This homework is due by the start of class on Wednesday September 6.

1. **Groups**

Recall that a *group* is a pair $(G, \ast)$ where $G$ is a non-empty set and $\ast$ is an associative binary operation on $G$, $\ast$ has an identity, and every $g \in G$ has an inverse.

(1) Let $G$ be a group and let $e$ be the identity element of $G$. Show that if $g \ast g = e$ for all $g \in G$ then $G$ is abelian.

Let $g, h \in G$. Then $g \ast h \in G$ and so by the assumption

$$(g \ast h) \ast (g \ast h) = e.$$ 

By associativity we can rearrange the product on the left hand side so that

$$g \ast (h \ast g) \ast h = e.$$ 

Note that there is no need for more brackets since $\ast$ is associative. Multiplying from the left by $g$ and from the right by $h$,

$$(g \ast g) \ast (h \ast g) \ast (h \ast h) = g \ast h.$$ 

Since by our assumption $g \ast g = h \ast h = e$,

$$e \ast (h \ast g) \ast e = g \ast h.$$ 

Now $e$ is the identity so that

$$h \ast g = g \ast h.$$ 

So $G$ is abelian.

(2) Let $H$ be an abelian group, where we will write the binary operation on $H$ as $+$ and will write the identity element of $H$ as $0$. For each $h \in H$ we will write $-h$ for the inverse of $h$.

We define a “subtraction” operation $-$ in $H$ by the equation $a - b = a + (-b)$.

Show that

(a) $-(-a) = a$ for all $a$.

It is easy to see that for any two elements $c$ and $d$, $c + d = 0$ if and only if $d = -c$. Now $a + (-a) = 0$ so $-(-a) = a$.

(b) $a - (a - b) = b$ for all $a, b$.

$$b + (a - b) = b + a + (-b) = (b + (-b)) + a = 0 + a = a.$$ 

Each step here is justified either by a definition, or by the associativity and commutativity of $+$. 

Adding \(-(a - b)\) to both sides,
\[
(b + (a - b)) - (a - b) = a - (a - b).
\]

Now
\[
(b + (a - b)) - (a - b) = b + (a - b) + (-a + b) = b + 0 = b,
\]
so
\[
a - (a - b) = b.
\]
\[(c)\] \(-(a - b) = b - a\) for all \(a, b\).

\[
(a - b) + (b - a) = a + (-b) + b + (-a) = (a + (-a)) + (b + (-b)) = 0 + 0 = 0,
\]
so \(b - a = -(a - b)\).

2. Rings

Recall that a ring is a triple \((R, +, \times)\) where + and \(\times\) are binary operations on \(R\), \((R, +)\) is an abelian group, \(\times\) is associative, and we have distributive laws \(a \times (b + c) = (a \times b) + (a \times c)\) and \((a + b) \times c = (a \times c) + (b \times c)\) for all \(a, b, c\). \(R\) is unital if \(\times\) has an identity and is commutative if \(\times\) is commutative.

We will adopt the following conventions: in any ring \(R\), 0 is the identity for + and \(-a\) is the +-inverse of \(a\). In a unital ring 1 is the identity for \(\times\), and if \(a\) has a multiplicative inverse then we write this as \(a^{-1}\).

1. Prove that in any ring \(a \times (-b) = -(a \times b)\) for all \(a, b\).

   We saw already that \(a \times 0 = 0\). By distributivity
   \[
a \times (b + (-b)) = a \times b + a \times (-b),
   \]
   so
   \[
a \times b + a \times (-b) = 0
   \]
   and hence
   \[
a \times (-b) = -(a \times b).
   \]

2. Prove that in any ring \((-a) \times (-b) = a \times b\) for all \(a, b\).

   Using the preceding exercise (and the corresponding version for \((-a) \times b\))
   \[
   (-a) \times (-b) = -((-a) \times b) = -(-a \times b).
   \]
   By an exercise from the groups part \(-(a \times b) = a \times b\).

3. Let \(R\) be a unital ring, and let \(U\) be the set of elements in \(R\) which have a multiplicative inverse. Prove that
   (a) The product of two elements of \(U\) is also in \(U\) (so that \(\times\) is a binary operation on \(U\)).
   Let \(u\) and \(v\) be units. It is easy to check that \(v^{-1} \times u^{-1}\) is a multiplicative inverse for \(u \times v\). Order is important here since \(\times\) many not be commutative.

(b) \((U, \times)\) is a group.
   \(\times\) is a binary operation on \(U\) by what we just proved. 1 is an identity for \(\times\) on \(U\), \(\times\) is associative, and for every \(u \in U\) we see easily that \(u^{-1} \in U\) so that every element has an inverse.

Note: \(U\) is called the group of units of \(R\).
(4) As we mentioned in class, for any $n > 1$ we can define a ring as follows: $R = \{0, 1, \ldots, n - 1\}$ and the $+$ and $\times$ are given by addition and multiplication modulo $n$. Find the units in this ring for $n = 8, 9, 10$.

For $n = 8$ the units are 1, 3, 5, 7. For $n = 9$ the units are 1, 2, 4, 5, 7, 8. For $n = 10$ the units are 1, 3, 7, 9.

(Not for credit) Try and guess a general rule for which number are units in this kind of ring.

In general the units are those $a$ such that $\gcd(a, n) = 1$.

(5) Find a ring in which the product of two nonzero elements is zero.

The ring from the last question for any composite value of $n$ will work.