1) Let R be a ring and I be an ideal of R.

(a) Prove that if J is an ideal of R containing I, then $\bar{J} \overset{\text{def}}{=} \{\bar{a} \in R/I \ : \ a \in J\}$ is an ideal of R/I.

Solution. First observe that if $\bar{a} \in \bar{J}$, then, there is some $b \in J$ such that $\bar{b} = \bar{a}$, i.e., $a - b \in I \subseteq J$. But then, since J is closed under addition and $b \in J$, this means that $a \in J$. Therefore, if $\bar{a} \in \bar{J}$, then $a \in J$.

Since $J \neq \varnothing$, clearly $\bar{J} \neq \varnothing$.

Let $\bar{a}, \bar{b} \in \bar{J}$. Then $a, b \in J$ and so $a + b \in J$, and hence $\bar{a} + \bar{b} = \overline{a + b} \in \bar{J}$ [by definition of $\bar{J}$].

In the same way, if $\bar{a} \in \bar{J}$ and $\bar{r} \in \bar{R}$, then $r \in R$ and $a \in J$. Since J is an ideal, we have that $r \cdot a \in J$. Thus, $\bar{r} \cdot \bar{a} = \overline{r \cdot a} \in \bar{J}$.

□

(b) Prove that if $\bar{J}'$ is an ideal of R/I, then $J' \overset{\text{def}}{=} \{a \in R \ : \ \bar{a} \in \bar{J}'\}$ is an ideal of R containing I.

Solution. Since $\bar{J}' \neq \varnothing$, clearly $J' \neq \varnothing$.

Let $a, b \in J'$. Then, $\bar{a}, \bar{b} \in \bar{J}'$ [by definition]. Since $\bar{J}'$ is an ideal, $\bar{a} + \bar{b} = \overline{a + b} \in \bar{J}'$. So, $a + b \in J'$ [by defintion of J' again].

In the same way, let $r \in R$ and $a \in J$, then $\bar{r} \in \bar{R}$ and $\bar{a} \in \bar{J}'$, and hence $\bar{r} \cdot \bar{a} = \overline{r \cdot a} \in \bar{J}'$. Thus, $r \cdot a \in J'$.

□

2) Let R be a commutative ring with identity and $a \in R$ such that $a^{n-1} \neq 0$, but $a^n = 0$, for some positive integer n. Prove that $R[x]/(ax-1) = \{\bar{0}\}$, i.e., it is the *zero ring*.

Solution. It suffices to show that $1 \in (ax-1)$. But, since $a^n = 0$

$$1 = (1 - a^n x^n) = (1 - ax)(1 + ax + a^2x^2 + \cdots + a^{n-1}x^{n-1}).$$

Since $1 \in (ax-1)$, we have that $(ax-1) = (1) = R[x]$, and the quotient is then the zero ring.

A more direct way to see this, is to see that we are adjoining an inverse of a to R, say α: $a \cdot \alpha = 1$ in $R' \stackrel{\text{def}}{=} R[x]/(ax-1) = R[\alpha]$. Then, for all b in R', we have that $a^n b = 0$, since $a^n = 0$. But then, $\alpha^n a^n b = (\alpha a)^n = 1_{R'} b = b = 0$. So, every element of R' is equal to zero. □

3) Let R be an integral domain, F be its field of fractions [or quotient field], and K be field such that $R \subseteq K$. Prove that there is an *injective homomorphism* $\phi : F \to K$, such that for all $a \in R$, $\phi\left(\frac{a}{1}\right) = a$. [**Hint:** To start, you need to find the formula for ϕ. Think of the most natural way of seeing an element of F inside of K, remembering that the image is contained in a *field*. Also, you will have to show that your formula is well defined, i.e., if $\frac{a}{b} = \frac{c}{d}$, then $\phi\left(\frac{a}{b}\right) = \phi\left(\frac{c}{d}\right)$.]

Solution. Let $\phi : R \to K$ defined by $\phi(a/b) \stackrel{\text{def}}{=} a \cdot b^{-1}$. [Note that since K is a field, and $b \in R - \{0\} \subseteq K - \{0\}$, we have $b^{-1} \in K$.]

Well defined: Suppose that $a/b = c/d$, i.e., $ad = bc$. Then, since $d \neq 0$, we have $a = bcd^{-1}$ [in K]. So, $\phi(a/b) = ab^{-1} = bcd^{-1}b^{-1} = cd^{-1} = \phi(c/d)$. Hence, ϕ is well defined.

