Chapter 9

A little Boolean Algebra

$\mathbb{Z}_2$ is the simplest ring there is, and an interesting one at that. We can view the elements as representing “bits” on a computer or true/false in logic. Let’s look at the tables:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Taking $1 = true$ and $0 = false$, the tables imply that $+$ and $\cdot$ are the “exclusive or” and “and” operators respectively. That is, $x + y$ is true exactly when one or the other but not both variables are true, while $x \cdot y$ is true if and only if $x$ and $y$ are both true. We introduce, few more symbols: (inclusive)“ or” $\lor$, and “not” $\neg$ defined by

\[ x \lor y = x + y + xy \]
\[ \neg x = x + 1 \]

While we’re at it, let’s introduce the more traditional symbol for “and”

\[ x \land y = x \cdot y \]

We can now prove standard facts from logic by translating them into commutative ring theory. Note that $\mathbb{Z}_2$ has some special properties which makes the algebra quite simple, namely $2x = 0$ and $x^2 = x$.

**Lemma 9.1 (De Morgan).** $\neg(x \lor y) = (\neg x) \land (\neg y)$

This says, for example, that the negation of “it’s a duck or it swims” is “it’s not bird and it doesn’t swim”.
Proof. We’ll start at both ends and work toward a common value.

\[ \neg(x \lor y) = x + y + xy + 1 \]

\[(\neg x) \land (\neg y) = (x + 1)(y + 1) \]

\[ = xy + x + y + 1 \]

\[ \square \]

The following is the “law of excluded middle”, and it is the basis of proof by contradiction.

**Lemma 9.2.** \((\neg x) \lor x = 1\)

**Proof.**

\[(\neg x) \lor x = (x + 1) + x(x + 1) \]

\[= 2x + 1 + x^2 + x \]

\[= 1 + 2x \]

\[= 1 \]

\[ \square \]

For really complicated Boolean (i. e. \&, \lor, \neg) expressions, we can have Maple help us out in converting these to polynomials. For example, let’s convert both sides of the equation in lemma 9.1.

\[ > \text{convert(not (x or y), mod2);} \]

\[ 1 + x + y + xy \]

\[ > \text{convert((not x) and (not y), mod2);} \]

\[ 1 + x + y + xy \]

### 9.3 Exercises

1. Prove the remaining De Morgan law \(\neg(x \land y) = (\neg x) \lor (\neg y)\).

2. Prove that \(\lor\) is associative.

3. Prove the distributive law \(x \land (y \lor z) = (x \land y) \lor (x \land z)\).

4. Check that \(\neg(x \land (\neg z)) \lor ((z \lor x) \lor (\neg y)) = 1\) either by hand or using Maple.

5. A commutative ring \(R\) is called Boolean if \(x^2 = x\) holds for each \(x \in R\). Prove that \(2x = 0\) in any Boolean ring. (Hint: evaluate \((x + 1)^2\).) \(\mathbb{Z}_2\) is Boolean, for other examples, see the exercises of 22. All the results of this section extend to Boolean rings.