HW 5 Solutions
Eric Hintikka
April 6, 2014

1. (a)

$$\begin{aligned}
0 \cdot x =& 0 \cdot x + 0 \\
=& 0 \cdot x + (0 \cdot x + -(0 \cdot x)) \\
=& (0 \cdot x + 0 \cdot x) + -(0 \cdot x) \\
=& (0 + 0) \cdot x + -(0 \cdot x) \\
=& 0 \cdot x + -(0 \cdot x) \\
=& 0
\end{aligned}$$

(b)

$$\begin{aligned}
(-1) \cdot x =& (-1) \cdot x + 0 \\
=& (-1) \cdot x + (x + -x) \\
=& ((-1) \cdot x + x) + -x \\
=& ((-1) \cdot x + 1 \cdot x) + -x \\
=& (-1 + 1) \cdot x + -x \\
=& 0 \cdot x + -x \\
=& 0 + -x \\
=& -x
\end{aligned}$$

2. Parts (a) and (b) are straightforward. See the top of page 88 from the text for an explanation of parts (c) and (d).

   (a) $2\mathbb{Z}$

   (b) $20\mathbb{Z}$

   (c) $2\mathbb{Z}$

   (d) $1\mathbb{Z}$

3. Each principal ideal in $\mathbb{Z}_{14}$ can be written as $a\mathbb{Z}_{14}$, where $a \in \mathbb{Z}_{14}$. These are:

$$\begin{aligned}
[0]\mathbb{Z}_{14} =& \{[0]\} \\
[1]\mathbb{Z}_{14} =& \mathbb{Z}_{14} \\
[2]\mathbb{Z}_{14} =& \{[0], [2], [4], [6], [8], [10], [12]\} \\
[3]\mathbb{Z}_{14} =& \mathbb{Z}_{14} \\
[4]\mathbb{Z}_{14} =& \{[0], [2], [4], [6], [8], [10], [12]\} \\
[5]\mathbb{Z}_{14} =& \mathbb{Z}_{14} \\
[6]\mathbb{Z}_{14} =& \{[0], [2], [4], [6], [8], [10], [12]\} \\
[7]\mathbb{Z}_{14} =& \{[0], [7]\} \\
[8]\mathbb{Z}_{14} =& \{[0], [2], [4], [6], [8], [10], [12]\} \\
[9]\mathbb{Z}_{14} =& \mathbb{Z}_{14} \\
[10]\mathbb{Z}_{14} =& \{[0], [2], [4], [6], [8], [10], [12]\} \\
[11]\mathbb{Z}_{14} =& \mathbb{Z}_{14} \\
[12]\mathbb{Z}_{14} =& \{[0], [2], [4], [6], [8], [10], [12]\} \\
[13]\mathbb{Z}_{14} =& \mathbb{Z}_{14}
\end{aligned}$$

Thus, the principal ideals are $\{[0]\}, \{[0],[7]\}, \{[0],[2],[4],[6],[8],[10],[12]\}$, and $\mathbb{Z}_{14}$. Now, we show that there are no ideals in $\mathbb{Z}_{14}$ which are not principal, and hence that the above list actually includes *all* the ideals.

Suppose that $I \subseteq Z_{14}$ is an ideal. Let's say that an element in $\mathbb{Z}_{14}$ is "even" if it can be written as $[a]$, where $0 \leq a < 14$ and a is even, and let's call it odd otherwise. We proceed by considering two cases: (1) I contains a nonzero even element $[a]$; and (2) I does not contain any nonzero even element.

In the first case, we can show that I also contains $[2]$. Though there is a somewhat more generalizable argument that could be made, we instead show this by brute force, as follows: if $[a] = [2]$, then obviously $[2] \in I$. If $[a] = [4]$, then $[2] = [4][a] \in I$. If $[a] = [6]$, then $[2] = [5][a] =\in I$. If $[a] = [8]$, then $[2] = [2][a] \in I$. If $[a] = [10]$, then $[2] = [3][a] \in I$. Finally, if $[a] = [12]$, then $[2] = [6][a] \in I$. Then, it is clear that $\{[0],[2],[4],[6],[8],[10],[12]\} \subseteq I$, since I must contain all multiples of $[2]$. Now, if I contains no odd elements, then $I = \{[0],[2],[4],[6],[8],[10],[12]\}$, so I is principal. If I contains an odd element $[b]$, then I must contain $[b]+[2], [b]+[4], [b]+[6]$, etc., which give all of the odd elements, so $I = \mathbb{Z}_{14}$ and hence I is principal.

In the second case, we can show that I must not contain any odd element other than $[7]$. This is because if $[b]$ is an odd element of $\mathbb{Z}_{14}$ and $[b] \neq [7]$, then b is relatively prime with 14, so by the theorem on page 90 $[b]$ generates $\mathbb{Z}_{14}$, and hence $I = \mathbb{Z}_{14}$. This is a contradiction, since we are working in the case where I contains no nonzero even elements. So, the only odd element that I can contain here is $[7]$. Note that since I is an ideal it is a subgroup of $(\mathbb{Z}_{14}, +)$, so it must contain the additive identity element $[0]$. Thus, either $I = \{[0]\}$ or $I = \{[0],[7]\}$. These are both principal ideals.

