $h, g \in G$.*

Example 4.7 ($(\mathbb{Z}, +)$). 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 4.8. $S = \mathbb{Z}$ 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 4.9 ($(\mathbb{R}\setminus\{0\}, \cdot)$). $G = \mathbb{R}\setminus\{0\} =: \mathbb{R}^*$, and $* =$“$\cdot$” is a commutative group, $e = 1$, an inverse to a is $1/a$.

Example 4.10. $S = \mathbb{R}\setminus\{0\}$ with $* =$ “\” = “$\div$”. In this case $*$ is not associative since

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

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 4.11. 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 4.12 ($GL_2(\mathbb{R})$). 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

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

Example 4.13 ($SL_2(\mathbb{R})$). 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 $A, B \in SL_2(\mathbb{R})$.

5

Lecture 5 (1/14/2009)

5.1 Elementary Properties of Groups

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

Lemma 5.1. *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 5.2. *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 5.3 (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 5.4. *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 5.5 *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 5.6. 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 5.7. *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 $g_1 \dots g_n g_{n+1}$. 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

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

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. $\dots g_n \overbrace{) \dots)}^{k+1}$. 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 $\dots g_n \overbrace{) \dots)}^{k+1} = M_{n+1} (g_1, \dots, g_{n+1})$. ■

Notation 5.8 *For $n \in \mathbb{Z}$ and $g \in G$, let $g^n := \overbrace{g \dots g}^{n \ times}$ and $g^{-n} := \overbrace{g^{-1} \dots g^{-1}}^{n \ times} = \left(g^{-1}\right)^n$ 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,

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

5.2 More Examples of Groups

Example 5.9. 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 5.10 ($\mathbb{Z}_n$). For any $n \geq 2$, $G := \mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ 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 5.11. Suppose that $S = \{0, 1, 2, \dots, n-1\}$ 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 9.8. 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.)

6

Lecture 6 (1/16/2009)

Theorem 6.1 (The groups, $U(n)$). *For $n \geq 2$, let*

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

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 commutative.

Claim: an element $a \in \{1, 2, \dots, n-1\}$ is in $U(n)$ iff there exists $r \in \{1, 2, \dots, n-1\}$ 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 $r := s \bmod n \in \{1, 2, \dots, n-1\}$ and $r * a = 1$.

$(\Longleftarrow)$ If there exists $r \in \{1, 2, \dots, n-1\}$ such that $1 = r * a = ra \bmod n$, then $n | (ra - 1)$, 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 6.2 ($U(10)$). $U(10) = \{1, 3, 7, 9\}$ 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 6.3. If p is prime, then $U(p) = \{1, 2, \dots, p\}$. For example $U(5) = \{1, 2, 3, 4\}$ with Cayley table given by,

$$\begin{array}{c|cccc} a\backslash b & 1 & 2 & 3 & 4 \\ \hline 1 & 1 & 2 & 3 & 4 \\ 2 & 2 & 4 & 1 & 3 \\ 3 & 3 & 1 & 4 & 2 \\ 4 & 4 & 3 & 2 & 1 \end{array}.$$

Exercise 6.1. Compute 23^{-1} inside of $U(50)$.

Solution to Exercise. We use the division algorithm (see below) to show $1 = 6 \cdot 50 - 13 \cdot 23$. Taking this equation mod 50 shows that $23^{-1} = (-13) = 37$. As a check we may show directly that $(23 \cdot 37) \bmod 50 = 1$.

Here is the division algorithm calculation:

$$\begin{aligned} 50 &= 2 \cdot 23 + 4 \\ 23 &= 5 \cdot 4 + 3 \\ 4 &= 3 + 1. \end{aligned}$$

So working backwards we find,

$$\begin{aligned} 1 &= 4 - 3 = 4 - (23 - 5 \cdot 4) = 6 \cdot 4 - 23 = 6 \cdot (50 - 2 \cdot 23) - 23 \\ &= 6 \cdot 50 - 13 \cdot 23. \end{aligned}$$

6.1 $O(2)$ – reflections and rotations in $\mathbb{R}^2$

Definition 6.4 (Sub-group). *Let $(G,\cdot)$ be a group. A non-empty subset, $H \subset G$, is said to be a subgroup of G if H is also a group under the multiplication law in G. We use the notation, $H \leq G$ to summarize that H is a subgroup of G and $H < G$ to summarize that H is a **proper** subgroup of 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 6.1 let

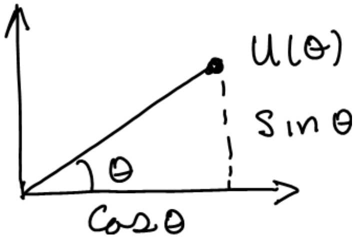


Fig. 6.1. The unit vector, $u(\theta)$, at angle θ to the x – axis.

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

We also let R_α denote rotation by α degrees counter clockwise so that $R_\alpha u(\theta) = u(\theta+\alpha)$ as in Figure 6.2. We may represent R_α as a matrix, namely

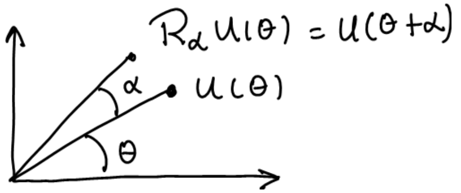


Fig. 6.2. Rotation by α degrees in the counter clockwise direction.

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

We also define reflection, S_α, across the line determined by $u(\alpha)$ as in Figure 6.3 so that $S_\alpha u(\theta) := u(2\alpha-\theta)$. We may compute the matrix representing S_α

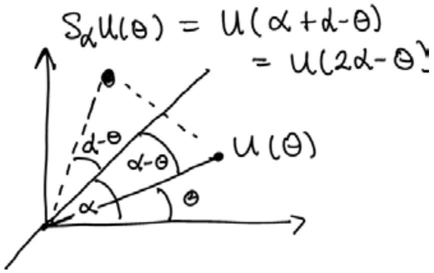


Fig. 6.3. Computing S_α.

as,

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

7

Lecture 7 (1/21/2009)

Definition 7.1 (Sub-group). *Let $(G, \cdot)$ be a group. A non-empty subset, $H \subset G$, is said to be a subgroup of G if H is also a group under the multiplication law in G. We use the notation, $H \leq G$ to summarize that H is a subgroup of G and $H < G$ to summarize that H is a* ***proper*** *subgroup of G.*

Theorem 7.2 (Two-step Subgroup Test). *Let G be a group and H be a non-empty subset. Then $H \leq G$ 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 $h \in H$.*

Proof. First off notice that $e = h^{-1}h \in H$. It also clear that H contains inverses and the multiplication law is associative, thus $H \leq G$. ∎

Theorem 7.3 (One-step Subgroup Test). *Let G be a group and H be a non-empty subset. Then $H \leq G$ iff $ab^{-1} \in H$ whenever $a, b \in H$.*

Proof. If $a \in H$, then $e = a\, a^{-1} \in H$ and hence so is $a^{-1} = ae^{-1} \in H$. Thus it follows that for $a, b \in H$, that $ab = a\left(b^{-1}\right)^{-1} \in H$ and hence $H \leq G$. and the result follows from Theorem 7.2. ∎

Example 7.4. Here are some examples of sub-groups and not sub-groups.

1. $2\mathbb{Z} < \mathbb{Z}$ while $3\mathbb{Z} \subset \mathbb{Z}$ but is not a sub-group.
2. $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\} \subset \mathbb{Z}$ is not a subgroup of $\mathbb{Z}$ since they have different group operations.
3. $\{e\} \leq G$ is the trivial subgroup and $G \leq G$.

Example 7.5. Let us find the smallest sub-group, H containing $7 \in U(15)$. Answer,

$$7^2 \bmod 15 = 4,\ 7^3 \bmod 15 = 13,\ 7^4 \bmod 15 = 1$$

so that H must contain, $\{1, 7, 4, 13\}$. One may easily check this is a subgroup and we have $|7| = 4$.

Proposition 7.6. *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:*

$$R_\alpha R_\beta = R_{\alpha+\beta}, \quad S_\alpha S_\beta = R_{2(\alpha-\beta)}, \tag{7.1}$$
$$R_\beta S_\alpha = S_{\alpha+\beta/2}, \quad \text{and } S_\alpha R_\beta = S_{\alpha-\beta/2}. \tag{7.2}$$

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

$$R_\alpha = R_\beta \iff \alpha = \beta \bmod 360 \tag{7.3}$$

while,

$$S_\alpha = S_\beta \iff \alpha = \beta \bmod 180. \tag{7.4}$$

Proof. Equations (7.1) and (7.2) 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,

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

which verifies equations (7.1) and (7.2). 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.

To finish the proof we will now verify Eq. (7.4) and leave the proof of Eq. (7.3) to the reader. The point is that $S_\alpha = S_\beta$ iff

$$u(2\alpha-\theta) = S_\alpha u(\theta) = S_\beta u(\theta) = u(2\beta-\theta) \text{ for all } \theta$$

which happens iff

$$[2\alpha-\theta] \bmod 360 = [2\beta-\theta] \bmod 360$$

which is equivalent to $\alpha = \beta \bmod 180$. ∎

8

Lecture 8 (1/23/2009)

Notation 8.1 *The **order of a group,** G, is the number of elements in G which we denote by $|G|$.*

Example 8.2. We have $|\mathbb{Z}| = \infty$, $|\mathbb{Z}_n| = n$ for all $n \geq 2$, and $|D_3| = 6$ and $|D_4| = 8$.

Definition 8.3 (Euler Phi – function). *For $n \in \mathbb{Z}_+$, let*

$$\varphi(n) := |U(n)| = \#\{1 \leq k \leq n : \gcd(k, n) = 1\}.$$

*This function, φ, is called the **Euler Phi – function.***

Example 8.4. If p is prime, then $U(p) = \{1, 2, \ldots, p-1\}$ and $\varphi(p) = p - 1$. More generally $U(p^n)$ consists of $\{1, 2, \ldots, p^n\} \setminus \{\text{multiples of } p \text{ in } \{1, 2, \ldots, p^n\}\}$. Therefore,

$$\varphi(p^n) = |U(p^n)| = p^n - \#\{\text{multiples of } p \text{ in } \{1, 2, \ldots, p^n\}\}$$

Since

$$\{\text{multiples of } p \text{ in } \{1, 2, \ldots, p^n\}\} = \left\{kp : k = 1, 2, \ldots, p^{n-1}\right\}$$

it follows that $\#\{\text{multiples of } p \text{ in } \{1, 2, \ldots, p^n\}\} = p^{n-1}$ and therefore,

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

valid for all primes and $n \geq 1$.

Example 8.5 ($\varphi(p^m q^n)$). Let $N = p^m q^n$ with $m, n \geq 1$ and p and q being distinct primes. We wish to compute $\varphi(N) = |U(N)|$. To do this, let let $\Omega := \{1, 2, \ldots, N-1, N\}$, A be the multiples of p in Ω and B be the multiples of q in Ω. Then $A \cap B$ is the subset of common multiples of p and q or equivalently multiples of pq in Ω so that;

$$\begin{aligned} \#(A) &= N/p = p^{m-1}q^n, \\ \#(B) &= N/q = p^m q^{n-1} \text{ and} \\ \#(A \cap B) &= N/(pq) = p^{m-1}q^{n-1}. \end{aligned}$$

Therefore,

$$\begin{aligned} \varphi(N) &= \#(\Omega \setminus (A \cup B)) = \#(\Omega) - \#(A \cup B) \\ &= \#(\Omega) - [\#(A) + \#(B) - \#(A \cap B)] \\ &= N - \left[\frac{N}{p} + \frac{N}{q} - \frac{N}{p \cdot q}\right] \\ &= p^m \cdot q^n - p^{m-1} \cdot q^n - p^m \cdot q^{n-1} + p^{m-1} \cdot q^{n-1} \\ &= \left(p^m - p^{m-1}\right)\left(q^n - q^{n-1}\right). \end{aligned}$$

which after a little algebra shows,

$$\varphi(p^m q^n) = \left(p^m - p^{m-1}\right)\left(q^n - q^{n-1}\right) = N\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right).$$

The next theorem generalizes this example.

Theorem 8.6 (Euler Phi function). *Suppose that $N = p_1^{k_1} \ldots p_n^{k_n}$ with $k_i \geq 1$ and p_i being distinct primes. Then*

$$\varphi(N) = \varphi\left(p_1^{k_1} \ldots p_n^{k_n}\right) = \prod_{i=1}^n \left(p_i^{k_i} - p_i^{k_i - 1}\right) = N \cdot \prod_{i=1}^n \left(1 - \frac{1}{p_i}\right).$$

Proof. (Proof was not given in class!) Let $\Omega := \{1, 2, \ldots, N\}$ and $A_i := \{m \in \Omega : p_i | m\}$. It then follows that $U(N) = \Omega \setminus (\cup_{i=1}^n A_i)$ and therefore,

$$\varphi(N) = \#(\Omega) - \#(\cup_{i=1}^n A_i) = N - \#(\cup_{i=1}^n A_i).$$

To compute the later expression we will make use of the inclusion exclusion formula which states,

$$\#(\cup_{i=1}^n A_i) = \sum_{l=1}^n (-1)^{l+1} \sum_{1 \leq i_1 < i_2 < \cdots < i_l \leq n} \#(A_{i_1} \cap \cdots \cap A_{i_l}). \tag{8.1}$$

Here is a way to see this formula. For $A \subset \Omega$, let $1_A(k) = 1$ if $k \in A$ and 0 otherwise. We now have the identity,

$$\begin{aligned} 1 - 1_{\cup_{i=1}^n A_i} &= \prod_{i=1}^n (1 - 1_{A_i}) \\ &= 1 - \sum_{l=1}^n (-1)^l \sum_{1 \le i_1 < i_2 < \dots < i_l \le n} 1_{A_{i_1} \cap \dots \cap A_{i_l}}. \end{aligned}$$

Summing this identity on $k \in \Omega$ then shows,

$$N - \# \left(\cup_{i=1}^n A_i \right) = N - \sum_{l=1}^n (-1)^l \sum_{1 \le i_1 < i_2 < \dots < i_l \le n} \# \left(A_{i_1} \cap \dots \cap A_{i_l} \right)$$

which gives Eq. (8.1).

Since $A_{i_1} \cap \dots \cap A_{i_l}$ consists of those $k \in \Omega$ which are common multiples of $p_{i_1}, p_{i_2}, \dots, p_{i_l}$ or equivalently multiples of $p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_l}$, it follows that

$$\# \left(A_{i_1} \cap \dots \cap A_{i_l} \right) = \frac{N}{p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_l}}.$$

Thus we arrive at the formula,

$$\begin{aligned} \varphi(N) &= N - \sum_{l=1}^n (-1)^{l+1} \sum_{1 \le i_1 < i_2 < \dots < i_l \le n} \frac{N}{p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_l}} \\ &= N + \sum_{l=1}^n (-1)^l \sum_{1 \le i_1 < i_2 < \dots < i_l \le n} \frac{N}{p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_l}} \end{aligned}$$

Let us now break up the sum over those terms with $i_l = n$ and those with $i_l < n$ to find,

$$\begin{aligned} \varphi(N) = & \left[N + \sum_{l=1}^{n-1} (-1)^l \sum_{1 \le i_1 < i_2 < \dots < i_l < n} \frac{N}{p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_l}} \right] \\ & + \left[\sum_{l=1}^{n} (-1)^l \sum_{1 \le i_1 < i_2 < \dots < i_{l-1} < i_l = n} \frac{N}{p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_l}} \right]. \end{aligned}$$

We may factor out $p_n^{k_n}$ in the first term to find,

$$\varphi(N) = p_n^{k_n} \varphi\left(p_1^{k_1} \dots p_{n-1}^{k_{n-1}} \right) + \sum_{l=1}^n (-1)^l \sum_{1 \le i_1 < i_2 < \dots < i_{l-1} < i_l = n} \frac{N}{p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_l}}.$$

Similarly the second term is equal to:

$$\begin{aligned} & p_n^{k_n - 1} \left[-p_1^{k_1} \dots p_{n-1}^{k_{n-1}} + \sum_{l=2}^n (-1)^l \sum_{1 \le i_1 < i_2 < \dots < i_{l-1} < n} \frac{p_1^{k_1} \dots p_{n-1}^{k_{n-1}}}{p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_{l-1}}} \right] \\ &= p_n^{k_n - 1} \left[-p_1^{k_1} \dots p_{n-1}^{k_{n-1}} - \sum_{l=1}^{n-1} (-1)^l \sum_{1 \le i_1 < i_2 < \dots < i_l < n} \frac{p_1^{k_1} \dots p_{n-1}^{k_{n-1}}}{p_{i_1} \cdot p_{i_2} \cdot \dots \cdot p_{i_l}} \right] \\ &= -p_n^{k_n - 1} \varphi\left(p_1^{k_1} \dots p_{n-1}^{k_{n-1}} \right). \end{aligned}$$

Thus we have shown

$$\begin{aligned} \varphi(N) &= p_n^{k_n} \varphi\left(p_1^{k_1} \dots p_{n-1}^{k_{n-1}} \right) - p_n^{k_n - 1} \varphi\left(p_1^{k_1} \dots p_{n-1}^{k_{n-1}} \right) \\ &= \left(p_n^{k_n} - p_n^{k_n - 1} \right) \varphi\left(p_1^{k_1} \dots p_{n-1}^{k_{n-1}} \right) \end{aligned}$$

and so the result now follows by induction. ■

Corollary 8.7. *If $m, n \ge 1$ and $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m) \varphi(n)$.*

Notation 8.8 *For $g \in G$, let $\langle g \rangle := \{ g^n : n \in \mathbb{Z} \}$. We call $\langle g \rangle$ the **cyclic subgroup generated by** g (as justified by the next proposition).*

Proposition 8.9 (Cyclic sub-groups). *For all $g \in G$, $\langle g \rangle \le G$.*

Proof. For $m, n \in \mathbb{Z}$ we have $g^n (g^m)^{-1} = g^{n-m} \in \langle g \rangle$ and therefore by the one step subgroup test, $\langle g \rangle \le G$. ■

Notation 8.10 *The **order of an element,** $g \in G$, is*

$$|g| := \min \{ n \ge 1 : g^n = e \}$$

with the convention that $|g| = \infty$ if $\{ n \ge 1 : g^n = e \} = \emptyset$.

Lemma 8.11. *Let $g \in G$. Then $|g| = \infty$ iff no two elements in the list,*

$$\{ g^n : n \in \mathbb{Z} \} = \left\{ \dots, g^{-2}, g^{-1}, g^0 = e, g^1 = g, g^2, \dots \right\}$$

are equal.

Theorem 8.12. *Suppose that g is an element of a group, G. Then either:*

1. *If $|g| = \infty$ then all elements in the list, $\{ g^n : n \in \mathbb{Z} \}$, defining $\langle g \rangle$ are distinct. In particular $|\langle g \rangle| = \infty = |g|$.*
2. *If $n := |g| < \infty$, then $g^m = g^{m \bmod n}$ for all $m \in \mathbb{Z}$,*

$$\langle g \rangle = \left\{ e, g, g^2, \dots, g^{n-1} \right\} \tag{8.2}$$

with all elements in the list being distinct and $|\langle g \rangle| = n = |g|$. We also have,

$$g^k g^l = g^{(k+l) \bmod n} \text{ for all } k, l \in \mathbb{Z}_n \tag{8.3}$$

which shows that $\langle g \rangle$ is "equivalent" to $\mathbb{Z}_n$.

So in all cases $|g| = |\langle g \rangle|$.

Proof. 1. If $g^i = g^j$ for some $i < j$, then

$$e = g^i g^{-i} = g^j g^{-i} = g^{j-i}$$

so that $g^m = e$ with $m = j - i \in \mathbb{Z}_+$ from which we would conclude that $|g| < \infty$. Thus if $|g| = \infty$ it must be that all elements in the list, $\{g^n : n \in \mathbb{Z}\}$, are distinct. In particular $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ has an infinite number of elements and therefore $|\langle g \rangle| = \infty$.

