.1 Further remarks and examples

Problem .1.1. Generalize the CRT for two ideals, as follows. Let I, J be ideals in a commutative ring R; prove that there is an exact sequence of R-modules

$$0 \longrightarrow I \cap J \longrightarrow R \xrightarrow{\varphi} \frac{R}{I} \times \frac{R}{J} \longrightarrow \frac{R}{I+J} \longrightarrow 0$$

where φ is the natural map. (Also, explain why this implies the first part of Theorem 6.1, for $k = 2$.)

Solution. Let the map for $I \cap J \to R$ be the inclusion. Since it is injective, its kernel is 0 and the first part of the sequence is exact. Furthermore, its image is merely $I \cap J$. Now consider the map φ which sends $r \in R$ ot $(r + I,\ r + J)$. Certainly the kernel of this map is the set of elements in R which are in both I and J; that is, the kernel is $I \cap J$. The image of this map is merely the set $\{r+I,\ r+J) \mid r \in R\}$. Note that this may not be the entirety of $(R/I)\times(R/J)$. Define a map from $(R/I) \times (R/J)$ to $R/(I + J)$ which sends $(a + I, b + J)$ to $a - b + (I + J)$. One can easily verify that this is indeed a homomorphism of modules. Note that the kernel of this image is precisely the image of φ. Furthermore, the homomorphism is surjective; and arbitrary $a + (I + J)$ is mapped to by $(a + I, 0 + J)$. With these homomorphisms, we have shown the existence of such an exact sequence of R-modules.

In the case where $I + J = (1)$, then the map φ is surjective. This can be seen by noting that there exist $i \in I$, $j \in J$ such that $i+j = 1$. Then for all $(r+I, s+J)$, we have

$$\begin{aligned}
\varphi(rj + si) &= (rj + I, si + J) \\
&= (rj + ri + I, si + sj + J) \\
&= (r(j + i) + I, s(i + j) + J) \\
&= (r + I, s + J).
\end{aligned}$$

Thus, we have recovered the desired statement. □

Problem .1.2. Let R be a commutative ring, and let $a \in R$ be an element such that $a^2 = a$. Prove that $R \cong R/(a) \times R/(1 - a)$.

Show that the multiplication in R endows the ideal (a) with a *ring* structure, with a as the identity. Prove that $(a) \cong R/(1 - a)$ as rings. Prove that $R \cong (a) \times (1 - a)$ as rings.

Solution. Consider the natural homomorphism φ from R to $R/(a) \times R/(1 - a)$ which sends r to $(r + (a), r + (1 - a))$. The kernel of this homomorphism is the set of elements in $(a) \cap (1 - a)$. Let $x \in (a) \cap (1 - a)$ so $x = ra = s(1 - a)$ for some $r, s \in R$. Multiplying both sides by a yields $ra^2 = sa - sa^2$. But then we have

$$x = ra = sa - sa = 0.$$

Thus, $(a) \cap (1-a) = 0$ so φ is injective. To see that it is surjective, note that $(a) + (1-a) = (1)$. By Exercise 6.1, the natural homomorphism is surjective. Therefore, φ is a bijective ring homomorphism and thus an isomorphism.

The ideal (a) is already an abelian group under addition. To see that it is also a ring under multiplication in R with a as an identity, note that for $ax \in (a)$, we have $a \cdot ax = a^2 x = ax$. Distributivity is inherited from R, making (a) a ring.

Consider the natural map from (a) to $R/(1-a)$ which sends ax to $ax + (1-a)$. This map is surjective as any $x + (1-a) = ax + (x - ax) + (1-a) = ax + (1-a) = \varphi(ax)$. Furthermore, the kernel of this map is the set of elements $ax \in (1-a)$. But $ax = (1-a)y \implies a(x+y) = y \implies a(x+y) = ay \implies ax = 0$ so $x = 0$ and the homomorphism is injective. Thus, we have a bijective homomorphism from $(a) \to R/(1-a)$ so the rings are isomorphic. The third isomorphism is relatively similar to show. □

Problem .1.3. Recall (Exercise III.3.15) that a ring R is called *Boolean* if $a^2 = a$ for all $a \in R$. Let R be a finite Boolean ring; prove that $R \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$.

Solution. Suppose R has only two elements; then $R \cong \mathbb{Z}/2\mathbb{Z}$. If R has more than two elements, then there is some idempotent $e \notin \{0, 1\}$. Per Exercise 6.2, we can split R into $(e) \times (1-e)$, both of which have strictly fewer elements than R. Repeating this process will eventually yield a direct product in which each component is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. □

Problem .1.4. Let R be a finite commutative ring, and let p be the smallest prime dividing $|R|$. Let $I_1, \ldots, I_k$ be proper ideals such that $I_i + I_j = (1)$ for $i \neq j$. Prove that $k \leq \log_p |R|$. (Hint: Prove $|R|^{k-1} \leq |I_1| \cdots |I_k| \leq (|R|/p)^k$.)

Solution. To do. □

Problem .1.5. Show that the map $\mathbb{Z}[x] \to \mathbb{Z}[x]/(2) \times \mathbb{Z}[x]/(x)$ is not surjective.

Solution. Consider the element $(1, 2) \in \mathbb{Z}[x]/(2) \times \mathbb{Z}[x]/(x)$. Suppose some polynomial $f \in \mathbb{Z}[x]$ is sent to this element. Since $f \equiv 2 (\mod x)$, this forces the constant term of f to be 2. However, if this were the case then the constant term of $f \mod 2$ would be 0, a contradiction. Thus, there is no polynomial mapped to this element and the mapping is not surjective. □

Problem .1.6. Let R be a UFD.

- Let $a, b \in R$ such that $\gcd(a, b) = 1$. Prove that $(a) \cap (b) = (ab)$.
- Under the hypotheses of Corollary 6.4 (but only assuming that R is a UFD) prove that the function φ is injective.

Solution. To do. ☐

Problem .1.7. Find a polynomial $f \in \mathbb{Q}[x]$ such that $f \equiv 1 \mod (x^2+1)$ and $f \equiv x \mod x^{100}$.

Solution. To do. ☐

Problem .1.8. Let $n \in \mathbb{Z}$ be a positive integer and $n = p_1^{a_1} \cdots p_r^{a_r}$ its prime factorization. By the classification theorem for finite abelian groups (or, in fact, simplier considerations; cf. Exercise II.4.9)

$$\frac{\mathbb{Z}}{(n)} \cong \frac{\mathbb{Z}}{(p_1^{a_1})} \times \cdots \times \frac{\mathbb{Z}}{(p_r^{a_r})}$$

as abelian groups.

- Use the CRT to prove that this is in fact a *ring* isomorphism.
- Prove that
$$\left(\frac{\mathbb{Z}}{(n)}\right)^* \cong \left(\frac{\mathbb{Z}}{(p_1^{a_1})}\right)^* \times \cdots \times \left(\frac{\mathbb{Z}}{(p_r^{a_r})}\right)^*$$
(recall that $(\mathbb{Z}/n\mathbb{Z})^*$ denotes the group of units of $\mathbb{Z}/n\mathbb{Z}$).
- Recall (Exercise II.6.14) that *Euler's ϕ-function* $\phi(n)$ denotes the number of positive integers $< n$ that are relatively prime to n. Prove that
$$\phi(n) = p_1^{a_1-1}(p_1-1) \cdots p_r^{a_r-1}(p_r-1).$$

Solution. To do. ☐

Problem .1.9. Let I be an ideal of