So, in either case it must be that I is principal, which means that there are no nonprincipal ideals. Hence the list of principal ideals that we gave earlier is in fact a complete list of ideals in $\mathbb{Z}_{14}$.

4. Suppose that there are finitely many primes. Then for some $n \in \mathbb{N}$ we can let $p_1, \ldots, p_n$ be a complete list of primes. Since $p_1 \cdots p_n + 1$ is a natural number greater than 1, it must have a prime factorization. Hence there is some prime number p such that $p | p_1 \cdots p_n + 1$. But for every $i \in \{1, 2, \ldots, n\}$ we can see that $p_i \not| p_1 \cdots p_n + 1$, since $p_1 \cdots p_n + 1 = p_i(p_1 \cdots p_{i-1} \cdot p_{i+1} \cdots p_n + \frac{1}{p_i})$, and the value inside the parentheses is not an integer. Hence $p \neq p_i$ for any $i \in \{1, 2, \ldots, n\}$. That is, our list of primes was not a complete one. So, we have arrived at a contradiction, which means that our assumption must have been false; that is, there must be infinitely many primes.

5. Choose a prime number p and an integer n. The only positive divisors of p are 1 and p (since p is prime), and it follows that $\gcd(p, n)$ must be either 1 or p, since $\gcd(p, n)$ must be a divisor of p. But, if $\gcd(p, n) = p$, then p is a divisor of n as well, i.e. $p|n$. That is, either $p|n$ or $\gcd(p, n) = 1$.

6. (a) $110 = 2 \cdot 5 \cdot 11$
   (b) $792 = 2^3 \cdot 3^2 \cdot 11$
   (c) $343 = 7^3$
   (d) $3422 = 2 \cdot 29 \cdot 59$
   (e) $15 \times 10^{23} = (3 \cdot 5) \times (5 \cdot 2)^{23} = 3 \cdot 5 \cdot (5^{23} \cdot 2^{23}) = 3 \cdot 5^{24} \cdot 2^{23} = 2^{23} \cdot 3 \cdot 5^{24}$

7. The primes larger than 13 and less than 50 are: $17, 19, 23, 29, 31, 37, 41, 43$, and 47.

Interval Ratio	Semitones	Keyboard Approx.	Error
17	$12\log_2(17) \approx 49.050$	49 semitones	0.050 semitones = 5.0 cents
19	$12\log_2(19) \approx 50.975$	51 semitones	0.025 semitones = 2.5 cents
23	$12\log_2(23) \approx 54.283$	54 semitones	0.283 semitones = 28.3 cents
29	$12\log_2(29) \approx 58.296$	58 semitones	0.296 semitones = 29.6 cents
31	$12\log_2(31) \approx 59.450$	59 semitones	0.450 semitones = 45.0 cents
37	$12\log_2(37) \approx 62.513$	63 semitones	0.487 semitones = 48.7 cents
41	$12\log_2(41) \approx 64.291$	64 semitones	0.291 semitones = 29.1 cents
43	$12\log_2(43) \approx 65.115$	65 semitones	0.115 semiteons = 11.5 cents
47	$12\log_2(47) \approx 66.655$	67 semitones	0.345 semitones = 34.5 cents

The prime numbers $17, 19$, and 43 have good keyboard approximations.

8. First, we make an observation that we will use later in this problem. Suppose that X is an interval of x semitones. Then the opposite interval of X (let's call it $-X$) has $-x$ semitones. Converting these to interval ratios, we see that X has an interval ratio of $2^{x/12}$ and $-X$ has an interval ratio of $2^{-x/12} = \frac{1}{2^{x/12}}$. That is, the interval ratio of an interval is the reciprocal of the interval ratio of the opposite interval.

   Now, the proof of this problem. Let Q be a rational interval and let q be its interval ratio. Since q is rational, we can write $q = \frac{n}{m}$, where n and m are integers and $m \neq 0$, and since interval ratios must be positive, we can assume that n and m are both positive. Now, we saw in class that every positive integer has a prime factorization. So, we can write $n = p_1 p_2 \cdots p_k$ and $m = q_1 q_2 \cdots q_l$, where each p_i and each q_i is a prime number (note that we are not insisting here that $p_i \neq p_j$ or that $q_i \neq q_j$ when $i \neq j$). So, we have $q = p_1 p_2 \cdots p_k \frac{1}{q_1}\frac{1}{q_2}\cdots\frac{1}{q_l}$. (In the edge case where $n = m = 1$, instead write $q = 2 \cdot \frac{1}{2}$.) Each p_i is an interval ratio representing a prime interval, and by the observation we made earlier we know that each $\frac{1}{q_i}$ is an interval ratio representing the opposite of a prime interval. Since the composition of two intervals with interval ratios a and b is the interval with interval ratio ab, it follows that Q is the composition of prime intervals and the opposites of prime intervals.

9. The group of units $\mathbb{Z}_7^*$ is the set of elements in $(\mathbb{Z}_7, \cdot)$ that have inverses, together with the multiplication operation that they inherit from $\mathbb{Z}_7$. That is, $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$, since 1 is its own inverse, 2 and 4 are inverse to each other, 3 and 5 are inverse to each other, and 6 is its own inverse. This group is indeed cyclic, and its only generators are 3 and 5. This is straightforward to check.

10. Answers will vary. See page 91 in the text for an example. Ask me if you have questions.