2. Now suppose that $n = |g| < \infty$. Since $g^n = e$, it also follows that $g^{-n} = (g^n)^{-1} = e^{-1} = e$. Therefore if $m \in \mathbb{Z}$ and $m = sn + r$ where $r := m \mod n$, then $g^m = (g^n)^s g^r = g^r$, i.e. $g^m = g^{m \bmod n}$ for all $m \in \mathbb{Z}$. Hence it follows that $\langle g \rangle = \left\{e, g, g^2, \dots, g^{n-1}\right\}$. Moreover if $g^i = g^j$ for some $0 \le i \le j < n$, then $g^{j-i} = e$ with $j - i < n$ and hence $j = i$. Thus the list in Eq. (8.2) consists of distinct elements and therefore $|\langle g \rangle| = n$. Lastly, if $k, l \in \mathbb{Z}_n$, then

$$g^k g^l = g^{k+l} = g^{(k+l) \bmod n}.$$

■

9

Lecture 9 (1/26/2009)

Corollary 9.1. *Let $a \in G$. Then $a^i = a^j$ iff $|a|$ divides $(j-i)$. Here we use the convention that ∞ divides m iff $m = 0$. In particular, $a^k = e$ iff $|a|\,|k$.*

Corollary 9.2. *For all $g \in G$ we have $|g| \le |G|$.*

Proof. This follows from the fact that $|g| = |\langle g\rangle|$ and $\langle g\rangle \subset G$. ■

Theorem 9.3 (Finite Subgroup Test). *Let H be a non-empty finite subset of a group G which is closed under the group law, then $H \le G$.*

Proof. To each $h \in H$ we have $\left\{h^k\right\}_{k=1}^{\infty} \subset H$ and since $\#(H) < \infty$, it follows that $h^k = h^l$ for some $k \ne l$. Thus by Theorem 8.12, $|h| < \infty$ for all $h \in H$ and $\langle h\rangle = \left\{e, h, h^2, \dots, h^{|h|-1}\right\} \subset H$. In particular $h^{-1} \in \langle h\rangle \subset H$ for all $h \in H$. Hence it follows by the two step subgroup test that $H \le G$. ■

Definition 9.4 (Centralizer of a in G). *The **centralizer** of $a \in G$, denoted $C(a)$, is the set of $g \in G$ which commute with a, i.e.*

$$C(a) := \{g \in G : ga = ag\}.$$

More generally if $S \subset G$ is any non-empty set we define

$$C(S) := \{g \in G : gs = sg \text{ for all } s \in S\} = \cap_{s\in S} C(s).$$

Lemma 9.5. *For all $a \in G$, $\langle a\rangle \le C(a) \le G$.*

Proof. If $g \in C(a)$, then $ga = ag$. Multiplying this equation on the right and left by g^{-1} then shows,

$$ag^{-1} = g^{-1}gag^{-1} = g^{-1}agg^{-1} = g^{-1}a$$

which shows $g^{-1} \in C(a)$. Moreover if $g, h \in C(a)$, then $gha = gah = agh$ which shows that $gh \in C(a)$ and therefore $C(a) \le G$. ■

Example 9.6. If G is abelian, then $C(a) = G$ for all $a \in G$.

Example 9.7. Let $G = GL_2(\mathbb{R})$ we will compute $C(A_1)$ and $C(A_2)$ where

$$A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } A_2 := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

1. We have $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C(A_1)$ iff,

$$\begin{bmatrix} b & a \\ d & c \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}$$

which means that $b = c$ and $a = d$, i.e. B must be of the form,

$$B = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$$

and therefore,

$$C(A_1) = \left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix} : a^2 - b^2 \ne 0\right\}.$$

2. We have $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C(A_2)$ iff,

$$\begin{bmatrix} a & -b \\ c & -d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ -c & -d \end{bmatrix}$$

which happens iff $b = c = 0$. Thus we have,

$$C(A_2) = \left\{\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} : ad \ne 0\right\}.$$

Lemma 9.8. *If $\{H_i\}$ is a collection of subgroups of G then $H := \cap_i H_i \le G$ as well.*

Proof. If $h, k \in H$ then $h, k \in H_i$ for all i and therefore $hk^{-1} \in H_i$ for all i and hence $hk^{-1} \in H$. ■

Corollary 9.9. *$C(S) \le G$ for any non-empty subset $S \subset G$.*

Definition 9.10 (Center of a group). *Center of a group, denoted $Z(G)$, is the centralizer of G, i.e.*

$$Z(G) = C(G) := \{a \in G : ax = xa \text{ for all } x \in G\}$$

By Corollary 9.9, $Z(G) = C(G)$ is a group. Alternatively, if $a \in Z(G)$, then $ax = xa$ implies $a^{-1}x^{-1} = x^{-1}a^{-1}$ which implies $xa^{-1} = a^{-1}x$ for all $x \in G$ and therefore $a^{-1} \in Z(G)$. If $a, b \in Z(G)$, then $abx = axb = xab \implies ab \in Z(G)$, which again shows $Z(G)$ is a group.

Example 9.11. G is a abelian iff $Z(G) = G$, thus $Z(\mathbb{Z}_n) = \mathbb{Z}_n$, $Z(U(n)) = U(n)$, etc.

Example 9.12. Using Example 9.7 we may easily show $Z(GL_2(\mathbb{R})) = \{\lambda I : \lambda \in \mathbb{R}\setminus\{0\}\}$. Indeed,

$$Z(GL_2(\mathbb{R})) \subset C(A_1) \cap C(A_2) = \left\{\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a^2 \neq 0\right\} = \{\lambda I : \lambda \in \mathbb{R}\setminus\{0\}\}.$$

As the latter matrices commute with every matrix we also have,

$$Z(GL_2(\mathbb{R})) \subset \{\lambda I : \lambda \in \mathbb{R}\setminus\{0\}\} \subset Z(GL_2(\mathbb{R})).$$

Remark 9.13. If $S \subset G$ is a non-empty set we let $\langle S \rangle$ denote the smallest subgroup in G which contains S. This subgroup may be constructed as finite products of elements from S and $S^{-1} := \{s^{-1} : s \in S\}$. It is not too hard to prove that

$$C(S) = C(\langle S \rangle).$$

Let us also note that if $S \subset T \subset G$, then $C(T) \subset C(S)$ as there are more restrictions on $x \in G$ to be in $C(T)$ than there are for $x \in G$ to be in $C(S)$.

9.1 Dihedral group formalities and examples

Definition 9.14 (General 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 $|D_n| = 2n$.

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.

Theorem 9.15 (A presentation of D_n). *Let $n \geq 3$ and $r := R_{\frac{2\pi}{n}}$ and $f = S_0$. Then*

$$D_n = \{r^k, r^k f : k = 0, 1, 2, \ldots, n-1\} \tag{9.1}$$

and we have the relations, $r^n = 1$, $f^2 = 1$, and $frf = r^{-1}$. We say that r and f are generators for D_n.

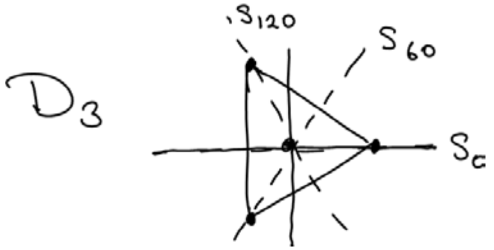


Fig. 9.1. The 3 reflection symmetries axis of a regular 3 – gon,. i.e. a equilateral triangle.

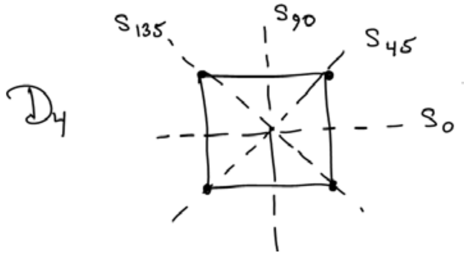


Fig. 9.2. The 4− reflection symmetries axis of a regular 4 – gon,. i.e. a square.

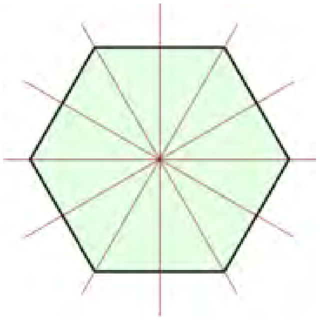


Fig. 9.3. The 6− reflection symmety axis of a regular 6 – gon,. i.e. a heagon. There are also 6 rotation symmetries.

Proof. We know that $r^k = R_{k\frac{2\pi}{n}}$ and that $r^k f = R_{k\frac{2\pi}{n}} S_0 = S_{k\frac{\pi}{n}}$ from which Eq. (9.1) follows. It is also clear that $r^n = 1 = f^2$. Moreover,

$$frf = S_0 R_{\frac{2\pi}{n}} S_0 = S_0 S_{\frac{\pi}{n}} = R_{2\left(0-\frac{\pi}{n}\right)} = r^{-1}$$

as desired. (Poetically, a rotation viewed through a mirror is a rotation in the opposite direction.) ■

For computational purposes, observe that

$$fr^3 f = frf\ frf\ frf = \left(r^{-1}\right)^3 = r^{-3}$$

and therefore $fr^{-3}f = f\left(fr^3 f\right)f = r^3$. In general we have $fr^k f = r^{-k}$ for all $k \in \mathbb{Z}$.

Example 9.16. If $f \in D_n$ is a reflection, then $f^2 = e$ and $|f| = 2$. If $r := R_{2\pi/n}$ then $r^k = R_{2\pi k/n} \neq e$ for $1 \le k \le n-1$ and $r^n = 1$, so $|r| = n$ and

$$\langle r \rangle = \left\{R_{2\pi k/n} : 0 \le k \le n-1\right\} \subset D_n.$$

Example 9.17. Suppose that $G = D_n$ and $f = S_0$. Recall that $D_n = \left\{r^k, r^k f\right\}_{k=0}^{n-1}$. We wish to compute $C\left(f\right)$. We have $r^k \in C\left(f\right)$ iff $r^k f = fr^k$ iff $r^k = fr^k f = r^{-k}$. There are only two rotations R_θ for which $R_\theta = R_\theta^{-1}$, namely $R_0 = e$ and $R_{180} = -I$. The latter is in D_n only if n is even.

Let us now check to see if $r^k f \in C\left(f\right)$. This is the case iff

$$r^k = \left(r^k f\right) f = f\left(r^k f\right) = r^{-k}$$

and so again this happens iff $r = R_0$ or R_{180}. Thus we have shown,

$$C\left(f\right) = \begin{cases} \langle f \rangle = \{e, f\} & \text{if } n \text{ is odd} \\ \left\{e, r^{n/2}, f, r^{n/2} f\right\} & \text{if } n \text{ is even.} \end{cases}$$

Let us now find $C\left(r^k\right)$. In this case we have $\langle r \rangle \subset C\left(r^k\right)$ (as this is a general fact). Moreover $r^l f \in C\left(r^k\right)$ iff $\left(r^l f\right) r^k = r^k\left(r^l f\right)$ which happens iff

$$r^{l-k} = r^l r^{-k} = \left(r^l f\right) r^k f = r^{k+l},$$

i.e. iff $r^{2k} = e$. Thus we may conclude that $C\left(r^k\right) = \langle r \rangle$ unless $k = 0$ or $k = \frac{n}{2}$ and when $k = 0$ or $k = n/2$ we have $C\left(r^k\right) = D_n$. Of course the case $k = n/2$ only applies if n is even. By the way this last result is not too hard to understand as $r^0 = I$ and $r^{n/2} = -I$ where I is the 2×2 identity matrix which commutes with all matrices.

Example 9.18. For $n \ge 3$,

$$Z\left(D_n\right) = \begin{cases} \{R_0 = I\} & \text{if } n \text{ is odd.} \\ \{R_0, R_{180}\} & \text{if } n \text{ is even} \end{cases} \tag{9.2}$$

To prove this recall that $S_\alpha R_\theta S_\alpha^{-1} = R_{-\theta}$ for all α and θ. So if $S_\alpha \in Z\left(D_n\right)$ we would have $R_\theta = S_\alpha R_\theta S_\alpha^{-1} = R_{-\theta}$ for $\theta = k2\pi/n$ which is impossible. Thus $Z\left(D_n\right)$ contains no reflections. Moreover this shows that R_θ can only be in the center if $R_\theta = R_{-\theta}$, i.e. R_θ can only be R_0 or R_{180}. This completes the proof since $R_{180} \in D_n$ iff n is even.

Alternatively, observe that $Z\left(D_n\right) = C\left(f\right) \cap C\left(r\right) = C\left(\{f, r\}\right)$ since if $g \in D_n$ commutes with the generators of a group it must commute with all elements of the group. Now according to Example 9.17, we again easily see that Eq. (9.2) is correct. For example when n is even we have,

$$Z\left(D_n\right) = C\left(f\right) \cap C\left(r\right) = \left\{e, r^{n/2}, f, r^{n/2} f\right\} \cap \langle r \rangle = \left\{e, r^{n/2}\right\} = \{R_0, R_{180}\}.$$

10

Lecture 10 (1/28/2009) Midterm I.

Lecture 11 (1/30/2009)

11.1 Cyclic Groups

Definition 11.1. *We say a group, G, is a* ***cyclic group*** *if there exists $g \in G$ such that $G = \langle g \rangle$. We call such a g a* ***generator of the cyclic group*** *G.*

Example 11.2. Recall that $U(9) = \{1, 2, 4, 5, 7, 8\}$ and that

$$\langle 2 \rangle = \left\{2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 7,\ 2^5 = 5,\ 2^6 = 1\right\}$$

so that $|2| = |\langle 2 \rangle| = 6$ and $U(9)$ and 2 is a generator.

Notice that $2^2 = 4$ is not a generator, since

$$\left\langle 2^2 \right\rangle = \{1, 4, 7\} \neq U(9).$$

Example 11.3. The group $U(8) = \{1, 3, 5, 7\}$ is not cyclic since,

$$\langle 3 \rangle = \{1, 3\},\ \ \langle 5 \rangle = \{1, 5\},\ \text{ and } \langle 7 \rangle = \{1, 7\}.$$

This group may be understood by observing that $3 \cdot 5 = 15 \bmod 8 = 7$ so that

$$U(8) = \left\{3^a 5^b : a, b \in \mathbb{Z}_2\right\}.$$

Moreover, the multiplication on $U(8)$ becomes two copies of the group operation on $\mathbb{Z}_2$, i.e.

$$\left(3^a 5^b\right)\left(3^{a'} 5'\right) = 3^{a+a'} 5^{b+b'} = 3^{\left(a+a'\right) \bmod 2} 5^{\left(b+b'\right) \bmod 2}.$$

So in a sense to be made precise later, $U(8)$ is equivalent to "$\mathbb{Z}_2^2$."

Example 11.4. Here are some more examples of cyclic groups.

1. $\mathbb{Z}$ is cyclic with generators being either 1 or -1.
2. $\mathbb{Z}_n$ is cyclic with 1 being a generator since

$$\langle 1 \rangle = \{0, 1, 2 = 1 + 1, 3 = 1 + 1 + 1, \dots, n - 1\}.$$

3. Let

$$G := \left\{e^{i \frac{k}{n} 2\pi} : k \in \mathbb{Z}\right\},$$

then G is cyclic and $g := e^{i 2\pi / n}$ is a generator. Indeed, $g^k = e^{i \frac{k}{n} 2\pi}$ is equal to 1 for the first time when $k = n$.

These last two examples are essentially the same and basically this is the list of all cyclic groups. Later today we will list all of the generators of a cyclic group.

Lemma 11.5. *If $H \subset \mathbb{Z}$ is a subgroup and $a := \min H \cap \mathbb{Z}_+$, then $H = \langle a \rangle = \{ka : k \in \mathbb{Z}\}$.*

Proof. It is clear that $\langle a \rangle \subset H$. If $b \in H$, we may write it as $b = ka + r$ where $0 \leq r < a$. As $r = b - ka \in H$ and $0 \leq r < a$, we must have $r = 0$. This shows that $b \in \langle a \rangle$ and thus $H \subset \langle a \rangle$. ■

Example 11.6. If $f = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in GL_2(\mathbb{R})$, then f is reflection about the line $y = x$. In particular $f^2 = I$ and $\langle f \rangle = \{I, f\}$ and $|f| = 2$. So we can have elements of finite order inside an infinite group. In fact any element of a Dihedral subgroup of $GL_2(\mathbb{R})$ gives such an example.

Notation 11.7 *Let $n \in \mathbb{Z}_+ \cup \{\infty\}$. We will write $b \equiv a \pmod{n}$ iff $(b - a) \bmod n = 0$ or equivalently $n | (b - a)$. here we use the convention that if $n = \infty$ then $b \equiv a \pmod{n}$ iff $b = a$ and $\infty | m$ iff $m = 0$.*

Theorem 11.8 (More properties of cyclic groups). *Let $a \in G$ and $n = |a|$. Then;*

1. *$a^i = a^j$ iff $i \equiv j \pmod{n}$,*
2. *If $k | m$ then $\langle a^m \rangle \subset \left\langle a^k \right\rangle$.*
3. *$\left\langle a^k \right\rangle = \left\langle a^{\gcd(n,k)} \right\rangle$.*
4. *$\left|a^k\right| = |a| / \gcd(|a|, k)$.*
5. *$\left\langle a^i \right\rangle = \left\langle a^j \right\rangle$ iff $\gcd(i, n) = \gcd(j, n)$*
6. *$\left\langle a^k \right\rangle = \langle a \rangle$ iff $\gcd(k, n) = 1$.*

Proof. 1. We have $a^i = a^j$ iff

$$e = a^{i-j} = a^{(i-j) \bmod n}$$

which happens iff $(i - j) \bmod n = 0$ by Theorem 8.12.

2. If $m = lk$, then $(a^m)^q = \left(a^{lk}\right)^q = \left(a^k\right)^{lq}$, and therefore $\langle a^m \rangle \subset \left\langle a^k \right\rangle$.

3. Let $d := \gcd(n, k)$, then $d|k$ and therefore $\left\langle a^k \right\rangle \subset \left\langle a^d \right\rangle$. For the opposite inclusion we must show $a^d \in \left\langle a^k \right\rangle$. To this end, choose $s, t \in \mathbb{Z}$ such that $d = sk + tn$. It then follows that

$$a^d = a^{sk}a^{tn} = \left(a^k\right)^s \in \left\langle a^k \right\rangle$$

as desired.

4. Again let $d := \gcd(n, k)$ and set $m := n/d \in \mathbb{N}$. Then $\left(a^d\right)^k = a^{dk} \neq e$ for $1 \leq k < m$ and $a^{dm} = a^n = e$. Hence we may conclude that $\left|a^d\right| = m = n/d$. Combining this with item 3. show,

$$\left|a^k\right| = \left|\left\langle a^k \right\rangle\right| = \left|\left\langle a^d \right\rangle\right| = \left|a^d\right| = n/d = |a| / \gcd(k, |a|).$$

5. By item 4., if $\gcd(i, n) = \gcd(j, n)$ then

$$\left\langle a^i \right\rangle = \left\langle a^{\gcd(i,n)} \right\rangle = \left\langle a^{\gcd(j,n)} \right\rangle = \left\langle a^j \right\rangle.$$

Conversely if $\left\langle a^i \right\rangle = \left\langle a^j \right\rangle$ then by item 4.,

$$\frac{n}{\gcd(i, n)} = \left|\left\langle a^i \right\rangle\right| = \left|\left\langle a^j \right\rangle\right| = \frac{n}{\gcd(j, n)}$$

from which it follows that $\gcd(i, n) = \gcd(j, n)$.

6. This follows directly from item 3. or item 5. ■

Example 11.9. Let use Theorem 11.8 to find all generators of $Z_{10} = \{0, 1, 2, \ldots, 9\}$. Since 1 is a generator it follow by item 6. of the previous theorem that the generators of Z_{10} are precisely those $k \geq 1$ such that $\gcd(k, 10) = 1$. (Recall we use the additive notation here so that a^k becomes ka.) In other words the generators of Z_{10} is precisely

$$U(10) = \{1, 3, 7, 9\}$$

of which their are $\varphi(10) = \varphi(5 \cdot 2) = (5 - 1)(2 - 1) = 4$.

More generally the generators of Z_n are the elements in $U(n)$. It is in fact easy to see that every $a \in U(n)$ is a generator. Indeed, let $b := a^{-1} \in U(n)$, then we have

$$\mathbb{Z}_n = \langle 1 \rangle = \langle (b \cdot a) \bmod n \rangle = \langle b \cdot a \rangle \subset \langle a \rangle \subset \mathbb{Z}_n.$$

Conversely if and $a \in [\mathbb{Z}_n \setminus U(n)]$, then $\gcd(a, n) = d > 1$ and therefore $\gcd(a/d, n) = 1$ and $a/d \in U(n)$. Thus a/d generates $\mathbb{Z}_n$ and therefore $|a| = n/d$ and hence $|\langle a \rangle| = n/d$ and $\langle a \rangle \neq \mathbb{Z}_n$.

