

Subgroups of \mathbf{Z} and of \mathbf{Z}_m
Math 100A UCSD Fall 2001

In this handout, we classify the subgroups of \mathbf{Z} and \mathbf{Z}_m . For every integer n , $n\mathbf{Z}$ is a subgroup of \mathbf{Z} and $n\mathbf{Z}_m = \{n\bar{k} : \bar{k} \in \mathbf{Z}_m\}$ is a subgroup of \mathbf{Z}_m . For example, the subgroup of \mathbf{Z}_{10} additively generated by 4 is

$$4\mathbf{Z}_{10} = \{4, 8, 12, 16, 0\} = \{4, 8, 2, 6, 0\} = \{0, 2, 4, 6, 8\}.$$

Theorem 1. *Every subgroup of \mathbf{Z} has the form $n\mathbf{Z}$ for a unique integer $n \geq 0$.*

Proof. The main idea is this: in the subgroup $n\mathbf{Z}$ for $n > 0$, n is the least positive element. Therefore if we want to prove an arbitrary nontrivial subgroup $H \subset \mathbf{Z}$ has the form $n\mathbf{Z}$, we should define n as the least positive element of H . First we need to show H has a positive element at all.

Let $H \subset \mathbf{Z}$ be a subgroup. If $H = \{0\}$, then $H = n\mathbf{Z}$ for $n = 0$. Assume now that $H \neq \{0\}$, so H contains a nonzero integer, say a . Since H is closed under negation, $-a \in H$. One of a or $-a$ is positive, so H contains a positive integer. Therefore H contains a *least* positive integer, say n . We will prove $H = n\mathbf{Z}$.

Since $n \in H$, closure of H under addition and negation implies $n\mathbf{Z} \subset H$. For the reverse inclusion, pick $h \in H$. To show $h \in n\mathbf{Z}$, we want to show $n|h$. Let's use the division algorithm, with division by n (not by h . why?). For some integers q and r ,

$$h = nq + r, \quad 0 \leq r < n.$$

Since $h \in H$ and $nq \in n\mathbf{Z} \subset H$, we have

$$r = h - nq \in H.$$

The inequalities $0 \leq r < n$ and the minimality of n among the positive integers in H imply $r = 0$. Therefore $h = nq \in n\mathbf{Z}$ and we have $H = n\mathbf{Z}$.

Concerning the uniqueness of n , note that within the subgroup $n\mathbf{Z}$ for $n > 0$, we can characterize n as the least positive element. Therefore n is uniquely determined by $n\mathbf{Z}$ (even when $n = 0$, for obvious reasons). \square

Corollary 1. *Fix a positive integer m . The subgroups of \mathbf{Z} satisfying*

$$m\mathbf{Z} \subset H \subset \mathbf{Z}$$

are precisely the subgroups $d\mathbf{Z}$ where $d|m, d > 0$.

Proof. If $d|m$, say $m = dk$, then $m\mathbf{Z} \subset d\mathbf{Z} \subset \mathbf{Z}$. Conversely, if $m\mathbf{Z} \subset H \subset \mathbf{Z}$, then we know by Theorem 1 that $H = n\mathbf{Z}$ for some $n > 0$. Since $m \in m\mathbf{Z} \subset H = n\mathbf{Z}$, we see that $m \in n\mathbf{Z}$, so $n|m$. Write n as d , so $H = d\mathbf{Z}$ and $d|m, d > 0$. \square

Theorem 2. *For integers a and b , $a|b$ if and only if $a\mathbf{Z} \supset b\mathbf{Z}$.*

Proof. If $a|b$, then $b = ak$ for an integer k . Thus $br = a(kr)$ for any integer r , so $b\mathbf{Z} \subset a\mathbf{Z}$. Conversely, if $b\mathbf{Z} \subset a\mathbf{Z}$, then $b \in b\mathbf{Z}$ is a multiple of a , say $b = al$. Then $a|b$. \square

In words, the theorem says ‘to divide is to contain.’ Commit this phrase to memory so you don’t think $a|b \Rightarrow a\mathbf{Z} \subset b\mathbf{Z}$ by mistake. Try out a concrete example, like $2\mathbf{Z}$ and $6\mathbf{Z}$. While $2|6$, the multiples of 6 are multiples of 2 (not the other way around), so $6\mathbf{Z} \subset 2\mathbf{Z}$.

Now we classify the subgroups of \mathbf{Z}_m , using the classification of the subgroups of \mathbf{Z} .

Theorem 3. *Fix a positive integer m . Each subgroup of \mathbf{Z}_m has the form $d\mathbf{Z}_m$ for a unique $d|m$, $d > 0$. In particular, in \mathbf{Z}_m every subgroup is cyclic and there is only one subgroup of each possible size, which is itself cyclic.*

Proof. It is clear that, for $d|m$ and $d > 0$, $d\mathbf{Z}_m$ is a subgroup of \mathbf{Z}_m . When $d|m$,

$$da \equiv db \pmod{m} \iff a \equiv b \pmod{m/d},$$

so $\#d\mathbf{Z}_m = m/d$, and therefore the subgroups $d\mathbf{Z}_m$ are distinguished by their size (since we can read off d from the size m/d , as m is of course known).

