# Units in Finite Rings

1. (a) Suppose $ca = 0$. Then by $ab = 1$ we have

\[ c = c \cdot 1 = c(ab) = (ca)b = 0 \cdot b = 0. \]

The same argument holds using $ba = 1$ for the case $ac = 0$.

(b) Using both cases of (a), we get: If $a$ is a unit, then $a$ is not a 0-divisor.

(c) $ar = as$ is equivalent to $a(r - s) = 0$ by the distributive property. Since $a \neq 0$ and $a$ is not a 0-divisor, we conclude that $r - s = 0$ and hence $r = s$. The same argument holds for $sa = ra$.

(d) **Notation:** We will often write $aR$ for the set \( \{ ar | r \in R \} \).

We note that (d) implies that the map sending each $r \in R$ to $ar$ (similarly $ra$) is injective (and surjective by definitions of the sets $aR$ and $Ra$). Therefore all the sets have the same cardinality.

(e) We observe that $c = c(ab) = (ca)b = b$, as desired.

(f) We have shown that if $a \in R$ is a unit, then it is not a 0-divisor. It suffices to show that if $a \neq 0$ is not a 0-divisor, then it is a unit (exercise to the reader: explain why this is enough). Suppose we have such an $a$. We have shown that $aR, Ra \subset R$ and $|aR| = |R| = |Ra|$ and we wish to conclude that $aR = R = Ra$.

(∇) This holds because we assumed $R$ was finite.

Therefore we have solutions to $ax = 1 = ya$ with $x, y \in R$ (since $1 \in R = aR = Ra$). By (e), $x = y$ and therefore $a$ is a unit as desired.

(g) For example, $2 \in \mathbb{Z}$ is neither a unit or 0-divisor. In fact, $\mathbb{Z}$ is an integral domain with only $\pm 1$ as units so almost every element is a counterexample. Observe that the only place the proof breaks is in the conclusion (∇) which fails since $\mathbb{Z}$ is infinite (note that $|2\mathbb{Z}| = |\mathbb{Z}|$ but $2\mathbb{Z} \not\subseteq \mathbb{Z}$).

2. If $n$ is prime, then $(a, n) = 1$ for every non-zero $a \in \mathbb{Z}_n$. Therefore, $ax + nt = 1$ for some $x, t \in \mathbb{Z}$, and hence $ax \equiv 1 \pmod{n}$. Thus $a$ is a unit (since $\mathbb{Z}_n$ is commutative) and so $\mathbb{Z}_n$ is a field.

If $n = rs$ for $1 < r \leq s < n$, then $rs \equiv 0 \pmod{n}$ and so $r \neq 0$ is a 0-divisor and hence not a unit by (a). (Can also use that $(r, n) = r > 1$ and so there are no integer solutions to $rx + tn = 1$ and thus $rx \not\equiv 1 \pmod{n}$ for all $x \in \mathbb{Z}_n$)

## Ring Isomorphisms

3. We note that the since $f$ is a bijection, we know that $f^{-1}$ is a bijection as well. Therefore, we need only show it is a homomorphism. We will demonstrate the additive property as multiplicative follows similarly. Since $f$ is a bijection, for any $c, d \in S$, there are $a, b \in R$ such that $f(a) = c$ and $f(b) = d$. Therefore

\[ f^{-1}(c + d) = f^{-1}(f(a + b)) = a + b = f^{-1}(f(a)) + f^{-1}(f(b)) = f^{-1}(c) + f^{-1}(d) \]
as desired.

4. In each of the following we try to show that an isomorphism cannot exist. Isomorphisms must satisfy two properties: They are bijective maps, and they are homomorphisms. In the below solutions, I simply present one of many ways of concluding that such a map can’t exist between the given objects.

(a) \(|Z_4| \neq |Z_6|\), so there are no bijections between them as sets.

(b) \(|Z_{10} shops 5) = |Z| once again.

(c) Since an isomorphism is a bijection and preserves all algebraic properties, it sometimes is easy to simply show that one side contains elements with a particular property while the other doesn’t. Here we note that \(Z\) has an element \(2 \neq 0\) which is not a unit, while \(Q\) has only units. i.e. one is a field and the other is not.

(d) Once again, \(Z\) is an integral domain, but unlike \(R\), it is not a field.

(e) Sometimes we can count particular elements with a given property. There is only one 0-divisor in \(Z_4\), while there two in \(Z_2 \times Z_2\).

(* Since \(R\) and \(C\) are both fields with the same cardinality, we can’t use any of the easy tricks that we did earlier. Instead we start by showing an important fact:

If \(f : R \rightarrow S\) is an isomorphism, then \(f(1_R) = 1_S\) (exercise to the reader: give an example where this is false when \(f\) is only a homomorphism). Observe that \(f(r) = 1_S\) for some \(r \in R\). Hence, \(f(1_R) = 1_S f(1_R) = f(r) f(1_R) = f(r 1_R) = f(r) = 1_S\).

Note that \(i \in C\) has the property that \(i^4 = i \cdot i \cdot i \cdot i = 1\), but \(i^2 = -1 \neq 1\). Observe that no such number exists in \(R\). Namely, \(\sqrt{-1} = i \notin R\). Therefore, there is no possible choice of \(f(i) \in R\) such that \(f : C \rightarrow R\) is a homomorphism.

3 Identifying Ring Homomorphisms

The idea in both of these problems is to learn about how homomorphisms can be determined by where a small set (sometimes a single element) is mapped.

5. Let’s take \(1 \in Z\) for example. If \(f(1) = a\) and \(f : Z \rightarrow R\) is a homomorphism, then we know exactly where \(f\) maps any \(x \in Z\). This is because \(f(x) = x \cdot f(1)\) where we don’t mean multiplication like \(x \in R\), but instead, add (or subtract if \(x < 0\)) \(f(1)\) \(x\)-many times. e.g. \(f(2) = 2 \cdot f(1) = f(1) + f(1)\).

Therefore the choice of where to send \(1 \in Z\) determines the entire map. This is the idea of using so called generators to describe homomorphisms, which we will talk about more as the course continues.

Back to the problem: where can we send \(f(1)\)? Since \(f(1) = f(1 \cdot 1) = f(1)f(1)\) there are only two choices in \(Z\). If \(f(1) = 1\), we get the identity map (an isomorphism). If \(f(1) = 0\), we get the trivial map (since \(f(x) = x \cdot f(1) = x \cdot 0 = 0\)) which is not an isomorphism.

6. By the above, we note that once again \(1 \in Z_n\) is what we called a generator. Therefore, there is a unique map with \(f(1_{Z_n}) = 1_{Z_n}\) if it is a well-defined homomorphism. What can go wrong? We note that \(0_{Z_m} = f(0_{Z_m}) = f(m \cdot 1_{Z_m}) = m \cdot f(1_{Z_m}) = m \cdot 1_{Z_n} = m\). Therefore, for such a map to be well defined, we need \(n | m\). (Exercise to the reader: show this is sufficient and that this is only non-trivial homomorphism between such rings)