12

Lecture 12 (2/2/2009)

Theorem 12.1 (Fundamental Theorem of Cyclic Groups). *Suppose that $G = \langle a \rangle$ is a cyclic group and H is a sub-group of G, and*

$$m := m(H) = \min \left\{ k \geq 1 : a^k \in H \right\}. \tag{12.1}$$

Then:

1. *$H = \langle a^m \rangle$ – so all subgroups of G are of the form $\langle a^m \rangle$ for some $m \geq 1$.*
2. *If $n = |a| < \infty$, then $m|n$ and $|H| = n/m$.*
3. *To each divisor, $k \geq 1$, of n there is precisely one subgroup of G of order k, namely $H = \left\langle a^{n/k} \right\rangle$.*

In short, if $G = \langle a \rangle$ with $|a| = n$, then

$$\begin{array}{ccc} \{\textit{Positive divisors of } n\} & \longleftrightarrow & \{\textit{sub-groups of } G\} \\ m & \rightarrow & \langle a^m \rangle \\ m(H) & \leftarrow & H \end{array}$$

is a one to one correspondence. These subgroups may be indexed by their order, $k = |\langle a^m \rangle| = n/m$.

Proof. We prove each point in turn.

1. Suppose that $H \subset G$ is a sub-group and m is defined as in Eq. (12.1). Since $a^m \in H$ and H is closed under the group operations it follows that $\langle a^m \rangle \subset H$. So we must show $H \subset \langle a^m \rangle$. If $a^l \in H$ with $l \in \mathbb{Z}$, we write $l = jm + r$ with $r := l \bmod m$. Then $a^l = a^{mj} a^r$ and hence $a^r = a^l (a^m)^{-j} \in H$. As $0 \leq r < m$, it follows from the definition of m that $r = 0$ and therefore $a^l = a^{jm} = (a^m)^j \in \langle a^m \rangle$. Thus we have shown $H \subset \langle a^m \rangle$ and therefore that $H = \langle a^m \rangle$.
2. From Theorem 11.8 we know that $H = \langle a^m \rangle = \left\langle a^{\gcd(m,n)} \right\rangle$ and that $|H| = n/\gcd(m,n)$. Using the definition of m, we must have $m \leq \gcd(m,n)$ which can only happen if $m = \gcd(m,n)$. This shows that $m|n$ and $|H| = n/m$.
3. From what we have just shown, the subgroups, $H \subset G$, are precisely of the form $\langle a^m \rangle$ where m is a divisor of n. Moreover we have shown that $|\langle a^m \rangle| = n/m =: k$. Thus for each divisor k of n, there is exactly one subgroup of G of order k, namely $\langle a^m \rangle$ where $m = n/k$.

■

Example 12.2. Let $G = \mathbb{Z}_{20}$. Since $20 = 2^2 \cdot 5$ it has divisors, $k = 1$, 2, 4, 5, 10, 20. The subgroups having these orders are,

Order		
1	$\langle 0 \rangle = \left\langle \frac{20}{1} \cdot 1 \right\rangle$	$= \{0\}$
2	$\langle 10 \rangle = \left\langle \frac{20}{2} \cdot 1 \right\rangle$	$= \{0, 10\}$
4	$\langle 5 \rangle = \left\langle \frac{20}{4} \cdot 1 \right\rangle$	$= \{0, 5, 10, 15\}$
5	$\langle 4 \rangle = \left\langle \frac{20}{5} \cdot 1 \right\rangle$	$= \{0, 4, 8, 12, 16, 20\}$
10	$\langle 2 \rangle = \left\langle \frac{20}{10} \cdot 1 \right\rangle$	$= \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20\}$
20	$\langle 1 \rangle = \left\langle \frac{20}{20} \cdot 1 \right\rangle$	$= \mathbb{Z}_{20}$

Corollary 12.3. *Suppose G is a cyclic group of order n with generator g, d is a divisor of n, and $a = g^{n/d}$. Then*

$$\{\textit{elements of order } d \textit{ in } G\} = \left\{ a^k : k \in U(d) \right\}$$

and in particular G contains exactly $\varphi(d)$ elements of order d. It should be noted that $\left\{ a^k : k \in U(d) \right\}$ is also the list of all the elements of G which generate the unique cyclic subgroup of order d.

Proof. We know that $a := g^{n/d}$ is the generator of the unique (cyclic) subgroup, $H \leq G$, of order d. This subgroup must contain all of the elements of order d for if not there would be another distinct cyclic subgroup of order d in G. The elements of H which have order d are precisely of the form a^k with $1 \leq k < d$ and $\gcd(k, d) = 1$, i.e. with $k \in U(d)$. As there are $\varphi(d)$ such elements the proof is complete. ■

Example 12.4. Let us find all the elements of order 10 in $\mathbb{Z}_{20}$. Since $|2| = 10$, we know from Corollary 12.3 that

$$\{2k : k \in U(10)\} = \{2k : k = 1, 3, 7, 9\} = \{2, 6, 14, 18\}$$

are precisely the elements of order 10 in $\mathbb{Z}_{20}$.

Corollary 12.5. *The Euler Phi – function satisfies, $n = \sum_{1 \leq d : d|n} \varphi(d)$.*

Proof. Every element of $\mathbb{Z}_n$ has a unique order, d, which divides n and therefore,

$$n = \sum_{1 \le d : d|n} \# \{k \in \mathbb{Z}_n : |k| = d\} = \sum_{1 \le d : d|n} \varphi(d).$$

■

Example 12.6. Let us test this out for $n = 20$. In this case we should have,

$$\begin{aligned} 20 &\overset{?}{=} \varphi(1) + \varphi(2) + \varphi(4) + \varphi(5) + \varphi(10) + \varphi(20) \\ &= 1 + 1 + 2 + 4 + 4 + \left(2^2 - 2\right)(5 - 1) \\ &= 1 + 1 + 2 + 4 + 4 + 8 = 20. \end{aligned}$$

Remark 12.7. In principle it is possible to use Corollary 12.5 to compute φ. For example using this corollary and the fact that $\varphi(1) = 1$, we find for distinct primes p and q that,

$$\begin{aligned} p &= \varphi(1) + \varphi(p) = 1 + \varphi(p) \implies \varphi(p) = p - 1, \\ p^2 &= \varphi(1) + \varphi(p) + \varphi\left(p^2\right) = p + \varphi\left(p^2\right) \implies \varphi(p) = p^2 - p \\ pq &= \varphi(1) + \varphi(p) + \varphi(q) + \varphi(pq) = p + q - 1 + \varphi(pq) \end{aligned}$$

which then implies,

$$\varphi(pq) = pq - p - q + 1 = (p - 1)(q - 1).$$

Similarly,

$$\begin{aligned} p^2 q &= \varphi(1) + \varphi(p) + \varphi(q) + \varphi(pq) + \varphi\left(p^2\right) + \varphi\left(p^2 q\right) \\ &= pq + \left(p^2 - p\right) + \varphi\left(p^2 q\right) \end{aligned}$$

and hence,

$$\begin{aligned} \varphi\left(p^2 q\right) &= p^2 q - pq - \left(p^2 - 1\right) = p^2 q - p^2 - pq + p \\ &= p(pq - p - q + 1) = p(p - 1)(q - 1). \end{aligned}$$

Theorem 12.8. *Suppose that G is any finite group and $d \in \mathbb{Z}_+$, then the number elements of order d in G is divisible by $\varphi(d)$.*

Proof. Let

$$G_d := \{g \in G : |g| = d\}.$$

If $G_d = \emptyset$, the statement of the theorem is true since $\varphi(d)$ divides $0 = \#(G_d)$.

If $a \in G_d$, then $\langle a \rangle$ is a cyclic subgroup of order d with precisely $\varphi(d)$ element of order d. If $G_d \setminus \langle a \rangle = \emptyset$ we are done since there are precisely $\varphi(d)$ elements of order d in G. If not, choose $b \in G_d \setminus \langle a \rangle$. Then the elements of order d in $\langle b \rangle$ must be distinct from the elements of order d in $\langle a \rangle$ for otherwise $\langle a \rangle = \langle b \rangle$, but $b \notin \langle a \rangle$. If $G_d \setminus (\langle a \rangle \cup \langle b \rangle) = \emptyset$ we are again done since now $\#(G_d) = 2\varphi(d)$ will be the number of elements of order d in G. If $G_d \setminus (\langle a \rangle \cup \langle b \rangle) \neq \emptyset$ we choose a third element, $c \in G_d \setminus (\langle a \rangle \cup \langle b \rangle)$ and argue as above that $\#(G_d) = 3\varphi(d)$ if $G_d \setminus (\langle a \rangle \cup \langle b \rangle \cup \langle c \rangle) = \emptyset$. Continuing on this way, the process will eventually terminate since $\#(G_d) < \infty$ and we will have shown that $\#(G_d) = n\varphi(d)$ for some $n \in \mathbb{N}$. ■

Example 12.9 (Exercise 4.20). Suppose that G is an Abelian group, $|G| = 35$, and every element of G satisfies $x^{35} = e$. Prove that G is cyclic. Since $x^{35} = e$, we have seen in Corollary 9.1 that $|x|$ must divide $35 = 5 \cdot 7$. Thus every element in G has order either, 1, 5, 7, or 35. If there is an element of order 35, G is cyclic and we are done. Since the only element of order 1 is e, there are 34 elements of either order 5 or 7. As $\varphi(5) = 4$ and $\varphi(7) = 6$ do not divide 35, there must exists $a, b \in G$ such that $|a| = 5$ and $|b| = 7$. We now let $x := ab$ and claim that $|x| = 35$ which is a contradiction. To see that $|x| = 35$ observe that $|x| > 1$, $x^5 = a^5 b^5 = eb^5 \neq e$ so $|x| \neq 5$ and $x^7 = a^7 b^7 = a^2 \neq e$ so that $|x| \neq 7$. Therefore $|x| = 35$ and we are done.

Alternatively, for this last part. Notice that $x^n = a^n b^n = e$ iff $a^n = b^{-n}$. If $a^n = b^{-n} \neq e$, then $|a^n| = 5$ while $|b^{-n}| = 7$ which is impossible. Thus the only way that $a^n b^n = e$ is if $a^n = e = b^n$. Thus we must $5|n$ and $7|n$ and therefore $35|n$ and therefore $|x| = 35$.

Lecture 13 (2/4/2009)

The **least common multiple**, $\operatorname{lcm}(a_1,\dots,a_k)$, of k integers, $a_1,\dots,a_k\in\mathbb{Z}_+$, is the smallest integer $n\ge 1$ which is a multiple of each a_i for $i=1,\dots,k$.

For example,

$$\operatorname{lcm}(10,14,15)=\operatorname{lcm}(2\cdot 5,2\cdot 7,3\cdot 5)=2\cdot 3\cdot 5\cdot 7=210$$

Corollary 13.1. *Let $a_1,\dots,a_k\in\mathbb{Z}_+$, then*

$$\langle a_1\rangle\cap\dots\cap\langle a_k\rangle=\langle\operatorname{lcm}(a_1,\dots,a_k)\rangle\subset\mathbb{Z}.$$

Moreover, $m\in\mathbb{Z}$ is a common multiple of $a_1,\dots,a_k$ iff m is a multiple of $\operatorname{lcm}(a_1,\dots,a_k)$.

Proof. First observe that

$$\{\text{common multiples of } a_1,\dots,a_k\}=\langle a_1\rangle\cap\dots\cap\langle a_k\rangle$$

which is a sub-group of $\mathbb{Z}$ and therefore by Lemma 11.5,

$$\{\text{common multiples of } a_1,\dots,a_k\}=\langle n\rangle$$

where

$$n=\min\{\text{common multiples of } a_1,\dots,a_k\}\cap\mathbb{Z}_+=\operatorname{lcm}(a_1,\dots,a_k).$$

■

Corollary 13.2. *Let $a_1,\dots,a_k\in\mathbb{Z}_+$, then*

$$\operatorname{lcm}(a_1,\dots,a_k)=\operatorname{lcm}(a_1,\operatorname{lcm}(a_1,\dots,a_k)).$$

Proof. This follows from the following sequence of identities,

$$\begin{aligned}\langle\operatorname{lcm}(a_1,\dots,a_k)\rangle&=\langle a_1\rangle\cap\dots\cap\langle a_k\rangle=\langle a_1\rangle\cap(\langle a_2\rangle\cap\dots\cap\langle a_k\rangle)\\&=\langle a_1\rangle\cap\langle\operatorname{lcm}(a_1,\dots,a_k)\rangle=\langle\operatorname{lcm}(a_1,\operatorname{lcm}(a_1,\dots,a_k))\rangle.\end{aligned}$$

■

Proposition 13.3. *Suppose that G is a group and a and b are two finite order commuting elements of a group G such that*[1] $\langle a\rangle\cap\langle b\rangle=\{e\}$. *Then $|ab|=\operatorname{lcm}(|a|,|b|)$.*

Proof. If $e=(ab)^m=a^m b^m$ for some $m\in\mathbb{Z}$ then

$$\langle a\rangle\ni a^m=b^{-m}\in\langle b\rangle$$

from which it follows that $a^m=b^{-m}\in\langle a\rangle\cap\langle b\rangle=\{e\}$, i.e. $a^m=e=b^m$. This happens iff m is a common multiple of $|a|$ and $|b|$ and therefore the order of ab is the smallest such multiple, i.e. $|ab|=\operatorname{lcm}(|a|,|b|)$. ■

It is not possible to drop the assumption that $\langle a\rangle\cap\langle b\rangle=\{e\}$ in the previous proposition. For example consider $a=2$ and $b=6$ in $\mathbb{Z}_8$, so that $|a|=4$, $|6|=8/\gcd(6,8)=4$, and $\operatorname{lcm}(4,4)=4$, while $a+b=0$ and $|0|=1$. More generally if $b=a^{-1}$ then $|ab|=1$ while $|a|=|b|$ can be anything. In this case, $\langle a\rangle\cap\langle b\rangle=\langle a\rangle$.

13.1 Cosets and Lagrange's Theorem (Chapter 7 of the book)

Let G be a group and H be a non-empty subset of G. Soon we will assume that H is a subgroup of G.

Definition 13.4. *Given $a\in G$, let*

1. *$aH:=\{ah:h\in H\}$ – called the **left coset of** H **in** G **containing** a when $H\le G$,*
2. *$Ha:=\{ha:h\in H\}$ – called the **right coset of** H **in** G **containing** a when $H\le G$, and*
3. *$aHa^{-1}:=\left\{aha^{-1}:h\in H\right\}$.*

Definition 13.5. *If $H\le G$, we let*

$$G/H:=\{aH:a\in G\}$$

[1] You showed in Exercise 4.54 of homework 4, that if $|a|$ and $|b|$ are relatively prime, then $\langle a\rangle\cap\langle b\rangle=\{e\}$ holds automatically.

be the set of left cosets of H in G. The ***index*** *of H in G is $|G:H| := \#(G/H)$, that is*

$$|G:H| = \#(G/H) = (\textit{the number of distinct cosets of } H \textit{ in } G).$$

Example 13.6. Suppose that $G = GL(2,\mathbb{R})$ and $H := SL(2,\mathbb{R})$. In this case for $A \in G$ we have,

$$AH = \{AB : B \in H\} = \{C : \det C = \det A\}.$$

Each coset of H in G is determined by value of the determinant on that coset. As G/H may be indexed by $\mathbb{R}\setminus\{0\}$, it follows that

$$|GL(2,\mathbb{R}) : SL(2,\mathbb{R})| = \#(\mathbb{R}\setminus\{0\}) = \infty.$$

Example 13.7. Let $G = U(20) = U(2^2 \cdot 5) = \{1,3,7,9,11,13,17,19\}$ and take

$$H := \langle 3 \rangle = \{1,3,9,7\}$$

in which case,

$$\begin{aligned} 1H &= 3H = 9H = 7H = H, \\ 11H &= \{11,13,19,17\} = 13H = 17H = 19H. \end{aligned}$$

We have $|G:H| = 2$ and

$$|G:H| \times |H| = 2 \times 4 = 8 = |G|.$$

Example 13.8. Let $G = \mathbb{Z}_9$ and $H = \langle 3 \rangle = \{0,3,6\}$. In this case we use additive notation,

$$\begin{aligned} 0 + H &= 3 + H = 6 + H = H \\ 1 + H &= \{1,4,7\} = 4 + H = 7 + H \\ 2 + H &= \{2,5,8\} = 2 + H = 8 + H \end{aligned}$$

We have $|G:H| = 3$ and

$$|G:H| \times |H| = 3 \times 3 = 9 = |G|.$$

Example 13.9. Suppose that $G = D_4 := \{r^k, r^k f\}_{k=0}^3$ with $r^4 = 1$, $f^2 = 1$, and $frf = r^{-1}$. If we take $H = \langle f \rangle = \{1, f\}$ then

$$r^k H = \{r^k, r^k f\} = \{r^k f, r^k f f\} = r^k f H \text{ for } k = 0,1,2,3.$$

In this case we have $|G:H| = 4$ and

$$|G:H| \times |H| = 4 \times 2 = 8 = |G|$$

Recall that we have seen if G is a finite cyclic group and $H \le G$, then $|H|$ divides G. This along with the last three examples suggests the following theorem of Lagrange. They also motivate Lemma 14.2 below.

Theorem 13.10 (Lagrange's Theorem). *Suppose that G is a finite group and $H \le G$, then $|H|$ divides $|G|$ and $|G|/|H|$ is the number of distinct cosets of H in G, i.e.*

$$|G:H| \times |H| = |G|.$$

Corollary 13.11. *If G is a group of prime order p, then G is cyclic and every element in $G \setminus \{e\}$ is a generator of G.*

Proof. Let $g \in G \setminus \{e\}$ and take $H := \langle g \rangle$. Then $|H| > 1$ and $|H| \mid |G| = p$ implies $|H| = p$. Thus it follows that $H = G$, i.e. $G = \langle g \rangle$. ■

Before proving Theorem 13.10, we will pause for some basic facts about the cosets of H in G.

14

Lecture 14 (2/6/2009)

Suppose that $f : X \to Y$ is a bijection (f being one to one is actually enough here). Then if A, B are subsets of X, we have

$$A = B \iff f(A) = f(B),$$

where $f(A) = \{f(a) : a \in A\} \subset Y$. Indeed, it is clear that $A = B \implies f(A) = f(B)$. For the opposite implication, let $g : Y \to X$ be the inverse function to f, then $f(A) = f(B) \implies g(f(A)) = g(f(B))$. But $g(f(A)) = \{a = g(f(a)) : a \in A\} = A$ and $g(f(B)) = B$.

Let us also observe that if f is one to one and $A \subset X$ is a finite set with n elements, then $\#(f(A)) = n = \#(A)$. Indeed if $\{a_1, \dots, a_n\}$ are the distinct elements of A then $\{f(a_1), \dots, f(a_n)\}$ are the distinct elements of $f(A)$.

Lemma 14.1. *For any $a \in G$, the maps $L_a : G \to G$ and $R_a : G \to G$ defined by $L_a(x) = ax$ and $R_a(x) = xa$ are bijections.*

Proof. We only prove the assertions about L_a as the proofs for R_a are analogous. Suppose that $x, y \in G$ are such that $L_a(x) = L_a(y)$, i.e. $ax = ay$, it then follows by cancellation that $x = y$. Therefore L_a is one to one. It is onto since if $x \in G$, then $L_a\left(a^{-1}x\right) = x$.

Alternatively. Simply observe that $L_{a^{-1}} : G \to G$ is the inverse map to L_a. ■

Lemma 14.2. *Let G be a group, $H \leq G$, and $a, b \in H$. Then*

1. *$a \in aH$,*
2. *$aH = H$ iff $a \in H$.*
3. *If $a \in G$ and $b \in aH$, then $aH = bH$.*
4. *If $aH \cap bH \neq \emptyset$ then $aH = bH$. So either $aH = bH$ or $aH \cap bH = \emptyset$.*
5. *$aH = bH$ iff $a^{-1}b \in H$.*
6. *G is the disjoint union of its **distinct** cosets.*
7. *$aH = Ha$ iff $aHa^{-1} = H$.*
8. *$|aH| = |H| = |bH|$ where $|aH|$ denotes the number of element in aH.*
9. *aH is a subgroup of G iff $a \in H$.*

Proof. For the most part we refer the reader to p. 138-139 of the book for the details of the proof. Let me just make a few comments.

