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:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

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" $\vee$, and "not" $\neg$ defined by

$$x \vee y = x + y + xy$$

$$\neg x = x + 1$$

While we're at it, let's introduce the more traditional symbol for "and"

$$x \wedge y = x \cdot y$$

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). $\neg(x \vee y) = (\neg x) \wedge (\neg y)$

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 an work toward a common value.

$$\neg(x \vee y) = x + y + xy + 1$$

$$\begin{aligned}(\neg x) \wedge (\neg y) &= (x+1)(y+1) \\ &= xy + x + y + 1\end{aligned}$$

□

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

Lemma 9.2. $(\neg x) \vee x = 1$

Proof.

$$\begin{aligned}(\neg x) \vee x &= (x+1) + x + x(x+1) \\ &= 2x + 1 + x^2 + x \\ &= 1 + 2x \\ &= 1\end{aligned}$$

□

For really complicated Boolean (i. e. $\wedge, \vee, \neg$) 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.

```
> convert(not (x or y), mod2);
```

$$1 + x + y + x\,y$$

```
> convert((not x) and (not y), mod2);
```

$$1 + x + y + x\,y$$

9.3 Exercises

1. Prove the remaining De Morgan law $\neg(x \wedge y) = (\neg x) \vee (\neg y)$.
2. Prove that $\vee$ is associative.
3. Prove the distributive law $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.
4. Check that $\neg(x \wedge (\neg z)) \vee ((z \vee x) \vee (\neg y)) = 1$ 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.