For example, $2\mathbf{Z}_6 = \{0, 2, 4\}$ has size $6/2 = 3$.

Now we show any subgroup of \mathbf{Z}_m has the desired form. Let $H \subset \mathbf{Z}_m$ be a subgroup. We consider the reduction homomorphism $f: \mathbf{Z} \rightarrow \mathbf{Z}_m$, which sends a to $\bar{a} = a \pmod{m}$. The inverse image $f^{-1}(H)$ is a subgroup of \mathbf{Z} which contains $f^{-1}(0) = m\mathbf{Z}$. By Corollary 1, any subgroup of \mathbf{Z} containing $m\mathbf{Z}$ has the form $d\mathbf{Z}$ where $d|m$ and $d > 0$. That is,

$$d\mathbf{Z} = f^{-1}(H) = \{n \in \mathbf{Z} : n \pmod{m} \in H\}.$$

Since f is surjective, $f(f^{-1}(H)) = H$, and thus

$$H = f(d\mathbf{Z}) = d\mathbf{Z}_m.$$

\square

Note especially that there is a one-to-one correspondence between the subgroups of \mathbf{Z}_m and the subgroups of \mathbf{Z} intermediate between $m\mathbf{Z}$ and \mathbf{Z} . In a sense, the way we get the subgroups of \mathbf{Z}_m is by starting with an inclusion like

$$m\mathbf{Z} \subset d\mathbf{Z} \subset \mathbf{Z}$$

and ‘reducing’ all groups modulo m to get

$$\{\bar{0}\} \subset d\mathbf{Z}_m \subset \mathbf{Z}_m.$$

So the subgroup structure of \mathbf{Z}_m is essentially like the subgroup structure of \mathbf{Z} lying ‘above’ $m\mathbf{Z}$.

For example, the subgroups of \mathbf{Z} containing $6\mathbf{Z}$ are

$$6\mathbf{Z}, 3\mathbf{Z}, 2\mathbf{Z}, \mathbf{Z},$$

which correspond to the subgroups of \mathbf{Z}_6 by reducing all the elements of a subgroup modulo 6:

$$\{0\}, \{3, 0\}, \{2, 4, 0\}, \{1, 2, 3, 4, 5, 0\}.$$

Although every subgroup of \mathbf{Z}_m is cyclic and is generated by a unique positive divisor of m (the trivial group, for instance, corresponds to the positive divisor m : $m\mathbf{Z}_m = \{0\}$), the subgroups do not have to always arise this way. Consider, for instance, the subgroup of \mathbf{Z}_6 generated by 4. Although 4 does not divide 6, we can still consider

$$4\mathbf{Z}_6 = \{4k(\bmod 6) : k \in \mathbf{Z}\},$$

which is certainly a subgroup of \mathbf{Z}_6 . In fact, it equals

$$\{4, 8, 0\} = \{4, 2, 0\} = 2\mathbf{Z}_6,$$

so the group generated by 4 is also the group generated by 2, and 2 *does* divide 6.

Theorem 4. For m a positive integer and j an arbitrary integer,

$$j\mathbf{Z}_m = \gcd(j, m)\mathbf{Z}_m.$$

That is, the subgroup generated additively by \bar{j} is also generated by $\overline{\gcd(j, m)}$.

Proof. Any group containing j contains every multiple of j , and any group containing $\gcd(j, m)$ contains every multiple of $\gcd(j, m)$. Therefore, to prove the equation of the theorem, it suffices to show each of j and $\gcd(j, m)$ is a multiple of the other in the group \mathbf{Z}_m .

Since j is a multiple of $\gcd(j, m)$ in \mathbf{Z} , it is also in \mathbf{Z}_m . The other direction is more interesting: we must explain why $\gcd(j, m)$ is a multiple of j in \mathbf{Z}_m (it certainly usually is not in \mathbf{Z}). By the handout on greatest common divisors, for some $x, y \in \mathbf{Z}$ we have

$$jx + my = \gcd(j, m).$$

Reducing modulo m , we have $\gcd(j, m) \equiv jx \pmod{m}$, so $\gcd(j, m)$ is a multiple of j in \mathbf{Z}_m . \square

For example, in \mathbf{Z}_{15} , the group additively generated by 6 is also the group additively generated by $\gcd(6, 15) = 3$:

$$\{6, 12, 18, 24, 0\} = \{6, 12, 3, 9, 0\} = \{3, 6, 9, 12, 0\} = 3\mathbf{Z}_{15}.$$