1. Since $e \in H$ we have $a = ae \in aH$.
2. If $aH = H$, then $a = ae \in aH = H$. Conversely, if $a \in H$, then $aH \subset H$ since H is a group. For the opposite inclusion, if if $h \in H$, then $h = a\left(a^{-1}h\right) \in aH$, i.e. $H \subset aH$. **Alternatively:** as above it follows that $a^{-1}H \subset H$ and therefore, $H = a\left(a^{-1}H\right) \subset aH$.
3. If $b \in ah' \in aH$, then $bH = ah'H = aH$.
4. If $ah = bh' \in aH \cap bH$, then $b = ah\, h'^{-1} \in aH$ and therefore $bH = aH$.
5. If $a^{-1}b \in H$ then $a^{-1}b = h \in H$ and $b = ah$ and hence $aH = bH$. Conversely if $aH = bH$ then $b = be = ah$ for some for some $h \in H$. Therefore, $a^{-1}b = h \in H$.
6. See item 1 shows G is the union of its cosets and item 4. shows the distinct cosets are disjoint.
7. We have $aH = Ha \iff H = (Ha)a^{-1} = (aH)a^{-1} = aHa^{-1}$.
8. Since L_a and L_b are bijections, it follows that $|aH| = \#(L_a(H)) = \#(H)$. Similarly, $|bH| = |H|$.
9. $e \in aH$ iff $a \in H$.

■

Remark 14.3. Much of Lemma 14.2 may be understood with the aid of the following equivalence relation. Namely, write $a \sim b$ iff $a^{-1}b \in H$. Observe that $a \sim a$ since $a^{-1}a = e \in H$, $a \sim b \implies b \sim a$ since $a^{-1}b \in H \implies b^{-1}a = \left(a^{-1}b\right)^{-1} \in H$, and $a \sim b$ and $b \sim c$ implies $a \sim c$ since $a^{-1}b \in H$ and

$$b^{-1}c \in H \implies a^{-1}c = a^{-1}bb^{-1}c \in H.$$

The equivalence class, $[a]$, containing a is then

$$[a] = \{b : a \sim b\} = \left\{b : h := a^{-1}b \in H\right\} = \{ah : h \in H\} = aH.$$

Definition 14.4. *A subgroup, $H \leq G$, is said to be **normal** if $aHa^{-1} = H$ for all $a \in G$ or equivalently put, $aH = Ha$ for all $a \in G$. We write $H \lhd G$ to mean that H is a normal subgroup of G.*

We will prove later the following theorem. (If you want you can go ahead and try to prove this theorem yourself.)

Theorem 14.5 (Quotient Groups). *If $H \lhd G$, the set of left cosets, G/H, becomes a group under the multiplication rule,*

$$aH \cdot bH := (ab)\,H \text{ for all } a, b \in H.$$

In this group, eH is the identity and $(aH)^{-1} = a^{-1}H$.

We are now ready to prove Lagrange's theorem which we restate here.

Theorem 14.6 (Lagrange's Theorem). *Suppose that G is a finite group and $H \leq G$, then*

$$|G : H| \times |H| = |G|,$$

where $|G : H| := \#(G/H)$ is the number of ***distinct*** *cosets of H in G. In particular $|H|$ divides $|G|$ and $|G| / |H| = |G : H|$.*

Proof. Let $n := |G : H|$ and choose $a_i \in G$ for $i = 1, 2, \dots, n$ such that $\{a_i H\}_{i=1}^n$ is the collection of distinct cosets of H in G. Then by item 6. of Lemma 14.2 we know that

$$G = \cup_{i=1}^n [a_i H] \text{ with } a_i H \cap a_j H = \emptyset \text{ for all } i \neq j.$$

Thus we may conclude, using item 8. of Lemma 14.2 that

$$|G| = \sum_{i=1}^n |a_i H| = \sum_{i=1}^n |H| = n \cdot H = |G : H| \cdot |H|.$$

■

Remark 14.7 (Becareful!). Despite the next two results, it is **not** true that all groups satisfy the converse to Lagrange's theorem. That is there exists groups G for which there is a divisor, d, of $|G|$ for which there is no subgroup, $H \leq G$ with $|H| = d$. We will eventually see that $G = A_4$ is a group of order 12 with no subgroups of order 6. Here, A_4, is the so called alternating group on four letters.

Lemma 14.8. *If H and K satisfy the converse to Lagrange's theorem, then so does $H \times K$. In particular, every finite abelian group satisfies the converse to Lagrange's theorem.*

Proof. Let $m := |H|$ and $n = |K|$. If $d|mn$, then we may write $d = d_1 d_2$ with $d_1|m$ and $d_2|n$. We may now choose subgroups, $H' \leq H$ and $K' \leq K$ such that $|H'| = d_1$ and $|K'| = d_2$. It then follows that $H' \times K' \leq H \times K$ with $|H' \times K'| = d_1 d_2 = d$.

The second assertion follows from the fact that all finite abelian groups are isomorphic to a product of cyclic groups and we already know the converse to Lagrange's theorem holds for these groups. ■

Example 14.9. Consider $G = D_n = \left\langle r, f : r^n = e = f^2 \text{ and } frf = r^{-1} \right\rangle$. The divisors of $2n$ are the divisors, Λ of n and 2Λ. If $d \in \Lambda$, let $H := \left\langle r^{n/d} \right\rangle$ to construct a group of order d. To construct a group of order $2d$, take,

$$H = \left\langle r^{n/d} \right\rangle f \cup \left\langle r^{n/d} \right\rangle.$$

Notice that this is subgroup of G since,

$$\begin{aligned} \left(r^{kn/d} f\right) \left(r^{ln/d} f\right) &= r^{kn/d} r^{ln/d} f f = r^{(k-l)n/d} \\ \left(r^{kn/d} f\right) r^{ln/d} &= r^{(k-l)n/d} f \\ r^{ln/d} r^{kn/d} f &= r^{(k+l)n/d} f. \end{aligned}$$

This shows that D_n satisfies the converse to Lagrange's theorem.

Example 14.10. Let $G = U(30) = U(2 \cdot 3 \cdot 5) = \{1, 7, 11, 13, 17, 19, 23, 29\}$ and $H = \langle 11 \rangle = \{1, 11\}$. In this case we know $|G : H| = |G| / |H| = 8/2 = 4$, i.e. there are 4 distinct cosets which we now find.

$$\begin{aligned} 1H &= H = \{1, 11\} \\ 7H &= \{7, 17\} \\ 13H &= \{13, 13 \cdot 11 \bmod 30 = 23\} \\ 19H &= \{19, 19 \cdot 11 \bmod 30 = 29\}. \end{aligned}$$

Notice that

$$19 \cdot 11 = -11^2 \bmod 30 = -121 \bmod 30 = -1 \bmod 30 = 29.$$

Corollary 14.11. *If G is a finite group and $g \in G$, then $|g|$ divides $|G|$, i.e.*

Proof. Let $H := \langle g \rangle$, then $|H| = |g|$ and $|G : H| \cdot |g| = |G|$. ■

Corollary 14.12. *If G is a finite group and $g \in G$, then $g^{|G|} = e$.*

Proof. By the previous corollary, we know that $|G| = |g|\,n$ where $n := |G : \langle g \rangle|$. Therefore $g^{|G|} = g^{|g|n} = \left(g^{|g|}\right)^n = e^n = e$. ■

Corollary 14.13 (Fermat's Little Theorem). *Let p be a prime number and $a \in \mathbb{Z}$. Then*

$$a^p \bmod p = a \bmod p. \tag{14.1}$$

Proof. Let $r := a \bmod p \in \{0, 1, 2, \dots, p-1\}$. Since

$$a^p \bmod p = (a \bmod p)^p \bmod p = r^p \bmod p$$

it suffices to show

$$r^p \bmod p = r \text{ for all } r \in \{0, 1, 2, \ldots, p-1\}.$$

As this latter equation is true when $r = 0$ we may now assume that $r \in U(p) = \{1, 2, \ldots, p-1\}$. The previous equation is then equivalent to $r^p = r$ in $U(p)$ which is equivalent to $r^{p-1} = 1$ in $U(p)$. However this last assertion is true by Corollary 14.12 and the fact that $|U(p)| = p - 1$. ■

15

Lecture 15 (2/9/2009)

Example 15.1. Consider

$$32 \bmod 5 = 2^5 \bmod 5 = 2 \bmod 5 = 2.$$

Example 15.2. Let us now show that 35 is not prime by showing

$$2^{35} \bmod 35 \neq 2 \bmod 35 = 2.$$

To do this we have

$$\begin{aligned} 2 \bmod 35 &= 2 \\ 2^2 \bmod 35 &= 4 \\ 2^4 \bmod 35 &= \left(2^2 \bmod 35\right)^2 \bmod 35 = 4^2 \bmod 35 = 16 \\ 2^8 \bmod 35 &= \left(2^4 \bmod 35\right)^2 \bmod 35 = (16)^2 \bmod 35 = 256 \bmod 35 = 11 \\ 2^{16} \bmod 35 &= (11)^2 \bmod 35 = 121 \bmod 35 = 16 \\ 2^{32} \bmod 35 &= (16)^2 \bmod 35 = 11 \end{aligned}$$

and therefore,

$$2^{35} \bmod 35 = \left(2^3 \bmod 35 \cdot 2^{32} \bmod 35\right) \bmod 35 = 88 \bmod 35 = 18 \neq 2.$$

Therefore 35 is not prime!

Example 15.3 (Primality Test). Suppose that $n \in \mathbb{Z}_+$ is a large number we wish to see if it is prime or not. Hard to do in general. Here are some tests to perform on n. Pick a few small primes, p, like $\{2, 3, 5, 7\}$ less than n:

1. compute $\gcd(p, n)$. If $\gcd(p, n) = p$ we know that $p|n$ and hence n is not prime.
2. If $\gcd(p, n) = 1$, compute $p^n \bmod n$ (as above). If $p^n \bmod n \neq p$, then n is again not prime.
3. If we have $p^n \bmod n = p = \gcd(p, n)$ for p from our list, the test has failed to show n is not prime. We can test some more by adding some more primes to our list.

Remark: This is not a fool proof test. There are composite numbers n such that $a^n \bmod n = a \bmod n$ for a. These numbers are called pseudoprimes and $n = 561 = 3 \times 11 \times 17$ is one of them. See for example:

http : //en.wikipedia.org/wiki/Fermat_primality_test
and
http : //en.wikipedia.org/wiki/Pseudoprime

Example 15.4 (Exercise 7.16.). The same proof shows that if $n \in \mathbb{Z}_+$ and $a \in \mathbb{Z}$ is relatively prime to n, then

$$a^{\varphi(n)} \bmod n = 1.$$

Indeed, we have $a^{\varphi(n)} \bmod n = r^{\varphi(n)} \bmod n$ where $r := a \bmod n$ and we have seen that $\gcd(r, n) = \gcd(a, n) = 1$ so that $r \in U(n)$. Since $\varphi(n) = |U(n)|$ we may conclude that $r^{\varphi(n)} = 1$ in $U(n)$, i.e.

$$a^{\varphi(n)} \bmod n = r^{\varphi(n)} \bmod n = 1.$$

Theorem 15.5. *Suppose G is a group of order $p \geq 3$ which is prime. Then G is isomorphic to $\mathbb{Z}_{2p}$ or D_p.*

Before giving the proof let us first prove a couple of lemmas.

Lemma 15.6. *If G is a group such that $a^2 = e$ for all $a \in G$, then G is abelian.*

Proof. Since $a^2 = e$ we know that $a = a^{-1}$ for all $a \in G$. So for any $a, b \in G$ it follows that

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba,$$

i.e. G must be abelian. ■

Lemma 15.7. *If G is a group having two distinct commuting elements, a and b, with $|a| = 2 = |b|$, then $H := \{e, a, b, ab\}$ is a sub-group of order 4.*

Proof. By cancellation ab is not equal to a or b. Moreover if $ab = e$, then $a = b^{-1} = b$ which again is not allowed by assumption. Therefore H has four elements. It is easy to see that $H \leq G$. ■

We are now ready for the proof of Theorem 15.5.

Proof. Proof of Theorem 15.5.

Case 1. There is an element, $g \in G$ of order $2p$. In this case $G = \langle g \rangle \cong \mathbb{Z}_{2p}$ and we are done.

Case 2. $|g| \leq p$ for all $g \in G$. In this case we must have at least one element, $a \in G$, such that $|a| = p$. Otherwise we would have (by Lagrange's theorem) $|g| \leq 2$ for all $g \in G$. However, by Lemmas 15.6 and 15.7 this would imply that G contains a subgroup, H, of order 4 which is impossible because of Lagrange's theorem.

Let $a \in G$ with $|a| = p$ and set

$$H := \langle a \rangle = \left\{ e, a, a^2, \dots, a^{p-1} \right\}.$$

As $[G : H] = |G| / |H| = 2p/p = 2$, there are two distinct disjoint cosets of H in G. So if b is **any** element in $G \setminus H$ the two distinct cosets are H and

$$bH = b \langle a \rangle = \left\{ b, ba, ba^2, \dots, ba^{p-1} \right\}.$$

We are now going to show that $b^2 = e$ for all $b \in G \setminus H$. What we know is that $b^2 H$ is either H or bH. If $b^2 H = bH$ then $b = b^{-1} b^2 \in H$ which contradicts the assumption that $b \notin H$. Therefore we must have $b^2 H = H$, i.e. $b^2 \in H$. If $b^2 \neq e$, then $b^2 = a^l$ for some $1 \leq l < p$ and therefore $\left| b^2 \right| = \left| a^l \right| = p / \gcd(l, p) = p$ and therefore $|b| = 2p$. However, we are in case 2 where it is assumed that $|g| \leq p$ for all $g \in G$ so this can not happen. Therefore we may conclude that $b^2 = e$ for all $b \notin H$.

Let us now fix some $b \notin H = \langle a \rangle$. Then $ba \notin H$ and therefore we know $(ba)^2 = e$ which is to say $ba = (ba)^{-1} = a^{-1} b^{-1}$, i.e. $bab^{-1} = a^{-1}$. Therefore

$$G = H \cup bH = \left\{ a^k, ba^k : 0 \leq k < n \right\} \text{ with } a^p = e, \; b^2 = e, \text{ and } bab = a^{-1}.$$

But his is precisely our description of D_p. Indeed, recall that for $n \geq 3$,

$$D_n = \left\{ r^k, fr^k : 0 \leq k < n \right\} \text{ with } f^2 = e, \; r^n = e, \text{ and } frf = r^{-1}.$$

Thus we may map $G \to D_{2p}$ via, $a^k \to r^k$ and $ba^k \to br^k$. This map is an "**isomorphism**" of groups – a notion we discuss next. ■

15.1 Homomorphisms and Isomorphisms

Definition 15.8. *Let G and $\bar{G}$ be two groups. A function, $\varphi : G \to \bar{G}$ is a **homomorphism** if $\varphi(ab) = \varphi(a) \varphi(b)$ for all $a, b \in G$. We say that φ is an **isomorphism** if φ is also a bijection, i.e. one to one and onto. We say G and $\bar{G}$ are **isomorphic** if there exists and isomorphism, $\varphi : G \to \bar{G}$.*

Lemma 15.9. *If $\varphi : G \to \bar{G}$ is an isomorphism, the inverse map, φ^{-1}, is also a homomorphism and $\varphi^{-1} : \bar{G} \to G$ is also an isomorphism.*

Proof. Suppose that $\bar{a}, \bar{b} \in \bar{G}$ and $a := \varphi^{-1}(\bar{a})$ and $b := \varphi^{-1}\left(\bar{b}\right)$. Then $\varphi(ab) = \varphi(a) \varphi(b) = \bar{a}\bar{b}$ from which it follows that

$$\varphi^{-1}\left(\bar{a}\bar{b}\right) = ab = \varphi^{-1}(\bar{a}) \varphi^{-1}\left(\bar{b}\right)$$

as desired. ■

Notation 15.10 *If $\varphi : G \to \bar{G}$ is a homomorphism, then the **kernel of** φ is defined by,*

$$\ker(\varphi) := \varphi^{-1}(\{e_{\bar{G}}\}) := \{x \in G : \varphi(x) = e_{\bar{G}}\} \subset G$$

*and the **range of** φ by*

$$\mathrm{Ran}(\varphi) := \varphi(G) = \{\varphi(g) : g \in G\} \subset \bar{G}.$$

Example 15.11. The **trivial homomorphism**, $\varphi : G \to \bar{G}$, is defined by $\varphi(g) = \bar{e}$ for all $g \in G$. For this example,

$$\ker(\varphi) = G \text{ and } \mathrm{Ran}(G) = \{\bar{e}\}.$$

Example 15.12. Let $G = GL(n, \mathbb{R})$ denote the set of $n \times n$ - invertible matrices with the binary operation being matrix multiplication and let $H = \mathbb{R}^* := \mathbb{R} \setminus \{0\}$ equipped with multiplication as the binary operation. Then $\det : G \to H$ is a homomorphism. In this example,

$$\ker(\det) = SL(n, \mathbb{R}) := \{A \in GL(n, \mathbb{R}) : \det A = 1\} \text{ and}$$
$$\mathrm{Ran}(\det) = \mathbb{R}^* \text{ (why?)}.$$

Example 15.13. Suppose that $G = \mathbb{R}^n$ and $H = \mathbb{R}^m$ both equipped with $+$ as their binary operation. Then any $m \times n$ matrix, A, gives rise to a homomorphism[1] from $G \to H$ via the map, $\varphi_A(x) := Ax$ for all $x \in \mathbb{R}^n$. In this case $\ker(\varphi_A) = \mathrm{Nul}(A)$ and $\mathrm{Ran}(\varphi_A) = \mathrm{Ran}(A)$. Moreover, φ_A is an isomorphism iff $m = n$ and A is invertible.

[1] **Fact:** any continuous homomorphism is of this form.

16

Lecture 16 (2/11/2009)

Example 16.1. Suppose that $G = \mathbb{R}$ and $\bar{G} = S^1 := \{z \in \mathbb{Z} : |z| = 1\}$. We use addition on G and multiplication of $\bar{G}$ as the group operations. Then for each $\lambda \in \mathbb{R}$, $\varphi_\lambda(t) := e^{i\lambda t}$ is a homomorphism from G to $\bar{G}$. For this example, if $\lambda \neq 0$ then $\varphi_\lambda(t) = 1$ iff $\lambda t \in 2\pi\mathbb{Z}$ and therefore

$$\ker(\varphi_\lambda) = \frac{2\pi}{\lambda}\mathbb{Z} \text{ and } \operatorname{Ran}(\varphi_\lambda) = S^1.$$

If $\lambda = 0$, $\varphi_\lambda = \varphi_0$ is the trivial homomorphism.

Example 16.2. Suppose that $G = \bar{G} = S^1 := \{z \in \mathbb{Z} : |z| = 1\}$. Then for each $n \in \mathbb{Z}$, $\varphi_n(z) := z^n$ is a homomorphism and when $n = \pm 1$ it is an isomorphism. If $n = 0$, $\varphi_n = \varphi_0$ is the trivial homomorphism while if $n \neq 0$, $\varphi_n(z) = 1$ iff $z^n = 1$ iff $z = e^{i\frac{2\pi}{n}k}$ for some $k = 0, 1, 2, \dots, n-1$, so that

$$\ker(\varphi_n) = \left\{e^{i\frac{2\pi}{n}k} : k = 0, 1, 2, \dots, n-1\right\} \text{ while}$$
$$\operatorname{Ran}(\varphi_n) = S^1 = \bar{G}.$$

Theorem 16.3. *If $\varphi : G \to \bar{G}$ is a homomorphism, then*

1. $\varphi(e) = \bar{e} \in \bar{G}$,
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$ *for all* $a \in G$,
3. $\varphi(a^n) = \varphi(a)^n$ *for all* $n \in \mathbb{Z}$,
4. *If* $|g| < \infty$ *then* $|\varphi(g)|$ *divides* $|g|$,
5. $\varphi(G) \leq \bar{G}$,
6. $\ker(\varphi) \leq G$,
7. $\varphi(a) = \varphi(b)$ *iff* $a^{-1}b \in \ker(\varphi)$ *iff* $a\ker(\varphi) = b\ker(\varphi)$, *and*
8. *If* $\varphi(a) = \bar{a} \in \bar{G}$, *then*

$$\varphi^{-1}(\bar{a}) := \{x \in G : \varphi(x) = \bar{a}\} = a\ker\varphi.$$

Proof. We prove each of these results in turn.

