MATH 8510, Abstract Algebra I
Fall 2016
Exercises 12
Collaborators: Daozhou Zhu, Xiaoyuan Liu
Name: **Shuai Wei**

Exercise 1. Let R be a commutative ring with identity. Let $f \in R[x]$ be monic of degree $d \geq 1$. In the quotient ring $S = R[x]/fR[x]$, for all $g \in R[X]$, set $\overline{g} := g + fR[x]$.

(a) Prove that for every element $s \in S$ there exist unique elements $r_0, \ldots, r_{d-1} \in R$ such that $s = \sum_{k=0}^{d-1} \overline{r_k}\ \overline{x}^k$. (Hint: Division Algorithm)

Proof. Let $s \in S$.
Let $g = f(\overline{x}) \in R[\overline{x}]$.
Since $f \in R[x]$ is monic of degree d, g is monic of degree d.
Then by the Division Algorithm, there is unique $q, r \in S$ such that $s = qg + r$ with $\deg(r) < \deg(f) = d$.
Since $S = R[x]/fR[x]$ and $s \in S$, $\deg(s) < \deg(f) = \deg(g) = d$,
we have

$$q = 0_S \in S.$$

So ther is a unique $r \in S$ with $\deg(r) < d$ such that $s = r$.
Namely, there exsits unique elements $\overline{r\prime_0}, \ldots, \overline{r\prime_{d-1}} \in S$ such that $s = \sum_{k=0}^{d-1} \overline{r\prime_k}\ \overline{x}^k$.
Since for $k = 0, 1, \ldots, d-1$,

$$\deg(\overline{r\prime_k}) = 0$$

and

$$\overline{r\prime_k} = r\prime_k + fR[x],$$

where $r\prime_k \in R[x]$,
in addtion, $\deg(f) = d \geq 1$,
we have for $k = 0, 1, \ldots, d-1$, there is only one representative for $\overline{r\prime_k}$.
Moreover, by the Division Algorithm, given $r\prime_k \in R[x]$, there exists unique $r_k, p \in R[x]$ such that

$$r\prime_k = pf + r_k.$$

Then we have $r_k = r\prime_k + f(-p) \in \overline{r\prime_k}$ is the unique representative for $\overline{r\prime_k}$ for $k = 0, 1, \ldots, d-1$.
Then

$$\deg(r_k) = \deg(\overline{r\prime_k}) = 0.$$

So such $r_k \in R$ is unique for $k = 0, 1, \ldots, d-1$.
Therefore, for every element $s \in S$, there exists unique elements $r_0, \ldots, r_{d-1} \in R$ such that $s = \sum_{k=0}^{d-1} \overline{r_k}\ \overline{x}^k$. $\square$

(b) Prove that the function $\epsilon\colon R \to S$ given by $r \mapsto \overline{r}$ is a ring monomorphism, that is, a 1-1 ring homomorphism. Conclude that $R \cong \operatorname{Im}(\epsilon) \subseteq S$.
Note: We often use this to identify R with its image in S, so that, e.g., we think of R as a subring of S, and the formula in part (a) becomes $s = \sum_{k=0}^{d-1} r_k \overline{x}^k$.

Proof. Since $\forall\ r, s \in R$, we have $r, s \in R[x]$, and since $fR[x] \leq R[x]$, we have

$$\begin{aligned}\epsilon(r+s) &= \overline{r+s}\\ &= r+s+fR[x]\\ &= (r+fR[x])+(s+fR[x])\\ &= \overline{r}+\overline{s}\\ &= \epsilon(r)+\epsilon(s),\end{aligned}$$

and

$$\begin{aligned}\epsilon(rs) &= \overline{rs}\\ &= rs+fR[x]\\ &= (r+fR[x])(s+fR[x])\\ &= \overline{r}\ \overline{s}\\ &= \epsilon(r)\epsilon(s),\end{aligned}$$

it is a ring homomorphism.
Let $r, s \in R$, if $\overline{r} = \overline{s}$, then $r = s$ since $\overline{r}$ and $\overline{s}$ have unique polynomial form, respectively, by part (a).
Let $r \in R$, then

$$\begin{aligned}r \in \operatorname{Ker}(\epsilon) &\iff \epsilon(r) = 0_s\\ &\iff \overline{r} = \overline{0_r}\\ &\iff r = 0_r.\end{aligned}$$

So ϵ is 1-1.
Thus, ϵ is a ring monomorphism.
Since $\operatorname{Im}(\epsilon) \subseteq S$ and it is onto from R to S, we have

$$R \cong \operatorname{Im}(\epsilon) \subseteq S.$$

□

(c) What happens in part (b) when $d = 0$? Specifically, what can you say about S and ϵ in this case?
Soln: In the proof of part (a), we know when $d = 0$, for $s \in S$, s may have more than one representative from R, so we can not make conclusion for part (a).
Also, since for $s \in S$, s may have alternative polynomial form, ϵ may not be 1-1, but is still a homomorphism.
At last, $\operatorname{Im}(\epsilon) \subseteq S$ always holds.

Exercise 2 ($\exists\mathbb{C}$)**.** Consider the ring $C = \mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$, and set $i := \overline{x} \in C$.

(a) Prove that $i^2 = -1$.

Proof.

$$\begin{aligned} i^2 + \overline{1} &= \overline{x}^2 + \overline{1} \\ &= \overline{x}\ \overline{x} + \overline{1} \\ &= \overline{x^2} + \overline{1} \\ &= \overline{x^2 + 1} \\ &= \overline{0}, \end{aligned}$$

so by Exercise 12#2(b),

$$i^2 = \overline{0} - \overline{1} = \overline{-1} = -1.$$

□

(b) Using Exercise 1(b) identify $\mathbb{R}$ with its image in C. Observe that Exercise 1(a) implies that for every element $z \in C$ there exist unique elements $a, b \in \mathbb{R}$ such that $z = a + bi$. (There is nothing to prove here.)
Soln:
Since $\deg(x^2+1) = 2 \geq 1$, by Exercise 12#1(a), we have for $c \in C$, there exists unique $a, b \in \mathbb{R}$ such that

$$c = a + bi.$$

Let $r \in \mathbb{R}$, then by Exercise 12#1(b),

$$r = \overline{r} = r + 0i.$$

(c) Prove that $(a + bi) + (c + di) = (a + c) + (b + d)i$ and $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.

Proof. Since $a, bi, c, di \in R[\overline{x}]$ and $R[\overline{x}]$ is a polynomial ring, we have the commutative law and associated law of addition inherit from the polynomial ring $R[\overline{x}]$.
So

$$\begin{aligned} (a + bi) + (c + di) &= a + c + bi + di \\ &= (a + c) + (b + d)i. \end{aligned}$$

Since $\mathbb{R}$ is a commutative ring, $R[x]$ is also commutative ring, so are C and $R[\overline{x}]$.
Since $a, bi, c, di \in R[\overline{x}]$, we have the commutative law and associated law of addition and multiplication and the distributative law inherit from the polynomial ring $R[\overline{x}]$.
So

$$\begin{aligned} (a + bi)(c + di) &= ac + adi + bci + dbi^2 \\ &= ac + adi + bci - db \\ &= (ac - bd) + (ad + bd)i. \end{aligned}$$

□

Note that this can be used to show that C satisfies the properties defining the field of complex numbers. In particular, the ideal $(x^2 + 1)\mathbb{R}[x]$ is maximal. (You are not required to prove anything here.)