Rowan Lochrin
MATH415B - Klaus Lux
1/20/18
Homework 1

11 Let $d \in \mathbb{Z}$, prove that $Z[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ is an integral domain.

Proof. We will show first that $Z[\sqrt{d}]$ is a subring of $\mathbb{R}$ by the two step subring test. Assume

$$(x_1 + y_1\sqrt{d}), (x_2 + y_2\sqrt{d}) \in Z[\sqrt{d}]$$

Then

$$(x_1 + y_1\sqrt{d}) - (x_2 + y_2\sqrt{d}) = (x_1 - x_2) + (y_1 - y_2)\sqrt{d} \in Z[\sqrt{d}]$$

Because $(x_1 + x_2), (y_1 + y_2) \in \mathbb{Z}$. Also,

$$\begin{aligned}(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) &= (x_1x_2) + (x_1y_2\sqrt{d}) + (x_2y_2\sqrt{d}) + (y_1y_2d) \\ &= (x_1x_2 + y_1y_2d) + (x_1y_2 + x_2y_1)\sqrt{d} \in Z[\sqrt{d}]\end{aligned}$$

$Z[\sqrt{d}]$ is a subring of $\mathbb{R}$. Because there are no zero divisors in $\mathbb{R}$,$\mathbb{R}$ is commutative and $1 \in Z[\sqrt{d}]$. $Z[\sqrt{d}]$ is an integral domain □

30 Let $d > 0 \in \mathbb{Z}$, prove that $Q[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in Q\}$ is a field

Proof. By the same argument in question 11 we know that $Q[\sqrt{d}]$ is a subring of $\mathbb{R}$. So $Q[\sqrt{d}]$ is a commutative ring. To verify that $Q[\sqrt{d}]$ is a field we will also have to show every nonzero element has an identity so for any nonzero element x:

$$x = (a + b\sqrt{d}) \in Q[\sqrt{d}]$$

We seek to find some $a', b' \in Q$

$$x^{-1} = (a' + b'\sqrt{d}) \in Q[\sqrt{d}]$$

Such that

$$\begin{aligned}xx^{-1} &= (a + b\sqrt{d})(a' + b'\sqrt{d}) \\ &= aa' + ab'\sqrt{d} + a'b\sqrt{d} + bb'd \\ &= aa' + bb'd + (ab' + a'b)\sqrt{d} \\ &= 1\end{aligned}$$

Meaning

$$aa' + bb'd + (ab' + a'b)\sqrt{d} = 1 \tag{1}$$

So

$$ab' + a'b = 0$$

And

$$aa' + bb' = 1$$

If $b = 0$ consider

$$a' = (bd)^{-1} \text{ and } b' = 0$$

We know $(bd)^{-1}$ exists because $bd \in \mathbb{Q}$, a field. Note that $bd = 0$ implies either d is not positive or $x = 0$. So our values for a' and b' solve 1.

If $b \neq 0$ then

$$a' = \frac{a^2}{a^2 - db^2}, b' = \frac{b^2}{b^2 - db^2}$$

Solve 1.

□

41 If a is an idempotent in a commutative ring, show that $1 - a$ is also an idempotent.

$$(1-a)^2 = (1-a) - a(1-a) = (1-a) - a + a^2$$

Because $a = a^2$

$$(1-a)^2 = (1-a)$$

42 Construct a multiplication table for $*_{\mathbb{Z}}[i]$.

$*_{\mathbb{Z}_2[i]}$	0	1	i	1 + i
0	0	0	0	0
1	0	1	i	i + 1
i	0	i	1	i + 1
1 + i	0	1 + i	1 + i	0

$\mathbb{Z}_2$ is not a field because $1+i$ has no inverse. It's not a integral domain because $(1+i)^2 = 0$.

43 The nonzero elements of $\mathbb{Z}_3[i]$ form an Abelian group of order 8 under multiplication. Is it isomorphic to $\mathbb{Z}_8, \mathbb{Z}_4 \oplus \mathbb{Z}_4, or \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$?
$\mathbb{Z}_8$ we know this because from the theory Abelian group it must be isomorphic to one of the there and because

$$\{(i+1)^1, ..., (i+1)^8\} = \{1+i, 2i, 1+2i, 2, 2+2i, i, 2+i, 1\} = \mathbb{Z}_3[i]$$

So $\mathbb{Z}_3[i]$ is generated by $(i+1)$, implying that it's isomorphic to the cyclic group of order 8, $\mathbb{Z}_8$.

58 Find the characteristic of $\mathbb{Z}_4 \oplus 4\mathbb{Z}$

$$\text{char } \mathbb{Z}_4 \oplus 4\mathbb{Z} = 0$$

We know this because all non-zero elements of $4\mathbb{Z}$ have infinite order under addition.

62 Let F be a finite field with n elements. Prove that $x^{n-1} = 1$ for all nonzero x in F.

Proof. Consider the group F_* to be the group of elements in F under the operation of multiplication. Since F_* is finite by Lagrange's Theorem

$$k \text{ ord } x = n$$

For some integer k. So

$$x^n = x \to x^{n-1} = 1$$

Meaning $x^{n-1} = 1$ in F. □