1. By the homomorphism property,

$$\varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e)$$

and so by cancellation, we learn that $\varphi(e) = \bar{e}$.

2. If $a \in G$ we have,

$$\bar{e} = \varphi(e) = \varphi(a \cdot a^{-1}) = \varphi(a) \cdot \varphi(a^{-1})$$

and therefore, $\varphi(a^{-1}) = \varphi(a)^{-1}$.

3. When $n = 0$ item 3 follows from item 1. For $n \geq 1$, we have

$$\varphi(a^n) = \varphi(a \cdot a^{n-1}) = \varphi(a) \cdot \varphi(a^{n-1})$$

from which the result then follows by induction. For $n \leq 1$ we have,

$$\varphi(a^n) = \varphi\left(\left(a^{|n|}\right)^{-1}\right) = \varphi\left(a^{|n|}\right)^{-1} = \left(\varphi(a)^{|n|}\right)^{-1} = \varphi(a)^n.$$

4. Let $n = |g| < \infty$, then $\varphi(g)^n = \varphi(g^n) = \varphi(e) = e$. Therefore, $|\varphi(g)|$ divides $n = |g|$.
5. If $x, y \in G$, $\varphi(x)$ and $\varphi(y)$ are two generic elements of $\varphi(G)$. Since, $\varphi(x)^{-1}\varphi(y) = \varphi(x^{-1}y) \in \varphi(G)$, it follows that $\varphi(G) \leq \bar{G}$.
6. If x, y are now in $\ker(\varphi)$, i.e. $\varphi(x) = e = \varphi(y)$, then

$$\varphi(x^{-1}y) = \varphi(x)^{-1}\varphi(y) = e^{-1}e = e.$$

This shows $x^{-1}y \in \ker(\varphi)$ and therefore that $\ker(\varphi) \leq G$.

7. We have $\varphi(a) = \varphi(b)$ iff $e = \varphi(a)^{-1}\varphi(b) = \varphi(a^{-1}b)$ iff $a^{-1}b \in \ker(\varphi)$.
8. We have $x \in \varphi^{-1}(\bar{a})$ iff $\varphi(x) = \bar{a} = \varphi(a)$ which (by 7.) happens iff $a^{-1}x \in \ker(\varphi)$, i.e. iff $x \in a\ker(\varphi)$.

■

Corollary 16.4. *A homomorphism, $\varphi : G \to \bar{G}$ is an isomorphism iff* $\ker(\varphi) = \{e\}$ *and* $\varphi(G) = \bar{G}$.

Proof. According to item 7. of Theorem 16.3, φ is one to one iff $\ker(\varphi) = \{e\}$. Since φ is onto iff (by definition) $\varphi(G) = \bar{G}$ the proof is complete. ■

Proposition 16.5 (Classification of groups with all elments being order 2). *Suppose G is a non-trivial finite group such that $x^2 = 1$ for all $x \in G$. Then $G \cong \mathbb{Z}_2^k$ and $|G| = 2^k$ for some $k \in \mathbb{Z}_+$.*

Proof. We know from Lemma 15.6 that G is abelian. Choose $a_1 \neq e$ and let

$$H_1 := \{e, a_1\} = \{a_1^{\varepsilon} : \varepsilon \in \mathbb{Z}_2\} \leq G.$$

If $H_1 \neq G$, choose $a_2 \in G \setminus H_1$ and then let

$$H_2 := \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} : \varepsilon_i \in \mathbb{Z}_2\} \leq G.$$

Notice that $|H_2| = 2^2$. If $H_2 \neq G$ choose $a_3 \in G \setminus H_2$ and let

$$H_3 := \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} a_3^{\varepsilon_3} : \varepsilon_i \in \mathbb{Z}_2\}.$$

If $a_1^{\varepsilon_1} a_2^{\varepsilon_2} a_3 = a_1^{\varepsilon_1'} a_2^{\varepsilon_2'}$, then $a_3 \in H_2$ which is is not. If $a_1^{\varepsilon_1} a_2^{\varepsilon_2} a_3 = a_1^{\varepsilon_1'} a_2^{\varepsilon_2'} a_3$ then $a_1^{\varepsilon_1} a_2^{\varepsilon_2} = a_1^{\varepsilon_1'} a_2^{\varepsilon_2'}$ and therefore $\varepsilon_i = \varepsilon_i'$ for $i = 1, 2$. This shows that $|H_3| = 2^3$, i.e. all elements in the list are distinct. Continuing this way we eventually find $\{a_i\}_{i=1}^k \subset G$ such that

$$G = \{a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k} : \varepsilon_i \in \mathbb{Z}_2\}$$

with all elements being distinct in this list. We may now define $\varphi : \mathbb{Z}_2^k \to G$, by

$$\varphi(\varepsilon_1, \dots, \varepsilon_k) := a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k}.$$

This map is clearly one to one and onto and is easily seen to be a homomorphism and hence an isomorphism. Indeed, since G is abelian,

$$\begin{aligned}
\varphi(\varepsilon_1, \dots, \varepsilon_k)\, \varphi(\delta_1, \dots, \delta_k) &= a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k} a_1^{\delta_1} \dots a_k^{\delta_k} = a_1^{\varepsilon_1} a_1^{\delta_1} \dots a_k^{\varepsilon_k} a_k^{\delta_k} \\
&= a_1^{\varepsilon_1 + \delta_1} \dots a_k^{\varepsilon_k + \delta_k} = a_1^{(\varepsilon_1 + \delta_1) \bmod 2} \dots a_k^{(\varepsilon_k + \delta_k) \bmod 2} \\
&= \varphi((\varepsilon_1, \dots, \varepsilon_k) + (\delta_1, \dots, \delta_k)).
\end{aligned}$$

■

Example 16.6 (Essentially the same as a homework problem). Recall that $U(12) = \{1, 5, 7, 11\}$ has all elements of order 2. Since $|U(12)| = 2^2$ we know that $U(12) \cong \mathbb{Z}_2^2$. In this case we may take, $\varphi(\varepsilon_1, \varepsilon_2) := 5^{\varepsilon_1} 7^{\varepsilon_2}$. Notice that $5 \cdot 7 = 35 \bmod 12 = 11$. On the other hand,

$$U(10) = \{1, 3, 7, 9\} = \langle 3 \rangle = \left\{1, 3, 3^2 = 9, 3^3 = 7\right\}.$$

It will follows from Theorem 17.1 below that $U(10)$ and $U(12)$ can not be isomorphic.

17

Lecture 17 (2/13/2009)

Theorem 17.1. *If $\varphi : G \to \bar{G}$ is a group isomorphism, then φ preserves all group related properties. For example;*

1. *$|\varphi(g)| = |g|$ for all $g \in G$.*
2. *G is cyclic iff $\bar{G}$ is cyclic. Moreover $g \in G$ is a generator of G iff $\varphi(g)$ is a generator of $\bar{G}$.*
3. *$a, b \in G$ commute iff $\varphi(a), \varphi(b)$ commute in G. In particular, G is abelian iff $\bar{G}$ is abelian.*
4. *For $k \in \mathbb{Z}_+$ and $b \in G$, the equation $x^k = b$ in G and $\bar{x}^k = \varphi(b)$ in $\bar{G}$ have the same number of equations. In fact, if $x^k = b$ iff $\varphi(x)^k = \varphi(b)$.*
5. *$K \subset G$ is a subgroup of G iff $\varphi(K)$ is a subgroup of $\bar{G}$.*

Proof. 1. We have seen that $|\varphi(g)|\,|\,|g|$. Similarly it follows that $\left|\varphi^{-1}(\varphi(g))\right|\,|\,|\varphi(g)|$, i.e. $|g|\,|\,|\varphi(g)|$. Thus $|\varphi(g)| = |g|$.

2. If $G = \langle g \rangle$, then $\bar{G} = \varphi(G) = \langle \varphi(g) \rangle$ showing $\bar{G}$ is cyclic. The converse follows by considering φ^{-1}.

3. If $ab = ba$ then $\varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a)$. The converse assertion again follows by considering φ^{-1}.

4. We have $x^k = b$ implies $\varphi(b) = \varphi\left(x^k\right) = \varphi(x)^k$. Conversely if $\bar{x}^k = \varphi(b)$ then $\varphi^{-1}(\bar{x})^k = b$. Thus taking $x := \varphi^{-1}(\bar{x})$ we have $x^k = b$ and $\bar{x} = \varphi(x)$.

5. We know if $K \leq G$ then $\varphi(K) \leq \bar{G}$ and $\varphi(K) \leq \bar{G}$ then $K = \varphi^{-1}(\varphi(K)) \leq G$. ■

Example 17.2. Let $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ and $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ which are groups under multiplication. We claim they are not isomorphic. If they were the equations $z^4 = 1$ in $\mathbb{C}^*$ and $x^4 = 1$ in $\mathbb{R}^*$ would have to have the same number of solutions. However the first has four solutions, $z = \{\pm 1, \pm i\}$, while the second has only two, $\{\pm 1\}$.

Proposition 17.3. *Suppose that $\varphi : G \to \bar{G}$ is a homomorphism and $a \in G$, then the values of φ on $\langle a \rangle \leq G$ are uniquely determined by knowing $\bar{a} = \varphi(a)$. Let $\bar{n} := |\bar{a}|$ and $n = |a|$.*

1. *If $n = \infty$, then to every element $\bar{a} \in \bar{G}$ there is a unique homomorphism from G to $\bar{G}$ such that $\varphi(a) = \bar{a}$. If $\bar{n} = \infty$, then $\ker(\varphi) = \{e\}$ while if $\bar{n} < \infty$, then $\ker(\varphi) = \langle a^{\bar{n}} \rangle = \left\langle a^{|\bar{a}|} \right\rangle$.*
2. *If $n < \infty$, then to every element $\bar{a} \in \bar{G}$ such that $\bar{n}|n$, there is a unique homomorphism, φ, from G to $\bar{G}$. This homomorphism satisfies;*
   a) $\ker(\varphi) = \langle a^{\bar{n}} \rangle = \left\langle a^{|\bar{a}|} \right\rangle$ and
   b) $\varphi : \langle a \rangle \to \langle \bar{a} \rangle$ is an isomorphism iff $|a| = n = \bar{n} = |\bar{a}|$.

In particular, two cyclic groups are isomorphic iff they have the same order.

Proof. Since $\varphi\left(a^k\right) = \varphi(a)^k = \bar{a}^k$, it follows that φ is uniquely determined by knowing $\bar{a} = \varphi(a)$.

1. If $n = |a| = \infty$, we may define $\varphi\left(a^k\right) = \bar{a}^k$ for all $k \in \mathbb{Z}$. Then

$$\varphi\left(a^k a^l\right) = \varphi\left(a^{k+l}\right) = \bar{a}^{k+l} = \bar{a}^k \bar{a}^l = \varphi\left(a^k\right)\varphi\left(a^l\right),$$

showing φ is a homomorphism. Moreover, we have $e = \varphi\left(a^k\right) = \bar{a}^k$ iff $\bar{n} = |\bar{a}|$ divides $|k$, i.e.

$$\ker(\varphi) = \left\{a^{l \cdot \bar{n}} : l \in \mathbb{Z}\right\} = \left\langle a^{\bar{n}} \right\rangle.$$

2. Now suppose that n and $\bar{n}$ are finite and $\bar{n}|n$. Then again we define,

$$\varphi\left(a^k\right) := \bar{a}^k \text{ for all } k \in \mathbb{Z}.$$

However in this case we must show φ is "well defined," i.e. we must check the definition makes sense. The problem now is that $\left\{a^k : k \in \mathbb{Z}\right\}$ contains repetitions and in fact we know that $a^k = a^{k \bmod n}$. Thus we must show $\varphi\left(a^k\right) = \varphi\left(a^{k \bmod n}\right)$. Write $k = sn + r$ with $r = k \bmod n$, then

$$\varphi\left(a^k\right) = \bar{a}^k = \bar{a}^{sn}\bar{a}^r = \bar{a}^r = \varphi\left(a^r\right),$$

wherein we have used $\bar{a}^n = e$ since $\bar{n}|n$.

We now compute $\ker(\varphi)$. For this we have $\bar{e} = \varphi\left(a^k\right) = \bar{a}^k$ iff $\bar{n}|k$ and therefore,

$$\ker(\varphi) = \left\{a^k : \bar{n}|k\right\} = \left\{a^{l \cdot \bar{n}} : l \in \mathbb{Z}\right\} = \left\langle a^{\bar{n}} \right\rangle.$$

Notice that $\ker(\varphi) = \{e\}$ iff $\bar{n} = n$ and in this case $\varphi(\langle a \rangle) = \langle \bar{a} \rangle$ showing φ is an isomorphism. If G and $\bar{G}$ are cyclic groups of different orders, there is not bijective map from G to $\bar{G}$ let alone no bijective homomorphism. ■

Corollary 17.4. *If $G = \langle a \rangle$ and $|a| = \infty$, then $\varphi : G \to \mathbb{Z}$ defined by $\varphi\left(a^k\right) = k$ is an isomorphism. While if $|a| = n < \infty$, then $\varphi : G \to \mathbb{Z}_n$ defined by $\varphi\left(a^k\right) = k \bmod n$ is an isomorphism.*

Proof. Each of the maps are well defined (by Proposition 17.3) homomorphisms **onto** $\mathbb{Z}$ and $\mathbb{Z}_n$ respectively. Moreover the same proposition shows that $\ker(\varphi) = \{e\}$ in each case and therefore they are isomorphism. ■

Example 17.5. If $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_{30}$ is a homomorphism, then $\varphi(1) = k \in \mathbb{Z}_{30}$ where the order of $|k|$ must divide 12 which is equivalent to $k \cdot 12 = 0$ in $\mathbb{Z}_{30}$. This condition is easy to remember since, $12 = 0$ in $\mathbb{Z}_{12}$ and therefore $0 = \varphi(0) = \varphi(12) = k \cdot 12$. At any rate we know that $30|(k \cdot 12)$ or equivalently, $5|(2k)$, i.e. $5|k$. Thus the homomorphisms are of the form,

$$\varphi_k(x) = kx \text{ where } k \in \{0, 5, 10, 15, 20, 25\}.$$

Furthermore we have $\varphi_5(x) = 0$ iff $5x = 0 \,(\mathrm{mod})\, 30$ iff $x = 0 \,(\mathrm{mod})\, 6$ iff x is a multiple of 6, i.e. $x \in \langle 6 \rangle$. We also have

$$\varphi_5(\mathbb{Z}_{12}) = \langle 5 \rangle = \{1, 5, 10, 15, 20, 25\} \leq \mathbb{Z}_{30}.$$

More generally one shows

k	$\gcd(k, 30)$	$\lvert k\rvert = \frac{30}{\gcd(k,30)}$	$\operatorname{Ran}(\varphi_k) = \langle k \rangle =$ $\langle \gcd(k, 30) \rangle \leq \mathbb{Z}_{30}$	$\ker(\varphi_k) =$ $\langle \lvert k\rvert \rangle \leq \mathbb{Z}_{12}$
0	30	1	$\langle 0 \rangle = \langle 30 \rangle$	$\mathbb{Z}_{12} = \langle 1 \rangle$
5	5	6	$\langle 5 \rangle$	$\langle 6 \rangle$
10	10	3	$\langle 10 \rangle$	$\langle 3 \rangle$
15	15	2	$\langle 15 \rangle$	$\langle 2 \rangle$
20	10	3	$\langle 20 \rangle = \langle 10 \rangle$	$\langle 3 \rangle$
25	5	6	$\langle 25 \rangle = \langle 5 \rangle$	$\langle 6 \rangle$

as we will prove more generally in the next proposition.

Lemma 17.6. *Suppose that $m, n, k \in \mathbb{Z}_+$, then $m|(nk)$ iff $\frac{m}{\gcd(m,n)}|k$.*

Proof. Let $d := \gcd(m, n)$, $m' := m/d$ and $n' := n/d$. Then $\gcd(m', n') = 1$. Moreover we have $m|(nk)$ iff $\mathbb{Z} \ni \frac{nk}{m} = \frac{n'k}{m'}$ iff $m'|(n'k)$ iff (by Euclid's lemma) $m'|k$. ■

Proposition 17.7. *If $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ is a homomorphisms, then $\varphi = \varphi_k$ for some $k \in \left\langle \frac{m}{\gcd(m,n)} \right\rangle$ where $\varphi_k(x) = kx \; (= kx \bmod m)$. The list of distinct homomorphisms from $\mathbb{Z}_n \to \mathbb{Z}_m$ is given by,*

$$\left\{ \varphi_k : k \in \left\langle \frac{m}{\gcd(m,n)} \right\rangle \text{ with } 0 \leq k < \frac{m}{\gcd(m,n)} \right\}.$$

Moreover,

$$\operatorname{Ran}(\varphi_k) = \varphi(\mathbb{Z}_n) = \langle k \rangle = \langle \gcd(m, k) \rangle \leq \mathbb{Z}_m \text{ and}$$

$$\ker(\varphi) = \left\langle |k|_{\mathbb{Z}_m} \right\rangle = \left\langle \frac{m}{\gcd(k, m)} \right\rangle \leq \mathbb{Z}_n.$$

Proof. Let $d := \gcd(m, n)$ and $m' = m/d$. By Proposition 17.3 the homomorphisms, $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$, are of the form $\varphi_k(x) = kx$ where $k = \varphi_k(1)$ must satisfy, $|k|_{\mathbb{Z}_m} |n$, i.e. $\frac{m}{\gcd(k,m)}|n$. Alternatively, this is equivalent to (see the proof[1] of item 4. of Theorem 16.3) requiring $kn = 0$ in $\mathbb{Z}_m$, i.e. that $m|(kn)$ which by Lemma 17.6 is equivalent to $m'|k$. Thus the homomorphisms $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ are of the form $\varphi = \varphi_k$ where $k \in \langle m' \rangle = \left\langle \frac{m}{\gcd(m,n)} \right\rangle$.

If is now easy to see that $\operatorname{Ran}(\varphi_k) = \langle k \rangle = \langle \gcd(m, k) \rangle$ and from Proposition 17.3 we know that

$$\ker(\varphi_k) = \left\langle |k|_{\mathbb{Z}_m} \cdot 1 \right\rangle = \left\langle \frac{m}{\gcd(k, m)} \right\rangle.$$

Alternatively, $0 = \varphi_k(x)$ iff $kx = 0 \,(\mathrm{mod})\, m$, i.e. iff $m|(kx)$ which happens (by Lemma 17.6) iff $m'|x$, i.e.

$$x \in \langle m' \rangle = \left\langle \frac{m}{\gcd(k, m)} \right\rangle = \left\langle |k|_{\mathbb{Z}_m} \right\rangle \leq \mathbb{Z}_n.$$

■

Corollary 17.8. *If $m, n \in \mathbb{Z}_+$ are relatively prime there is only one homomorphism, $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$, namely the zero homomorphism.*

Proof. This follows from Proposition 17.7. We can also check it directly. Indeed, if $\varphi(1) = k$ then $0 = \varphi(0) = \varphi(n) = kn \bmod m$ which implies $m|(nk)$ and hence by Euclid's lemma, $m|k$. Therefore,

$$\varphi(x) = (kx) \bmod m = (k \bmod m)(x \bmod m) \bmod m = 0\,(x \bmod m) \bmod m = 0$$

for all $x \in \mathbb{Z}_n$. ■

[1] We can also see this using Lemma 17.6. By that lemma with the roles of n and k interchanged, $\frac{m}{\gcd(k,m)}|n$ iff $m|(nk)$.

Lecture 18 (2/16/2009)

Notation 18.1 *Given a group, G, let*

$$\operatorname{Aut}(G) := \{\varphi : G \to G | \varphi \text{ is an isomorphism}\}.$$

We call $\operatorname{Aut}(G)$ *the* ***automorphism group of*** G.

