Discrete Mathematics **2024**

Student: Jeferson Morales Mariciano <jmorale@ethz.ch>

Assignment 9 **Due date:** Thursday, 21 November 2024, 23:59

Exercise 9.5, More Elementary Properties of Rings ($\star\star$) (8 Points)

Note: in a previous version of this exercise the assumption that R is an integral domain was missing. However, the first statement is false in this case. Can you give a counterexample?
Let $\langle R; +, -, 0, \cdot, 1\rangle$ be a ring, and let $a \in R$ and $b \in R$. Prove the following statements:

a) If R is an integral domain and if $a^m = b^m$ and $a^n = b^n$ for some positive integers m and n with $\gcd(m, n) = 1$, then $a = b$.

b) If $1 - ab$ is a unit, then $1 - ba$ is also a unit. *Hint: if* $x = (1 - ab)^{-1}$ *consider the ring element* $1 + bxa$.

a)

Assumption: R is an integral domain and $\exists m, n \in \mathbb{Z}^+,\ a^m = b^m \ \wedge\ a^n = b^n \ \wedge\ \gcd(m, n) = 1$.
Claim: $a = b$.
Proof:
Distinguish two main cases for the proof, where $a = 0$ and $a \neq 0$.
Thanks to the integral domain property, whenever $a = 0$, then also $b = 0$ since $0^m = 0^n = 0$.
For $a \neq 0$, recall from Corollary 4.5, for $a, b \in \mathbb{Z}$ not both 0, $\exists u, v \in \mathbb{Z}$ such that $\gcd(a, b) = ua + vb$.
$\gcd(a, b) = 1 = um + vn$, where $m, n \in \mathbb{Z}^+$ since the assumption states they are positive integers.
It means that either $u < 0$ or $v < 0$ but not both, in order to comply for $1 = um + vn$.
Without loss of generality (w.l.o.g.), assume $u < 0$ and $v > 0$. Then, $-u > 0$.

$$
\begin{aligned}
a &\iff a^1 \\
&\iff a^{um+vn} && \text{(Corollary 4.5)} \\
&\iff a^{um} \cdot a^{vn} && \text{(multiplicative associativity)} \\
&\iff (a^m)^u \cdot (a^n)^v && \text{(multiplicative commutativity over } \mathbb{Z}) \\
&\iff (b^m)^u \cdot (b^n)^v && \text{(assumption } a^m = b^m, a^n = b^n) \\
&\iff (b^{um}) \cdot (b^{vn}) && \text{(associativity and commutativity of } \cdot) \\
&\iff b^{um+vn} && \text{(multiplicative associativity)} \\
&\iff b^1 && \text{(Corollary 4.5)} \\
&\iff b
\end{aligned}
$$

A symmetrical reasoning proves the case where $u > 0$ and $v < 0$. The statement is therefore true and $a = b$.

b)

Assumption: $\exists u_1 \in R^*, u_1 = 1 - ab$, i.e. it is a unit.
Claim: $\exists u_2 \in R^*, u_2 = 1 - ba$, it is also a unit.
Proof:
by Definition 5.20 of Units, u_1 is invertible, meaning $\exists v_1 \in R^*, u_1 \cdot v_1 = v_1 \cdot u_1 = 1$.
Let $v_1 = (1 - ab)^{-1}$, be the multiplicative inverse of u_1. Then, $u_1 \cdot v_1 = v_1 \cdot u_1 = 1$.

From the Hint, consider the ring element $w \in R, w = 1 + bv_1a$, where $v_1 = (1 - ab)^{-1}$.
In order for u_2 to be a unit, check if it is invertible, i.e. $\exists v_2 \in R^*, u_2 \cdot v_2 = v_2 \cdot u_2 = 1$.

Clearly, both $v_2, w \in R$, so let's check if u_2 is invertible by assigning $v_2 = w$.

$$
\begin{aligned}
u_2 \cdot v_2 &\overset{\cdot}{\Longrightarrow} (1 - ba) \cdot (1 + bv_1a) \\
&\overset{\cdot}{\Longrightarrow} (1 - ba) \cdot 1 + (1 - ba) \cdot bv_1a && \text{(left distributivity)} \\
&\overset{\cdot}{\Longrightarrow} 1 - ba + bv_1a - babv_1a && \text{(right distributivity)} \\
&\overset{\cdot}{\Longrightarrow} 1 - ba + b \cdot (v_1a - abv_1a) && \text{(left distributivity)} \\
&\overset{\cdot}{\Longrightarrow} 1 - ba + b \cdot ((1 - ab) \cdot v_1a) && \text{(right distributivity)} \\
&\overset{\cdot}{\Longrightarrow} 1 - ba + b \cdot ((1 - ab) \cdot (1 - ab)^{-1} \cdot a) && \text{(def } v_1\text{)} \\
&\overset{\cdot}{\Longrightarrow} 1 - ba + b \cdot (1 \cdot a) && \text{(assumption } u_1 \cdot v_1 = 1 \text{)} \\
&\overset{\cdot}{\Longrightarrow} 1 - ba + ba && \text{(multiplicative identity)} \\
&\overset{\cdot}{\Longrightarrow} 1 && \text{(abelian additive group inverse)}
\end{aligned}
$$

Symmetrically, $v_2 \cdot u_2 = 1$.

$$
\begin{aligned}
v_2 \cdot u_2 &\overset{\cdot}{\Longrightarrow} (1 + bv_1a) \cdot (1 - ba) \\
&\overset{\cdot}{\Longrightarrow} 1 \cdot (1 - ba) + bv_1a \cdot (1 - ba) && \text{(right distributivity)} \\
&\overset{\cdot}{\Longrightarrow} 1 - ba + bv_1a - bv_1aba && \text{(left distributivity)} \\
&\overset{\cdot}{\Longrightarrow} 1 - ba + (bv_1 - bv_1ab) \cdot a && \text{(right distributivity)} \\
&\overset{\cdot}{\Longrightarrow} 1 - ba + (bv_1 \cdot (1 - ab)) \cdot a && \text{(left distributivity)} \\
&\overset{\cdot}{\Longrightarrow} 1 - ba + (b \cdot (1 - ab)^{-1} \cdot (1 - ab)) \cdot a && \text{(def } v_1\text{)} \\
&\overset{\cdot}{\Longrightarrow} 1 - ba + (b \cdot 1) \cdot a && \text{(assumption } v_1 \cdot u_1 = 1 \text{)} \\
&\overset{\cdot}{\Longrightarrow} 1 - ba + ba && \text{(multiplicative identity)} \\
&\overset{\cdot}{\Longrightarrow} 1 && \text{(abelian additive group inverse)}
\end{aligned}
$$

Thus, w satifies the definition of the inverse of the unit u_2, therefore $u_1, v_1, u_2, v_2 \in R^*$, the statement is true and $1 - ba$ is also a unit.