Homomorphism: We have:

$$\begin{aligned}
\phi(1_F) &= \phi(1/1) = 1 \cdot 1^{-1} = 1, \\
\phi(a/b + c/d) &= \phi((ad+bc)/bd) = (ad+bc)(bd)^{-1} = (ad+bc)(b^{-1}d^{-1}) \\
&= ab^{-1} + cd^{-1} = \phi(a/b) + \phi(c/d), \\
\phi(a/b \cdot c/d) &= \phi((ac)/(bd)) = (ac)(bd)^{-1} = acb^{-1}d^{-1} \\
&= ab^{-1}cd^{-1} = \phi(a/b) \cdot \phi(c/d).
\end{aligned}$$

Injective: If $\phi(a/b) = 0$, then $ab^{-1} = 0$. Since we are in a field [and so a domain], there is no zero divisor, and so either $a = 0$ or $b^{-1} = 0$. Since $b \neq 0$, we have that $b^{-1} \neq 0$ [it is invertible], so $a = 0$. Then, $a/b = 0/b = 0_F$. Hence ϕ is injective

Now, by its definition, clearly $\phi(a/1) = a \cdot 1^{-1} = a$.

□

4) Prove that $\mathbb{Z}[\mathrm{i}\sqrt{3}]/(2-\mathrm{i}\sqrt{3}) \cong \mathbb{Z}/7\mathbb{Z}$.

Solution. [Here are a few preliminary comments: first, the ring $\mathbb{Z}[\mathrm{i}\sqrt{3}]$ is very much like the *Gaussian Integers* $\mathbb{Z}[\mathrm{i}]$. Note that $\mathbb{Z}[\mathrm{i}\sqrt{3}] \cong \mathbb{Z}[x]/(x^2+3)$, and hence $\{1, \mathrm{i}\sqrt{3}\}$ is a *basis*, i.e., every element in this ring can be represented *in a unique way* as $a + b\mathrm{i}\sqrt{3}$.]

Let $\phi : \mathbb{Z} \to \mathbb{Z}[\mathrm{i}\sqrt{3}]/(2-\mathrm{i}\sqrt{3})$ be the unique homormophism, i.e., $\phi(n) = n \cdot \bar{1} = \bar{n} = n + (2-\mathrm{i}\sqrt{3})$. [Note, we do not need to prove that the map "$n \mapsto n \cdot 1_R$" is a homomorphism! It is *always* a homomorphism.]

We have that

$$\phi(7) = \bar{7} = \overline{(2-\mathrm{i}\sqrt{3})\cdot(2+\mathrm{i}\sqrt{3})} = \overline{(2-\mathrm{i}\sqrt{3})} \cdot \overline{(2+\mathrm{i}\sqrt{3})} = \bar{0} \cdot \overline{(2+\mathrm{i}\sqrt{3})} = \bar{0}.$$

Hence, $(7) \subseteq \ker\phi$.

Now, let $n \in \ker\phi$. Then, $\phi(n) = \bar{n} = \bar{0}$, i.e., $n \in (2-\mathrm{i}\sqrt{3})$, or $n = (a+b\mathrm{i}\sqrt{3})(2-\mathrm{i}\sqrt{3})$. So, $n = (2a+3b) + (2b-a)\mathrm{i}\sqrt{3}$. Thus, $a = 2b$ [for the imaginary to be zero – we are using the unique representation here!!], which yields $n = 7b$, and therefore $\ker\phi \subseteq (7)$.

We can then conclude that $\ker\phi = (7)$.

Let $R \stackrel{\text{def}}{=} \mathbb{Z}[\mathrm{i}\sqrt{3}]/(2-\mathrm{i}\sqrt{3})$. Then, in R, $\overline{2-\mathrm{i}\sqrt{3}} = \bar{0}$, i.e., $\overline{\mathrm{i}\sqrt{3}} = \bar{2}$. So, given $\overline{a+b\mathrm{i}\sqrt{3}} \in R$ [and so $a, b \in \mathbb{Z}$], we have that $\phi(a+2b) = \overline{a+2b} = \overline{a+b\mathrm{i}\sqrt{3}}$, and ϕ is onto.

By the *First Isomorphism Theorem*, $\mathbb{Z}/(7) \cong \mathbb{Z}[\mathrm{i}\sqrt{3}]/(2-\mathrm{i}\sqrt{3})$.

□