Lemma 18.2. $\operatorname{Aut}(G)$ *is a group using composition of homomorphisms as the binary operation.*

Proof. We will show $\operatorname{Aut}(G)$ is a sub-group of the invertible functions from $G \to G$. We have already seen that $\operatorname{Aut}(G)$ is closed under taking inverses in Lemma 15.9. So we must now only show that $\operatorname{Aut}(G)$ is closed under function composition. But this is easy, since if $a, b \in G$ and $\varphi, \psi \in \operatorname{Aut}(G)$, then $\varphi \circ \psi$ is still a bijection with inverse function given by $(\varphi \circ \psi)^{-1} = \psi^{-1} \circ \varphi^{-1}$, and

$$\begin{aligned}(\varphi \circ \psi)(ab) &= \varphi(\psi(ab)) = \varphi(\psi(a)\psi(b)) \\ &= \varphi(\psi(a))\varphi(\psi(b)) = (\varphi \circ \psi)(a) \cdot (\varphi \circ \psi)(b)\end{aligned}$$

which shows that $\varphi \circ \psi \in \operatorname{Aut}(G)$. ■

Example 18.3. If $\varphi : \mathbb{Z} \to \mathbb{Z}$ is a homomorphism, then $\varphi(x) = kx$ where $k = \varphi(1)$. Conversely, $\varphi_k(x) := kx$ gives a homomorphism from $\mathbb{Z} \to \mathbb{Z}$ for all $k \in \mathbb{Z}$. Moreover we have $\ker(\varphi_k) = \langle 0 \rangle$ if $k \neq 0$ while $\ker(\varphi_0) = \mathbb{Z}$. Since $\varphi_k(\mathbb{Z}) = \langle k \rangle \leq \mathbb{Z}$ we see that $\varphi_k(\mathbb{Z}) = \mathbb{Z}$ iff $k = \pm 1$. So $\varphi_k : \mathbb{Z} \to \mathbb{Z}$ is an isomorphism iff $k \in \{\pm 1\}$ and we have shown (see Proposition 16.5),

$$\operatorname{Aut}(\mathbb{Z}) = \{\varphi_k : k = 1 \text{ or } k = -1\} \cong \mathbb{Z}_2.$$

To see that last statement directly simply check that $\psi : \mathbb{Z}_2 \to \operatorname{Aut}(\mathbb{Z})$ defined by $\psi(0) = \varphi_1$ and $\psi(1) = \varphi_{-1}$ is a homomorphism. The only case to check is as follows:

$$\varphi_1 = \psi(0) = \psi(1+1) \overset{?}{=} \psi(1) \circ \psi(1) = \varphi_{-1} \circ \varphi_{-1} = \varphi_{(-1)^2} = \varphi_1. \quad \checkmark$$

Theorem 18.4 ($\operatorname{Aut}(\mathbb{Z}_n) \cong U(n)$)**.** *All of the homomorphisms form $\mathbb{Z}_n$ to itself are of the form, $\varphi_k(x) = kx \bmod n$ for some $k \in \mathbb{Z}_n$. Moreover, these φ_k is an isomorphism iff $k \in U(n)$. Moreover the map,*

$$U(n) \ni k \to \varphi_k \in \operatorname{Aut}(\mathbb{Z}_n) \tag{18.1}$$

is an isomorphism of groups.

Proof. Since $kn = 0 \bmod n$ for all $k \in \mathbb{Z}_n$ it follows from Proposition 17.7 that all of the homomorphisms, $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ are of the form described. Moreover, by Proposition 17.7, $\operatorname{Ran}(\varphi_k) = \langle k \rangle = \langle \gcd(n,k) \rangle$ which is equal to $\mathbb{Z}_n$ iff $\gcd(n,k) = 1$, i.e. iff $k \in U(n)$. For such a k we know that φ_k is also one to one since $\mathbb{Z}_n$ is a finite set. Thus

$$\operatorname{Aut}(\mathbb{Z}_n) = \{\varphi_k : k \in U(n)\}. \tag{18.2}$$

Alternatively we have

$$\ker(\varphi_k) = \left\langle \frac{n}{\gcd(k,n)} \right\rangle$$

which is trivial iff $\frac{n}{\gcd(k,n)} = n$, i.e. $\gcd(k,n) = 1$, i.e. $k \in U(n)$. Thus for $k \in U(n)$ we know that φ_k is one to one and hence onto. So again we have verified Eq. (18.2).

Suppose that $k, l \in U(n)$, then with all arithmetic being done $\bmod n$ – i.e. in $\mathbb{Z}_n$ we have

$$\varphi_k \circ \varphi_l(x) = k(lx) = (kl)x = \varphi_{kl}(x) \text{ for all } x \in \mathbb{Z}_n.$$

This shows that map in Eq. (18.1) is a homomorphism and hence an isomorphism since it is one to one and onto. The inverse map is,

$$\operatorname{Aut}(\mathbb{Z}_n) \ni \varphi \to \varphi(1) \in U(n).$$

Third direct proof: Suppose that $k, l \in \mathbb{Z}_n$, then with all arithmetic being done $\bmod n$ – i.e. in $\mathbb{Z}_n$ we have

$$\varphi_k \circ \varphi_l(x) = k(lx) = (kl)x = \varphi_{kl}(x) \text{ for all } x \in \mathbb{Z}_n.$$

Using this it follows that if $k \in U(n)$ and k^{-1} is its inverse in $U(n)$, then $\varphi_k^{-1} = \varphi_{k^{-1}}$, so that $\varphi_k \in \operatorname{Aut}(\mathbb{Z}_n)$. Conversely if $d = \gcd(k,n) > 1$, then

$$\varphi_k\left(\frac{n}{d}\right) = \left(k\frac{n}{d}\right) \bmod n = \left(\frac{k}{d}n\right) \bmod n = 0$$

which shows $\ker(\varphi_k)$ contains $\frac{n}{d} \neq 0$ in $\mathbb{Z}_n$. Hence φ_k is not an isomorphism. ■

Proposition 18.5. *If $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ is a homomorphism, then $\varphi(x) = kx$ $(= kx \bmod n)$ where $k = \varphi(1) \in \mathbb{Z}_n$. Conversely to each $k \in \mathbb{Z}_n$, $\varphi_k(x) := kx$ defines a homomorphism from $\mathbb{Z} \rightarrow \mathbb{Z}_n$. The kernel and range of φ_k are given by*

$$\ker(\varphi_k) = \left\langle \frac{n}{\gcd(k,n)} 1 \right\rangle = \left\langle \frac{n}{\gcd(k,n)} \right\rangle \subset \mathbb{Z}$$

and

$$\operatorname{Ran}(\varphi_k) = \langle k \rangle = \langle \gcd(k,n) \rangle \subset \mathbb{Z}_n.$$

Thus $\ker(\varphi_k)$ *is never* 0 *and* $\operatorname{Ran}(\varphi_k) = \mathbb{Z}_n$ *iff* $k \in U(n)$.

Proof. Most of this is straight forward to prove and actually follows from Proposition 17.3. Since the order of $k \in \mathbb{Z}_n$ is $\frac{n}{\gcd(k,n)}$ we have,

$$\ker(\varphi_k) = \left\langle \frac{n}{\gcd(k,n)} \cdot 1 \right\rangle = \left\langle \frac{n}{\gcd(k,n)} 1 \right\rangle.$$

As a direct check notice that $0 = \varphi_k(x) = kx \bmod n$ happens iff $n | kx$ iff $\frac{n}{\gcd(k,n)} | x$ iff $x \in \left\langle \frac{n}{\gcd(k,n)} \cdot 1 \right\rangle$. We can also directly check that φ_k is a homomorphism:

$$\begin{aligned}\varphi_k(x+y) &= k(x+y) \bmod n = (kx+ky) \bmod n \\ &= kx \bmod n + ky \bmod n = \varphi_k(x) + \varphi_k(y).\end{aligned}$$

Finally,

$$\varphi_k(\mathbb{Z}) = \langle k \rangle = \langle \gcd(k,n) \rangle \leq \mathbb{Z}_n,$$

and therefore, $\varphi_k(\mathbb{Z}) = \langle k \rangle = \mathbb{Z}_n$ iff k is a generator of $\mathbb{Z}_n$ iff $\gcd(k,n) = 1$ iff $k \in U(n)$. ■

19

Lecture 19 (2/18/2009)

Definition 19.1. *The **external direct product** of groups, $G_1, \dots, G_n$, is,*

$$G_1 \oplus \cdots \oplus G_n := G_1 \times \cdots \times G_n \text{ as a set}$$

with group operation given by

$$(g_1, \dots, g_n)(g_1', \dots, g_n') = (g_1 g_1', \dots, g_n g_n'),$$

i.e. you just multiply componentwise. (It is easy to check this is a group with $\mathbf{e} := (e, \dots, e)$ *being the identity and*

$$(g_1, \dots, g_n)^{-1} = \left(g_1^{-1}, \dots, g_n^{-1}\right).$$

Example 19.2. Recall that $U(5) = \{1, 2, 3, 4\}$ and $\mathbb{Z}_3 = \{0, 1, 2\}$ and therefore,

$$U(5) \times \mathbb{Z}_3 = \{(i, j) : 1 \le i \le 4 \text{ and } 0 \le j \le 2\}.$$

Moroever, we have

$$(2, 1) \cdot (3, 1) = (2 \cdot 3 \bmod 5, 1 + 1 \bmod 3) = (1, 2).$$

and

$$(2, 1)^{-1} = (3, 2).$$

Example 19.3. Suppose that $|G| = 4$, then $G \cong \mathbb{Z}_4$ or $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. By Lagrange's theorem, we know that $|g| = 1$, 2, or 4 for all $g \in G$. If there exists $g \in G$ with $|g| = 4$, then $G = \langle g \rangle \cong \mathbb{Z}_4$ and if $|g| \le 2$ for all $g \in G$ we know that $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ from results we have proved above. In particular there are only two groups of order 4 and they are both abelian.

Fact 19.4 *Here are some simple facts about direct products:*

1. $|G_1 \oplus \cdots \oplus G_n| = |G_1| \times \cdots \times |G_n|$.
2. *Up to isomorphism, the groups $G_1 \oplus \cdots \oplus G_n$ are independent of how the factors are ordered. For example,*

$$G_1 \oplus G_2 \oplus G_3 \ni (g_1, g_2, g_3) \to (g_3, g_2, g_1) \in G_3 \oplus G_2 \oplus G_1$$

is an isomorphism.

3. *One may associate the direct product factors in any way you please up to isomorphism. So for example,*

$$(G_1 \oplus G_2) \oplus G_3 \ni ((g_1, g_2), g_3) \to (g_1, g_2, g_3) \in G_1 \oplus G_2 \oplus G_3$$

is an isomorphism.

Remark 19.5. Observe that if $g = (e, \dots, e, g_k, e, \dots, e)$ and $g' = (e, \dots, e, g_l, e, \dots, e)$ for some $l \ne k$, then g and g' commute. For example in $G_1 \times G_2$, (g_1, e) and (e, g_2) commute since,

$$(g_1, e)(e, g_2) = (g_1, g_2) = (e, g_2)(g_1, e).$$

Theorem 19.6. *Let $(g_1, \dots, g_n) \in G_1 \oplus \cdots \oplus G_n$, then*

$$|(g_1, \dots, g_n)| = \operatorname{lcm}(|g_1|, \dots, |g_n|).$$

(Also see Proposition 13.3.)

Proof. If $t \in \mathbb{Z}_+$, then

$$(g_1, \dots, g_n)^t = e = (e, \dots, e) \iff g_i^t = e \text{ for all } i$$

and this happens iff $|g_i| \, | t$ for all i, i.e. iff t is a common multiple of $\{|g_i|\}$. Therefore the order $(g_1, \dots, g_n)$ must be $\operatorname{lcm}(|g_1|, \dots, |g_n|)$. ■

Example 19.7 (Exercise 8.10 and 8.11).

1. How many elements of order 9 does $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ have? The elements of order 9 are of the form (a, b) where $|b| = 9$, i.e. $b \in U(9)$. Thus the elements of order 9 are $\mathbb{Z}_3 \times U(9)$ of which there are,

$$|\mathbb{Z}_3 \times U(9)| = 3 \cdot \varphi(9) = 3 \cdot \left(3^3 - 3\right) = 18.$$

2. Exercise 8.11 – how many elements of order 4 are there in $\mathbb{Z}_{400} \oplus \mathbb{Z}_{800}$? Recall that there is one subgroup of order 4 inside of $\mathbb{Z}_n$ when $4|n$ which is $\left\langle \frac{n}{4} \right\rangle$. All the elements of order 4 are inside this sub-group and hence there are $\varphi(4) = 2$ of them. The elements of order 2 in $\mathbb{Z}_n$ are in $\left\langle \frac{n}{2} \right\rangle$ and there is only one of them. So $\mathbb{Z}_n$ has 2 elements of order 4 and one each of order 2 and 1. The elements of order 4 inside of $\mathbb{Z}_m \oplus \mathbb{Z}_n$ are of the form (a, b) where $|a| = 1$ or 2 and $|b| = 4$ of which there are $2 \cdot 2 = 4$ of them or $|a| = 4$ and $|b| \in \{1, 2, 4\}$ or which there are $2 \cdot 4 = 8$, so the total is $8 + 4 = 12$.

Example 19.8 (p. 155 Example 5). Determine the number of cyclic subgroups of order 10 inside of $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$. The strategy is to observe that every cyclic subgroup $H = \langle (a,b) \rangle$, of order 10 contains $\varphi(10) = 1 \cdot 4 = 4$ elements of order 10. Thus if we count the number of elements of order 10 we must divide by 4 to get the number of cyclic subgroups of order 10 because no distinct cyclic subgroups of order 10 can share an element of order 10. We now count the number of elements $(a,b) \in \mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$ of order 10. Recall that $|(a,b)| = \mathrm{lcm}(|a|, |b|)$ and $100 = 10 \cdot 10 = 2^2 \cdot 5^2$ and $25 = 5^2$. So in order to get an element of order 10 we must either

1. $|a| = 10$ and $|b| = 1$ or 5 of which there are $\varphi(10) \cdot (\varphi(1) + \varphi(5)) = 4 \cdot (1+4) = 20$ of them, or
2. $|a| = 2$ and $|b| = 5$ of which there are $\varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4$.

Therefore there are $(20+4)/4 = 6$ cyclic subgroups of order 10 inside of $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$.

Lemma 19.9. *If G and H are groups such that $G \oplus H$ is cyclic, then both G and H are cyclic. Alternatively put, if either G or H is not cyclic, then $G \oplus H$ is not cyclic.*

Proof. Let $(g,h) \in G \oplus H$ be a generator of $G \oplus H$. Then every element of $G \oplus H$ is of the form

$$(g,h)^k = \left(g^k, h^k\right) \text{ for some } k \in \mathbb{Z}.$$

Thus every element of G must be of the form g^k for some $k \in \mathbb{Z}$ and every element of H must be of the form h^k for some $k \in \mathbb{Z}$, i.e. both G and H are cyclic. ■

Theorem 19.10. *Suppose that G and H are cyclic groups of finite order, then $G \oplus H$ is cyclic iff $|G|$ and $|H|$ are relatively prime.*

Proof. Let $m = |G|$ and $n = |H|$ and suppose that $G \oplus H$ is cyclic. Then there exists $(a,b) \in G \oplus H$ such that $|(a,b)| = mn$. Now if $d = \gcd(m,n)$ then

$$(a,b)^{\frac{mn}{d}} = \left(a^{m\frac{n}{d}}, b^{n\frac{m}{d}}\right) = \left(e^{\frac{n}{d}}, e^{\frac{m}{d}}\right) = (e,e)$$

so that $(mn)/d \geq |(a,b)| = mn$ and hence $d = 1$, i.e. m and n are relatively prime.

Conversely if m and n are relatively prime and $G = \langle a \rangle$ and $H = \langle b \rangle$, we have $|(a,b)| = \mathrm{lcm}(m,n) = mn = |G \oplus H|$. (Alternatively, see Proposition 13.3.) ■

Example 19.11. Using the above results,

$$\begin{aligned}\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} &\cong (\mathbb{Z}_2 \oplus \mathbb{Z}_5) \oplus (\mathbb{Z}_4 \oplus \mathbb{Z}_3) \\ &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \\ &\cong \mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{20} \oplus \mathbb{Z}_6\end{aligned}$$

and also,

$$\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_8.$$

By the way, $|\mathbb{Z}_{10} \oplus \mathbb{Z}_{12}| = 120$ as is true of all of the other isomorphic groups appearing above.

Corollary 19.12. *Suppose that G_i is cyclic for each i, then $G_1 \oplus \cdots \oplus G_n$ is cyclic iff $|G_i|$ and $|G_j|$ are relatively prime for all $i \neq j$.*

Proof. This is proved by induction. Rather than do this, let me show how the case $n = 3$ works. First suppose that $m_i := |G_i|$ and $m_j := |G_j|$ are relatively prime for all $i \neq j$. Then by Theorem 19.10, $G_2' := G_2 \oplus G_3$ is cyclic and observe that $|G_2'| = m_2 m_3$ is relatively prime to m_1. (Indeed, look at the prime number decompositions. Alternatively, if $d > 1$ is a divisor of m_1 and $(m_2 m_3)$, then by Euclid's lemma, d is also a divisor of m_2 or m_3 and either m_1 and m_2 or m_1 and m_3 are not relatively prime.) So by another application of Theorem 19.10, we know $G_1 \oplus G_2 \oplus G_3 \cong G_1 \oplus G_2'$ is cyclic as well.

Conversely if m_2 and m_3 are not relatively prime (for sake of argument), then $G_2' := G_2 \oplus G_3$ is not cyclic and therefore by Lemma 19.9 we know $G_1 \oplus G_2 \oplus G_3 \cong G_1 \oplus G_2'$ is not cyclic as well. ■

20

Lecture 20 (Review) (2/23/2009)

Lemma 20.1. *Let G be a group, $H \leq G$, and $a, b \in H$. Then*

1. *G is the disjoint union of its **distinct** cosets.*
2. *$aH = bH$ iff $a^{-1}b \in H$.*

Theorem 20.2 (Lagrange's Theorem). *Suppose that G is a finite group and $H \leq G$, then*

$$|G : H| \times |H| = |G|,$$

*where $|G : H| := \#(G/H)$ is the number of **distinct** cosets of H in G. In particular $|H|$ divides $|G|$ and $|G| / |H| = |G : H|$.*

Corollary 20.3. *If G is a group of prime order p, then G is cyclic and every element in $G \setminus \{e\}$ is a generator of G.*

Corollary 20.4 (Fermat's Little Theorem). *Let p be a prime number and $a \in \mathbb{Z}$. Then*

$$a^p \operatorname{mod} p = a \operatorname{mod} p.$$

Theorem 20.5. *If $\varphi : G \to \bar{G}$ is a homomorphism, then*

1. *$\varphi(a^n) = \varphi(a)^n$ for all $n \in \mathbb{Z}$,*
2. *If $|g| < \infty$ then $|\varphi(g)|$ divides $|g|$ or equivalently, $\varphi(g)^{|g|} = e$,*
3. *$\varphi(G) \leq \bar{G}$ and $\ker(\varphi) \leq G$,*
4. *$\varphi(a) = \varphi(b)$ iff $a^{-1}b \in \ker(\varphi)$ iff $a\ker(\varphi) = b\ker(\varphi)$, and*
5. *If $\varphi(a) = \bar{a} \in \bar{G}$, then*

$$\varphi^{-1}(\bar{a}) := \{x \in G : \varphi(x) = \bar{a}\} = a\ker\varphi.$$

Corollary 20.6. *A homomorphism, $\varphi : G \to \bar{G}$ is one to one iff $\ker\varphi = \{e\}$. So $\varphi : G \to \bar{G}$ is an isomorphism iff $\ker\varphi = \{e\}$ and $\varphi(G) = \bar{G}$.*

Corollary 20.7. *If G is a finite group and $\varphi : G \to G$ is a homomorphism, then the following are equivalent:*

1. *φ is an isomorphism.*
2. $\ker\varphi = \{e\}$.
3. *φ is one to one.*
4. *$\varphi(G) = G$, i.e. φ is onto.*

Theorem 20.8. *If $\varphi : G \to \bar{G}$ is a group isomorphism, then φ preserves all group related properties. For example;*

1. *$|\varphi(g)| = |g|$ for all $g \in G$.*
2. *G is cyclic iff $\bar{G}$ is cyclic. Moreover $g \in G$ is a generator of G iff $\varphi(g)$ is a generator of $\bar{G}$.*
3. *$a, b \in G$ commute iff $\varphi(a), \varphi(b)$ commute in G. In particular, G is abelian iff $\bar{G}$ is abelian.*
4. *For $k \in \mathbb{Z}_+$ and $b \in G$, the equation $x^k = b$ in G and $\bar{x}^k = \varphi(b)$ in $\bar{G}$ have the same number of equations. In fact, if $x^k = b$ iff $\varphi(x)^k = \varphi(b)$.*
5. *$K \subset G$ is a subgroup of G iff $\varphi(K)$ is a subgroup of $\bar{G}$.*

