# Ring Theory

## Dummit and Foote

### Section 7.6

**Exercise 2:** Let $R$ be a finite Boolean ring with identity $1 \neq 0$. Prove that $R \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$.

*Solution:* Let $R = \{0, a_1, \ldots, a_n\}$. By the previous problem,

$$R \cong Ra_1 \times R(1-a_1)$$

Now, we showed that $a_1$ is identity for $Ra_1$ and $(1-a_1)$ is an identity for $R(1-a_1)$. If $a_k \in Ra_1 \cap R(1-a_1)$ then $a_k = a_k a_1 (1-a_1) = a_k \left(a_1 - a_1^2\right) = a_k \left(a_1 - a_1\right) = 0$. Thus $Ra_1 \cap R(1-a_1) = 0$. Also, both $Ra_1$ and $R(1-a_1)$ are nonempty, since $a_1 = a_1 a_1 \in Ra_1$ and $1 - a_1 = (1-a_1)^2 \in R(1-a_1)$ - and also it always contains 0, so we see that the separation, at least 2 elements are in each new set.
Summarizing, we see that under such a separation, the cardinality of each new ideal has decreased by at least 1 and is also greater than or equal to 2.
Since each new ideal is also Boolean, we can choose any nonzero element and repeat the process. Then after at most $n$ reiterations, we find a product of ideals of $R$ of cardinality 2 each (containing 0 and some $a_k$ ). Each of these is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, hence we find

$$R \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}.$$

## Ekstraopgaver - Alg2

### Ugeseddel 5

**Ekstraopgave 1:** (a) Assume $a, b \in \mathbb{Z}$ are coprime. Let $u \in \mathbb{Z}$ be the inverse to $b$ mod $a^2 + b^2$. Show that the map

$$\varphi\colon \mathbb{Z}[i] \to \mathbb{Z}/\left(a^2+b^2\right)\mathbb{Z} \quad x + yi \mapsto [x - auy]_{(a^2+b^2\mathbb{Z})}$$

is a surjective ring homomorphism with $\operatorname{Ker}\varphi = (a+bi)$.

*Solution:* All except the kernel part is trivial.
Assume $\varphi(x+iy) = 0$. Then $x - auy \equiv 0 \pmod{a^2+b^2}$, so $xb - ay \equiv 0 \pmod{a^2+b^2}$. Thus $xb - ay = a^2t + b^2t$ for some $t \in \mathbb{Z}$. Now we find $xb \equiv b^2 t \implies x \equiv bt \pmod{a}$, so for some $s \in \mathbb{Z}$, $x = bt + as$. Likewise, $-ay \equiv a^2 t \implies y \equiv -at \pmod{b}$, so for some $r \in \mathbb{Z}$, $y = br - at$. Now putting it together, we have

$$a^2t + b^2t = xb - ay = b^2t + abs - abr + a^2t \implies ab(s-r) = 0 \implies s = r.$$

Thus we have

$$x + iy = bt + ar + i(br - at) = bt + ar + ibr - iat = (a+bi)(r-it).$$

Hence $x + iy \in (a+bi)$. The converse inclusion is trivial.

(b) We thus find by (a) that e.g.

$$\mathbb{Z}[i]/(5) = \mathbb{Z}[i]/((2+i)(2-i)) \cong \mathbb{Z}[i]/(2+i) \times \mathbb{Z}[i]/(2-i) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Likewise, in general, for all primes $p \equiv 1 \pmod{4}$, we have

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

by Fermat's theorem on sums of squares - note: the coprime condition is satisfies because $p$ is prime. Thus, we cannot do likewise for any $n$ that can be written as the sum of two squares.