Theorem 20.9 (Key Cyclic Group Facts). *Let $a \in G$ and $n = |a|$. Then;*

1. *$a^i = a^j$ iff $i \equiv j \,(\operatorname{mod}) \, n$,*
2. *If $k|m$ then $\langle a^m \rangle \subset \langle a^k \rangle$.*
3. *$\langle a^i \rangle = \langle a^j \rangle$ iff $\gcd(i, n) = \gcd(j, n)$.*
4. *$\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.*
5. *$|a^k| = |a| / \gcd(|a|, k)$.*
6. *a^k is a generator of $\langle a \rangle$ iff $k \in U(n)$.*
7. *If G is a cyclic group of order n, there there are $\varphi(n) := |U(n)|$ elements of order n in G which are given by, $\{a^k : k \in U(n)\}$.*

Theorem 20.10. *Suppose that G is any finite group and $d \in \mathbb{Z}_+$, then the number elements of order d in G is divisible by $\varphi(d) = |U(d)|$.*

Theorem 20.11. *If G is a cyclic group, then $G \cong \mathbb{Z}$ if $|G| = \infty$ or $G \cong \mathbb{Z}_n$ if $n := |G| < \infty$.*

Proof. Let $a \in G$ be a generator. If $|G| = \infty$, then $\varphi : \mathbb{Z} \to G$ defined by $\varphi(k) := a^k$ is an isomorphism of groups. If $|G| = n < \infty$, then $\varphi : \mathbb{Z}_n \to G$ again defined by $\varphi(k) := a^k$ is an isomorphism of groups. ■

Theorem 20.12 (Fundamental Theorem of Cyclic Groups). *Suppose that $G = \langle a \rangle$ is a cyclic group.*

1. *The subgroups of G are all of the form, $H = \langle a^m \rangle$ for some $m \in \mathbb{Z}$.*
2. *If $n = |a| < \infty$ and $H \leq G$, then $m := |H| \, | n$ and $H = \langle a^{n/m} \rangle$.*

3. *To each divisor, $k \geq 1$, of n there is precisely one subgroup of G of order k, namely $H = \left\langle a^{n/k} \right\rangle$.*

Proposition 20.13. *If $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ is a homomorphisms, then $\varphi = \varphi_k$ for some $k \in \left\langle \frac{m}{\gcd(m,n)} \right\rangle$ where $\varphi_k(x) = kx \ (= kx \bmod m)$. The list of distinct homomorphisms from $\mathbb{Z}_n \to \mathbb{Z}_m$ is given by,*

$$\left\{ \varphi_k : k \in \left\langle \frac{m}{\gcd(m,n)} \right\rangle \text{ with } 0 \leq k < \frac{m}{\gcd(m,n)} \right\}.$$

Moreover,

$$\operatorname{Ran}(\varphi_k) = \varphi(\mathbb{Z}_n) = \langle k \rangle = \langle \gcd(m,k) \rangle \leq \mathbb{Z}_m \text{ and}$$
$$\ker(\varphi) = \left\langle |k|_{\mathbb{Z}_m} \right\rangle = \left\langle \frac{m}{\gcd(k,m)} \right\rangle \leq \mathbb{Z}_n.$$

Corollary 20.14. *If $m, n \in \mathbb{Z}_+$ are relatively prime there is only one homomorphism, $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$, namely the zero homomorphism.*

Theorem 20.15. *Let $(g_1, \ldots, g_n) \in G_1 \oplus \cdots \oplus G_n$, then*

$$|(g_1, \ldots, g_n)| = \operatorname{lcm}(|g_1|, \ldots, |g_n|).$$

Theorem 20.16. *Suppose that G and H are cyclic groups of finite order, then $G \oplus H$ is cyclic iff $|G|$ and $|H|$ are relatively prime.*

Corollary 20.17. *Suppose that G_i is cyclic for each i, then $G_1 \oplus \cdots \oplus G_n$ is cyclic iff $|G_i|$ and $|G_j|$ are relatively prime for all $i \neq j$.*

20.1 Examples:

Example 20.18. Show all non-trivial subgroups, H, of $\mathbb{Z}$ are isomorphic to $\mathbb{Z}$. **Solution:** from class we know that $H = \langle n \rangle$ for some $n \neq 0$. Now let $\varphi(x) := nx$ for $x \in \mathbb{Z}$. Then φ is a homomorphism, $\ker \varphi = \{0\}$ and $\varphi(\mathbb{Z}) = \langle n \rangle$, so φ is an isomorphism.

Example 20.19. Write out all of the (left) cosets of $\langle 4 \rangle \leq \mathbb{Z}$ and compute $[\mathbb{Z} : \langle 4 \rangle]$. Answer, $\langle 4 \rangle = 0 + \langle 4 \rangle, 1 + \langle 4 \rangle, 2 + \langle 4 \rangle, 3 + \langle 4 \rangle$ – this is it. Why? well these are all distinct since $i + \langle 4 \rangle$ is the only coset containing i for $0 \leq i \leq 3$. Moreover, you should check that every integer in $\mathbb{Z}$ is in precisely one of these cosets. Thus it follows that $[\mathbb{Z} : \langle 4 \rangle] = 4$.

Example 20.20. Find $[\mathbb{Z}_{12} : \langle 3 \rangle]$. First off recall that $|\langle 3 \rangle| = |3| = \frac{12}{\gcd(3,12)} = \frac{12}{3} = 4$ and hence by Lagrange's theorem,

$$[\mathbb{Z}_{12} : \langle 3 \rangle] = \frac{|\mathbb{Z}_{12}|}{|\langle 3 \rangle|} = \frac{12}{4} = 3.$$

Example 20.21. What are the orders of the elements which occur in the group, $G := \mathbb{Z}_6 \oplus \mathbb{Z}_{10}$. To answer this suppose that $(a,b) \in G$ then we know $|(a,b)| = \operatorname{lcm}(|a|, |b|)$ where $|a| \in \{1,2,3,6\}$, and $|b| \in \{1,2,5,10\}$. Therefore one sees that

$$\begin{aligned} |(a,b)| &\in \{1,2,5,10\} \cup \{2,10\} \cup \{3,6,15,30\} \cup \{6,30\} \\ &= \{1,2,3,5,6,10,15,30\} \end{aligned}$$

are the possible orders.

Let us now compute the number element in G of order 10. This happens if $|a| = 1$ and $|b| = 10$, or $|a| = 2$ and $|b| = 5$ or 10. Noting that $\varphi(10) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4$ it follows that the number of elements of order 10 is: $1 \cdot 4 + 1 \cdot (4 + 4) = 12$.

Example 20.22. Suppose that $\varphi : \mathbb{Z}_8 \to \mathbb{Z}_4$ is a homomorphism such that $\varphi(3) = 1$. Find a formula for φ and then find $\ker(\varphi)$. **Solution:** First off we know that $\langle 3 \rangle = \langle \gcd(8,3) \rangle = \langle 1 \rangle = \mathbb{Z}_8$ (alternatively, $3 \in U(8)$ and is therefore a generator) and therefore 3 is a generator of $\mathbb{Z}_8$. Hence it follows that φ is determined by its value on 3 and since $\varphi(3 \cdot 8) = 1 \cdot 8 = 0 \,(\mathrm{mod})\, 4$, it follows that there is such a homomorphism φ. Since $3 \cdot 3 = 1$ in $\mathbb{Z}_8$ it follows that $\varphi(1) = \varphi(3 \cdot 3) = 3 \cdot \varphi(3) = 3 \cdot 1 = 3$ in $\mathbb{Z}_4$. Therefore,

$$\varphi(x) = \varphi(x \cdot 1) = x \cdot \varphi(1) = 3x \bmod 4.$$

Now $x \in \ker(\varphi)$ iff $3x \bmod 4 = 0$, i.e. iff $4|3x$ iff $4|x$. Thus $\ker(\varphi) = \langle 4 \rangle = \{1,4\} \leq \mathbb{Z}_8$.

Remark 20.23. In general if $k \in U(n)$, then we can find $s, t \in \mathbb{Z}$ by the division algorithm such that $sk + tn = 1$. Taking this equation mod n then allows us to conclude that $k \cdot (s \mod n) = 1$ in $\mathbb{Z}_n$. For example if $n = 8$ and $k = 3$, we have,

$$8 = 2 \cdot 3 + 2 \text{ and } 3 = 2 + 1$$

and therefore

$$1 = 3 - 2 = 3 - (8 - 2 \cdot 3) = 3 \cdot 3 - 8$$

and therefore $3 \cdot 3 = 1$ in $\mathbb{Z}_8$.

Theorem 20.24 ($\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$). *All of the homomorphisms form $\mathbb{Z}_n$ to itself are of the form, $\varphi_k(x) = kx \bmod n$ for some $k \in \mathbb{Z}_n$. Moreover, these φ_k is an isomorphism iff $k \in U(n)$. Moreover the map,*

$$U(n) \ni k \to \varphi_k \in \mathrm{Aut}(\mathbb{Z}_n)$$

is an isomorphism of groups.

21

Lecture 21 (Midterm II) (2/25/2009)

22

Lecture 22 (2/27/2009)

22.1 $U(n)$ groups

Lemma 22.1. *If $k, n \in \mathbb{Z}_+$ and $k|n$, then $\alpha_k : U(n) \to U(k)$ defined by $\alpha_k(x) := x \bmod k$ is a homomorphism.*

Proof. We first must check that $r := \alpha_k(x) \in U(k)$ for all $x \in U(n)$, i.e. that $\gcd(r, k) = 1$. To see this write $x = ak + r$ and observe that if d is a common divisor of both k and r, then d will divide x and n since $k|n$, i.e. d is a common divisor of x and n. But since $x \in U(n)$, x and n are relatively prime and therefore only have 1 as a common divisor. So $d = 1$ and we have shown $\gcd(r, k) = 1$, i.e. $r \in U(k)$.

The fact that it is a homomorphism follows from the basic properties of $\bmod k$ – arithmetic;

$$\alpha_k(xy) = xy \bmod k = (x \bmod k \cdot y \bmod k) \bmod k = \alpha_k(x) \cdot \alpha_k(y).$$

■

If k is not a divisor of n, then the map α_k is not well defined in general. For example, say $k = 3$ and $n = 10$, then

$$U(10) = \{1, 3, 7, 9\}$$

and we have $\alpha_3(3) = 3 \bmod 3 = 0 \notin U(3)$.

Definition 22.2. *For $k, n \in \mathbb{Z}_+$ with $k > 1$ and $k|n$, let*

$$U_k(n) := \ker(\alpha_k) = \{x \in U(n) : x \bmod k = 1\} \leq U(n).$$

Example 22.3. If $n = 10$, then $U(10) = \{1, 3, 7, 9\}$ and

$$U_2(10) = U(10) \text{ while } U_5(10) = \{1\}.$$

(On the other hand, $U_3(10) = \{1, 7\}$ which is not a subgroup since $7^2 = 49 = 9$.)

Example 22.4. If $n = 30 = 2 \cdot 3 \cdot 5$, then $U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$,

$$\begin{aligned}
U_2(30) &= U(30), \\
U_3(30) &= \{1, 7, 13, 19\}, \\
U_5(30) &= \{1, 11\}, \\
U_6(30) &= \{1, 7, 13, 19\}, \\
U_{10}(30) &= \{1, 11\}, \\
U_{15}(30) &= \{1\}.
\end{aligned}$$

Further, let $\alpha : U(30) \to U(10)$ be the homomorphism, $\alpha(x) = x \bmod 10$, then restricting α to $U_3(30)$ is given by;

$$\begin{array}{ccc}
 & \alpha|_{U_3(30)} & \\
U_3(30) & \to & U(10) \\
x & \to & x \bmod 10 \\
1 & \to & 1 \\
7 & \to & 7 \\
13 & \to & 3 \\
19 & \to & 9.
\end{array}$$

Notice that $\alpha : U_3(30) \to U(10)$ is an isomorphism. Similarly, if we let $\beta : U(30) \to U(3)$ be the homomorphism, $\beta(x) = x \bmod 3$, then restricting β to $U_{10}(30)$ is given by;

$$\begin{array}{ccc}
 & \beta|_{U_3(10)} & \\
U_{10}(30) & \to & U(3) \\
x & \to & x \bmod 3 \\
1 & \to & 1 \\
11 & \to & 2.
\end{array}$$

Therefore $\beta : U_{10}(30) \to U(3)$ is an isomorphism.

Lemma 22.5. *Suppose that $m, n \geq 2$ are relatively prime, then $U_m(mn) \cap U_n(mn) = \{1\}$.*

Proof. By definition, $x \in U_m(mn) \cap U_n(mn)$ iff $x \bmod m = 1$ and $x \bmod n = 1$, i.e.

$$x = am + 1 \text{ and } x = bn + 1 \text{ for some } a, b \in \mathbb{Z}.$$

From these equations we see that $am = bn$. Hence, $n|am$ and it follows by Euclid's lemma that $n|a$. Thus it follows that $x = \frac{a}{n}nm + 1$ with $a/n \in \mathbb{Z}$, i.e. $x = x \bmod nm = 1$. ■

Proposition 22.6. *Suppose that $m, n \geq 2$ are relatively prime, then $\alpha : U_m(mn) \to U(n)$ defined by $\alpha(x) := x \bmod n$ is an isomorphism.*

Proof. Since $\ker(\alpha) = U_m(mn) \cap U_n(mn) = \{1\}$, it follows that α is one to one. So to finish the proof we must show α is onto, i.e. to each $k \in U(n)$ we have to find an $x \in U_m(mn)$ such that $\alpha(x) = x \bmod n = k$, i.e. $x = qn + k$ for some $0 \leq q < m$. The condition that $x \in U(mn)$ is then,

$$1 = x \bmod m = (qn + k) \bmod m. \tag{22.1}$$

We are now going to finish the proof by solving this equation for q.

1. Since m and n are relatively prime there exists $s, t \in \mathbb{Z}$ such that $sn + tm = 1$. Taking this equation $\bmod m$ and replacing s by $s \mod m$ if necessary, we have found $1 \leq s < m$ such that $sn \bmod m = 1$.

2. Multiplying Eq. (22.1) by s (doing all arithmetic $\bmod m$) implies,

$$s = s(qn + k) = q + sk \text{ in } \mathbb{Z}_m.$$

Solving this equation for q shows that

$$q = s(1 - k) \bmod m. \tag{22.2}$$

3. We now check that $x = qn + k$ with q as in Eq. (22.2) satisfies, $x \in U(mn)$ and $\alpha(x) = x \bmod m = k$. First off, doing all arithmetic in $\mathbb{Z}_m$, we have

$$x = qn + k = s(1 - k)n + k = (1 - k)sn + k = (1 - k) + k = 1,$$

i.e. $x \bmod m = 1$ as desired. So we are only left to check $x \in U(mn)$. Since $k \in U(n)$, it follows that

$$\gcd(x, n) = \gcd(qn + k, n) = \gcd(k, n) = 1.$$

Since $x \bmod m = 1$ we also know that $\gcd(x, m) = 1$. Therefore, because m and n are relatively prime, $\gcd(x, mn) = 1$ by Euclid's lemma, i.e. $x \in U(mn)$. ■

Lemma 22.7. *Suppose that H, K, and G are groups and $\alpha : G \to H$ and $\beta : G \to K$ are homomorphisms, then $\varphi : G \to H \times K$ defined by $\varphi(g) := (\alpha(g), \beta(g))$ is a group homomorphism.*

Proof. *This is a routine check,*

$$\begin{aligned}\varphi(g_1 g_2) &= (\alpha(g_1 g_2), \beta(g_1 g_2)) = (\alpha(g_1)\alpha(g_2), \beta(g_1)\beta(g_2)) \\ &= (\alpha(g_1), \beta(g_1))(\alpha(g_2), \beta(g_2)) = \varphi(g_1)\varphi(g_2).\end{aligned}$$

■

Theorem 22.8. *If $m, n \in \mathbb{Z}_+$ are relatively prime, then $\varphi : U(mn) \to U(m) \times U(n)$ defined by*

$$\varphi(x) := (x \bmod m, x \bmod n)$$

is an isomorphism of groups.

Proof. By Lemma 22.7, φ is a homomorphism. Since

$$\begin{aligned}\ker(\varphi) &= \{x \in U(mn) : x \bmod m = 1 \text{ and } x \bmod n = 1\} \\ &= U_m(mn) \cap U_n(mn) = \{1\},\end{aligned}$$

we know that φ is one to one.

To see that φ is onto, let $(a, b) \in U(m) \times U(n)$. By Lemma **??**, there exists $x \in U_n(mn)$ and $y \in U_m(mn)$ such that $x \bmod m = a$ and $y \bmod n = b$. Then $xy \in U(mn)$ and

$$\begin{aligned}\varphi(xy) &= \varphi(x)\varphi(y) = (x \bmod m, x \bmod n)(y \bmod m, y \bmod n) \\ &= (a, 1)(1, b) = (a, b).\end{aligned}$$

■

Corollary 22.9. *If $m, n \in \mathbb{Z}_+$ are relatively prime, then $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.*

Corollary 22.10. *If $n \in \mathbb{Z}_+$ factors as $n = p_1^{n_1} \dots p_k^{n_k}$ with $\{p_i\}_{i=1}^k$ being distinct primes, then*

$$\varphi(n) = \prod_{i=1}^k \left(p_i^{n_i} - p_i^{n_i - 1}\right) = \prod_{i=1}^k p_i^{n_i - 1}(p_i - 1).$$

Fact 22.11 *Carl Gauss proved in 1801 that*

$$\begin{aligned}&U(p^n) \cong \mathbb{Z}_{p^n - p^{n-1}} \text{ if } p \text{ is an odd prime, and} \\ &U(2) \cong \{1\}, \quad U(4) = \{1, 3\} \cong \mathbb{Z}_2, \text{ while,} \\ &U(2^n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-2}} \text{ for } n \geq 3.\end{aligned}$$

*The only cyclic U – groups are the ones appearing in first two rows of the above list – $U(n)$ is **not** cyclic for all other n. Recall from Exercise 4.56 that it was shown that $U(2^n)$ has two distinct elements of order 2 and therefore we already know that $U(2^n)$ is **not** cyclic for $n \geq 3$.*

22.2 Public Key Encryption

Let us briefly explain the algorithm for sending "public key" encrypted messages. For the input to this scheme, the **receiver of the message prepares**:

1. two (large) distinct primes p and q.
   Let $n := pq$ and observe that
   $$U(n) = U(p) \oplus U(q) \cong \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{q-1}. \tag{22.3}$$
2. Compute $m := \operatorname{lcm}(p-1, q-1)$ which is the maximal possible order of any element in $U(n)$ because of Eq. (22.3).
3. Choose any $r \in U(m)$ other than 1, for example $r = m - 1$ would work.
4. Tell the sender publicly to send her/his message, M, encrypted as $R := M^r \bmod n$. The message M should be a number in $\{1, 2, \dots, \min(p, q) - 1\}$. This latter condition ensures that $\gcd(M, n) = \gcd(M, pq) = 1$, i.e. $M \in U(n)$.

The sender now sends his/her message, M, as $R := M^r \bmod n$. When the receiver gets the encrypted message, R, he/she uses the following algorithm to decode R back to the original message, M.

1. Compute $s := r^{-1} \in U(m)$. (This can be done by the division algorithm for finding $s, t \in \mathbb{Z}$ such that $sr + tm = 1$.)
2. Observe that $R = M^r$ as computed in $U(n)$. Since (as we have seen above) $|M|\,|m$, it follows that
   $$R^s = M^{rs} = M^{rs \mod m} = M^1 = M.$$
   Thus we may recover the original message, M, from the encrypted message R, via
   $$M = R^s \bmod n. \tag{22.4}$$

See the text book for an explicit example of the procedure in action.

22.3 Extras (This section may be safely skipped)

Remark 22.12. Here is alternative proof of the assertion in Theorem 22.8 that $U(mn) \cong U(m) \times U(n)$ when m and n are relatively prime.

Recall that if $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, then $k := |(a, b)| = \operatorname{lcm}(|a|, |b|)$ where
$$|a| = \frac{m}{\gcd(m, a)} \text{ and } |b| = \frac{n}{\gcd(n, b)}.$$
Since any common divisor of $|a|$ and $|b|$ would have to be a common divisor of m and n, we also know $\gcd(|a|, |b|) = 1$. Therefore,
$$|a| \cdot |b| = \operatorname{lcm}(|a|, |b|) \cdot \gcd(|a|, |b|) = \operatorname{lcm}(|a|, |b|) = |(a, b)|$$
for all $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$.

If $|(a, b)| = |a|\,|b|$ divides m, then we must have $|b|$ divides m as well. However, $|b|$ divides n and therefore is a common divisor of m and n and is therefore equal to 1 and we must have $b = 0$. Thus the only homomorphisms from $\mathbb{Z}_m \to \mathbb{Z}_m \times \mathbb{Z}_n$ are of the form, $\alpha(x) = (kx, 0)$ for some $k \in \mathbb{Z}_m$. So according to Lemma 22.13 below, if $\varphi : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_n$ is a homomorphism, then $\varphi(x, y) = (kx, ly)$ for some $(k, l) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Furthermore, such a φ is an isomorphism iff $k \in U(m)$ and $l \in U(n)$. Thus we have shown,
$$U(m) \times U(n) \cong \operatorname{Aut}(\mathbb{Z}_m \times \mathbb{Z}_n).$$
On the other hand since m and n are relatively prime, we know that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ and therefore $\operatorname{Aut}(\mathbb{Z}_m \times \mathbb{Z}_n) \cong \operatorname{Aut}(\mathbb{Z}_{mn}) \cong U(mn)$. Thus we may conclude,
$$U(m) \times U(n) \cong \operatorname{Aut}(\mathbb{Z}_m \times \mathbb{Z}_n) \cong \operatorname{Aut}(\mathbb{Z}_{mn}) \cong U(mn).$$

The next lemma appeared on the second midterm.

Lemma 22.13. *Suppose that G_1, G_2 and G are groups and $\varphi : G_1 \times G_2 \to G$ is a homomorphism. Then $\alpha(g_1) := \varphi(g_1, e)$ and $\beta(g_2) := \varphi(e, g_2)$ are homomorphisms from $G_1 \to G$ and $G_2 \to G$ respectively. Moreover the elements of $\alpha(G_1)$ commute with all of the elements of $\beta(G_2)$. Conversely if $\alpha : G_1 \to G$ and $\beta : G_2 \to G$ are homomorphisms such that the elements of $\alpha(G_1)$ commute with all of the elements of $\beta(G_2)$, then $\varphi(g_1, g_2) := \alpha(g_1)\beta(g_2)$ is a homomorphism from $G_1 \times G_2 \to G$. (See Proposition 22.14 above as well.)*

Proof. Observe that
$$\alpha(g_1 g_1') = \varphi(g_1 g_1', e) = \varphi((g_1, e)(g_1', e)) = \varphi(g_1, e)\varphi(g_1', e) = \alpha(g_1)\alpha(g_1')$$
showing $\alpha : G_1 \to G$ is a homomorphism. Furthermore,
$$\begin{aligned}\alpha(g_1)\beta(g_2) &= \varphi(g_1, e)\varphi(e, g_2) = \varphi((g_1, e)(e, g_2)) = \varphi((g_1, g_2)) \\ &= \varphi((e, g_2)(g_1, e)) = \varphi(e, g_2)\varphi(g_1, e) = \beta(g_2)\alpha(g_1)\end{aligned}$$
which proves the commutativity property. It is easy to check that $\varphi(g_1, g_2) := \alpha(g_1)\beta(g_2)$ is a homomorphism. ■

In this extra section, we will put the proof of Theorem 22.8 into a more general context.

Proposition 22.14. *Suppose that G, H, and K, are groups. Then G is isomorphic to $H \times K$ iff there exists homomorphisms, $\varphi : G \to H$ and $\psi : G \to K$ such that $\ker\varphi \cap \ker\psi = \{e\}$ and $\varphi(\ker\psi) = H$ and $\psi(\ker\varphi) = K$.*

Proof. Suppose that $\eta : G \to H \times K$ is an isomorphism of groups. Since the projection maps on $H \times K$ are homomorphism, it follows that $\eta = (\varphi, \psi)$ where $\varphi : G \to H$ and $\psi : G \to K$ are homomorphisms. Moreover, $\{e\} = \ker \eta = \ker \varphi \cap \ker \psi$ and since η is surjective, for each $h \in H$ there exists a $g \in G$ such that $(h, e) = \eta(g) = (\varphi(g), \psi(g))$. Thus we see that $g \in \ker \psi$ and $\varphi(g) = h$ showing $\varphi(\ker \psi) = H$. Similarly we may show $\psi(\ker \varphi) = K$.

Conversely, suppose that $\varphi : G \to H$ and $\psi : G \to K$ such that $\ker \varphi \cap \ker \psi = \{e\}$ and $\varphi(\ker \psi) = H$ and $\psi(\ker \varphi) = K$ and define $\eta := (\varphi, \psi) : G \to H \times K$. It is easily checked that η is a homomorphism and the $\ker \eta = \ker \varphi \cap \ker \psi = \{e\}$. Now suppose that $(h, k) \in H \times K$ and choose $a \in \ker \psi$ and $b \in \ker \varphi$ such that $\varphi(a) = h$ and $\psi(b) = k$. Then letting $g := ab$, we find

$$\varphi(g) = \varphi(ab) = \varphi(a)\varphi(b) = he = h \text{ and}$$
$$\psi(g) = \psi(ab) = \psi(a)\psi(b) = ek = k.$$

This shows that $\eta(g) = (h, k)$ and hence shows that η is surjective. ■

Lemma 22.15 (Number Theoretic). *Suppose that $s, t \in \mathbb{Z}_+$. Then $a \bmod st = b \bmod st$ implies $a \bmod s = b \bmod s$ and $a \bmod t = b \bmod t$. Moreover if $\gcd(s, t) = 1$, we have $a \bmod st = b \bmod st$ iff $a \bmod s = b \bmod s$ and $a \bmod t = b \bmod t$.*

Proof. First off $a \bmod st = b \bmod st$ iff $st|(a-b)$, $a \bmod s = b \bmod s$ iff $s|(a-b)$ and $a \bmod t = b \bmod t$ iff $t|(a-b)$. Since it is clear that $s|(a-b)$ and $t|(a-b)$ if $st|(a-b)$ the first assertion is proved. Moreover if $\gcd(s,t) = 1$, and $s|(a-b)$ and $t|(a-b)$, then $a - b = ks$ and $t|ks$. By Euclid's lemma, this implies that $t|k$ and therefore, $a - b = \frac{k}{t} st$, i.e. $st|(a-b)$ so that $a \bmod st = b \bmod st$. (Alternatively, use the fundamental theorem of arithmetic to prove the second assertion.) ■

Lemma 22.16. *Let $a, b, c \in \mathbb{Z}_+$, then $\gcd(a, bc) = 1$ iff $\gcd(a, b) = 1 = \gcd(a, c)$.*

Proof. This is easily proved with the aid of the fundamental theorem of arithmetic. Alternatively, it is clear that $\gcd(a, b)$ and $\gcd(a, c)$ are divisors of both a and bc and therefore if either of these is greater than 1 it would follows that $\gcd(a, bc) > 1$. Conversely if $\gcd(a, b) = 1 = \gcd(a, c)$, there would exists $s, t, u, v \in \mathbb{Z}$ such that $sa + tb = 1$ and $ua + vc = 1$. Hence it follows that

$$1 = 1^2 = (sa + tb)(ua + vc).$$

Taking this equation $\bmod a$ then implies, $1 = (tvbc) \bmod a$ from which it follows that $\gcd(a, bc) = 1$. ■

Lemma 22.17. *For all $a, b \in \mathbb{Z}_+$ we have $(x \bmod ab) \bmod a = x \bmod a$.*

Proof. Let $r := x \bmod ab$ and write $x = kab + r$. Then

$$x \bmod a = (kab + r) \bmod a = r \bmod a = (x \bmod ab) \bmod a.$$

■

Theorem 22.18. *Suppose that $m, n \geq 2$ and $\gcd(m, n) = 1$. Then*

$$U(mn) \ni x \to (x \bmod m, x \bmod n) \in U(m) \times U(n)$$

is an isomorphism. In particular, $\varphi(mn) := |U(mn)| = \varphi(m) \cdot \varphi(n)$. (See Remark 22.12 for another proof which is perhaps better!)

Proof. From Lemma 22.16, we know that $\gcd(x, mn) = 1$ implies $\gcd(x, m) = 1$ and $\gcd(x, n) = 1$. Thus if $x \in U(mn)$ and $r := x \bmod n$, we will have $x = kn + r$ and hence $1 = \gcd(x, n) = \gcd(x, r)$. Therefore we may define maps, $\varphi : U(mn) \to U(m)$ and $\psi : U(mn) \to U(n)$ via, $\varphi(x) = x \bmod m$ and $\psi(x) = x \bmod n$. Notice that both of these maps are homomorphisms. Indeed,

$$\begin{aligned} \varphi(xy) &= (xy \bmod mn) \bmod n = xy \bmod n \\ &= (x \bmod n \cdot y \bmod n) \bmod n = \varphi(x)\varphi(y) \end{aligned}$$

as desired.

Now $\varphi(x) = 1$ iff $x \bmod n = 1$ and $\psi(x) = 1$ iff $x \bmod m = 1$. Therefore $x \in \ker \varphi \cap \ker \psi$ iff $n|(x-1)$ and $m|(x-1)$. As $\gcd(m, n) = 1$, it follows by Euclid's lemma that $mn|(x-1)$ as well, i.e. $x \bmod mn = 1$ and we have shown $\ker \varphi \cap \ker \psi = \{1\}$. As before we denote $\ker \varphi$ by $U_n(mn)$ and $\ker \psi$ by $U_m(mn)$. To finish the proof we must now show $\psi(U_n(mn)) = U(m)$ and $\varphi(U_m(mn)) = U(n)$.

Let $0 \leq k < n$ and choose $1 \leq s < m$ such that $sn \bmod m = 1$ which is possible since $\gcd(m, n) = 1$. We claim there is an $q \in \mathbb{Z}$ such that $(qn + k) \bmod m = 1$. If such a q exists we must have,

$$s = [s(qn + k)] \bmod m = [q + sk] \bmod m$$

which is to say $q = s(1 - k) \bmod m$. Conversely if we take $q := s(1 - k) \bmod m$, then

$$(qn + k) \bmod m = (sn(1 - k) + k) \bmod m = ((1 - k) + k) \bmod m = 1.$$

With this fact in hand, we see that for all $k \in U(n)$ we can find a $0 \leq q < m$ such that $(qn + k) \bmod m = 1$. Thus if we let $x := qn + k$, we will have $x \bmod m = 1$ so that $\gcd(x, m) = 1$ and $x \bmod n = k$ so that $\gcd(x, n) = \gcd(k, n) = 1$ and therefore $\gcd(x, mn) = 1$. Thus $g := x \bmod mn$ satisfies, $\gcd(g, mn) = 1$, i.e. $g \in U(mn)$. Moreover,

$$\varphi(g) = g \bmod n = [(qn+k) \bmod mn] \bmod n = (qn+k) \bmod n = k$$

and

$$\psi(g) = g \bmod m = [(qn+k) \bmod mn] \bmod m = (qn+k) \bmod m = 1.$$

Thus we have shown $\varphi(\ker\psi) = U(n)$. Similarly we may show $\psi(\ker\varphi) = U(m)$. The result now follows by an application of Proposition 22.14. ■

22.4 Permutation Groups

The following proposition should be verified by the reader.

Proposition 22.19 (Permutation Groups). *Let Λ be a set and*

$$S(\Lambda) := \{\sigma : \Lambda \to \Lambda | \ \sigma \text{ is bijective}\}.$$

If we equip G with the binary operation of function composition, then G is a group. The identity element in G is the identity function, ε, and the inverse, σ^{-1}, to $\sigma \in G$ is the inverse function to σ.

Definition 22.20 (Finite permutation groups). *For $n \in \mathbb{Z}_+$, let $\Lambda_n := \{1, 2, \dots, n\}$, and $S_n := S(\Lambda_n)$ be the group described in Proposition 22.19. We will identify elements, $\sigma \in S_n$, with the following $2 \times n$ array,*

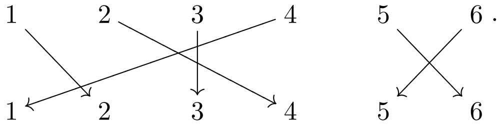
$$\begin{bmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{bmatrix}.$$

For examples, suppose that $n = 6$ and let

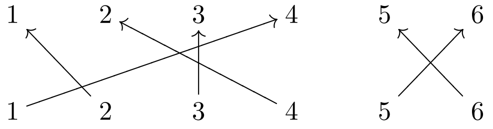
$$\varepsilon = \begin{bmatrix} 1\,2\,3\,4\,5\,6 \\ 1\,2\,3\,4\,5\,6 \end{bmatrix} \text{ – the identity, and}$$

$$\sigma = \begin{bmatrix} 1\,2\,3\,4\,5\,6 \\ 2\,4\,3\,1\,6\,5 \end{bmatrix}.$$

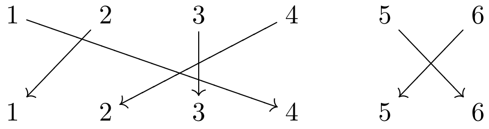
We identify σ with the following picture,



The inverse to σ is gotten pictorially by reversing all of the arrows above to find,



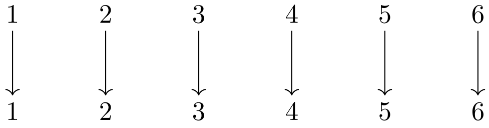
or equivalently,



and hence,

$$\sigma^{-1} = \begin{bmatrix} 1\,2\,3\,4\,5\,6 \\ 4\,1\,3\,2\,6\,5 \end{bmatrix}.$$

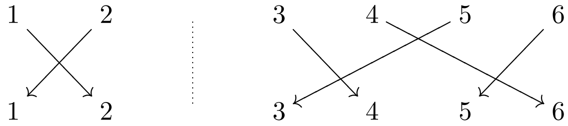
Of course the identity in this graphical picture is simply given by



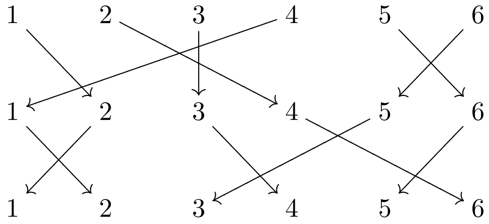
Now let $\beta \in S_6$ be given by

$$\beta = \begin{bmatrix} 1\,2\,3\,4\,5\,6 \\ 2\,1\,4\,6\,3\,5 \end{bmatrix},$$

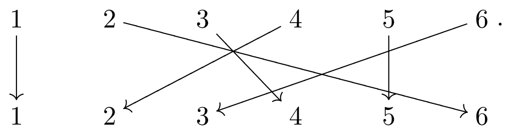
or in pictures;



We can now compose the two permutations $\beta \circ \sigma$ graphically to find,



which after erasing the intermediate arrows gives,



In terms of our array notation we have,

$$\begin{aligned}\beta\circ\sigma &= \begin{bmatrix}1\,2\,3\,4\,5\,6\\2\,1\,4\,6\,3\,5\end{bmatrix}\circ\begin{bmatrix}1\,2\,3\,4\,5\,6\\2\,4\,3\,1\,6\,5\end{bmatrix}\\ &= \begin{bmatrix}1\,2\,3\,4\,5\,6\\1\,6\,4\,2\,5\,3\end{bmatrix}.\end{aligned}$$

It is also worth observing that β splits into a product of two permutations,

$$\begin{aligned}\beta &= \begin{bmatrix}1\,2\,3\,4\,5\,6\\2\,1\,3\,4\,5\,6\end{bmatrix}\begin{bmatrix}1\,2\,3\,4\,5\,6\\1\,2\,4\,6\,3\,5\end{bmatrix}\\ &= \begin{bmatrix}1\,2\,3\,4\,5\,6\\1\,2\,4\,6\,3\,5\end{bmatrix}\begin{bmatrix}1\,2\,3\,4\,5\,6\\2\,1\,3\,4\,5\,6\end{bmatrix},\end{aligned}$$

corresponding to the non-crossing parts in the graphical picture for β. Each of these permutations is called a "cycle."

Lemma 22.21. *Suppose that $\sigma\in S_n$ and $1\le x\le n$, then there exists $k\ge 1$ such that $\sigma^k(x)=x$. Let $k(x)\ge 1$ be the minimal such k, then*

$$O_x(\sigma) := \left\{x,\sigma(x),\dots,\sigma^{k(x)-1}(x)\right\}$$

*are distinct element in Λ_n. We call $O_x(\sigma)$ the **orbit of** x under σ.*

Proof. As Λ_n is a finite set, it follows that $\{\sigma^m(x)\}_{m=0}^{\infty}$ are not all distinct elements and therefore $\sigma^m(x)=\sigma^l(x)$ for some $l<m$ and therefore, $\sigma^k(x)=x$ where $k=m-l\ge 1$.

Now let $k=k(x)$ be the minimal $k\ge 1$ such that $\sigma^k(x)=x$. if $\left\{x,\sigma(x),\dots,\sigma^{k(x)-1}(x)\right\}$ were not all distinct, then $\sigma^i(x)=\sigma^j(x)$ for some $0\le i<j\le k-1$ and it would follows that $\sigma^{j-i}(x)=x$ with $1\le j-i<k-1$ which would violate the definition of $k(x)$. ■

Definition 22.22. *Given $\sigma\in S_n$ and $x\in\Lambda_n$, we say $O_x(\sigma)$ is trivial if $O_x(\sigma)=\{x\}$, i.e. $\sigma(x)=x$. Further let*

$$F_\sigma := \{x\in\Lambda_n : O_x(\sigma)=x\} = \{x\in\Lambda_n : \sigma(x)=x\}$$

*be the **fixed points** of σ.*

Example 22.23. If $\sigma=\begin{bmatrix}1\,2\,3\,4\,5\,6\\2\,4\,3\,1\,6\,5\end{bmatrix}$ then the orbits of σ are,

$$\begin{aligned}&O_1=\{1,2,4\}=O_2=O_4,\\ &O_3=\{3\}\ \text{ and}\\ &O_5=\{5,6\}=O_6.\end{aligned}$$

Notice that the orbits have partitioned Λ_6 into disjoint sets. In this case $F_\sigma=\{3\}$. Also observe that the action of σ on each of the orbits is rather simple. For example the action of σ restricted to O_1 may be summarized by; $1\to 2\to 4\to 1$. In fact we may summarize the action of σ via the rules,

$$1\to 2\to 4\to 1;\quad 3\to 3,\quad \text{ and } 5\to 6\to 5.$$

We write this as,

$$\sigma=(124)\,(3)\,(56)\,.$$

Definition 22.24. *An element $\sigma\in S_n$ is said to be a **cycle** if it has at most one non-trivial orbit. Alternatively put, for all $x\notin F_\sigma$, $O_x(\sigma)=\Lambda_n\setminus F_\sigma$.*

Notation 22.25 *If $\sigma\ne\varepsilon$ is a cycle and x is any element in the non-trivial orbit of σ, then we abbreviate σ by,*

$$\sigma=\left(x,\sigma(x),\dots,\sigma^{k-1}(x)\right)$$

where k is the first time that $\sigma^k(x)=x$.

Theorem 22.26. *Every permutation, σ, may be written as a product of disjoint cycles which are unique modulo order. Since they all commute, the ordering of the cycles in this product is irrelevant.*

Example 22.27. For example,

$$\begin{bmatrix}1\,2\,3\,4\,5\,6\\2\,4\,3\,1\,6\,5\end{bmatrix}=(124)\,(3)\,(56)=(124)\,(56)=(56)\,(124)$$

and

$$\begin{bmatrix}1\,2\,3\,4\,5\,6\\3\,1\,2\,6\,4\,5\end{bmatrix}=(132)\,(465)=(465)\,(132)\,.$$

Lemma 22.28. *If σ is written a product of disjoint cycles, $\sigma_1,\dots,\sigma_k$, then $|\sigma|=\operatorname{lcm}(|\sigma_1|,\dots,|\sigma_k|)$.*

Proof. Let $t\in\mathbb{Z}_+$ such that $\sigma^t=\varepsilon$, then

$$\varepsilon=\sigma^t=(\sigma_1\dots\sigma_k)^t=\sigma_1^t\dots\sigma_k^t$$

which can only happen if $\sigma_i^t=\varepsilon$ for each i (why?). Therefore $|\sigma_i|\,|t$ for all i, i.e. t is a common multiple of $|\sigma_1|,\dots,|\sigma_k|$. Therefore the order of σ is the least common multiple of $|\sigma_1|,\dots,|\sigma_k|$. (This also could be proved by induction with the aid of Lemmas **??**, **??**, and Corollary 13.2.) ■