## Solutions to homework 6

Due October 16th

## Problem 1:

Let $R$ be a unitary commutative ring such that $1 \neq 0$ and $S \subseteq R$ be closed under multiplication (i.e. $\forall x, y \in S, x y \in S$ ) and contain 1. We define the relation $E$ on $R \times S$ by $(a, s) E(b, t)$ if and only if there exists $x \in S$ such that $x a t=x b s$.

1. Show that $E$ is an equivalence relation.

Solution: Let $a, b, c \in R$ and $s, t, u \in S$. We have $1 a s=1 a s$ so $(a, s) E(a, s)$ and $E$ is reflexive. If $(a, s) E(b, t)$, then there exists $x \in S$ such that $x a t=x b s$ and $x b s=x a t$ so $(b, t) E(a, s)$ and $E$ is symmetric. Finally, assume $(a, s) E(b, t)$ and $(b, t) E(c, u)$, then there exists $x$ and $y \in S$ such that $x a t=x b s$ and $y b u=y c t$. We then have $(x y t) a u=y x b s u=(x y t) c s$ where $x y t \in S$, so $(a, s) E(c, u)$ and $E$ is transitive.
2. Let $R_{S}$ denote the set $(R \times S) / E$ (it is the set of $E$-classes). If $(a, s) \in R \times S$, we $\underline{\text { denote }}$ by $\overline{(a, s)} \in R_{S}$ the $E$-class of $(a, s)$. Show that the map $(\overline{(a, s)}, \overline{(b, t)}) \mapsto$ $(a b, s t)$ is well defined. We denote this map $\star$.

Solution: Assume $\left(a_{1}, s_{1}\right) E\left(a_{2}, s_{2}\right)$ and $\left(b_{1}, t_{1}\right) E\left(b_{2}, t_{2}\right)$, then there exists $x$ and $y \in S$ such that $x a_{1} s_{2}=x a_{2} s_{1}$ and $y b_{1} t_{2}=y b_{2} t_{1}$. It follows that $(x y)\left(a_{1} b_{1}\right)\left(s_{2} t_{2}\right)=$ $(x y)\left(a_{2} b_{2}\right)\left(s_{1} t_{1}\right)$ and $\star$ is well defined.
3. Show that the map $(\overline{(a, s)}, \overline{(b, t)}) \mapsto \overline{(a t+b s, s t)}$ is well defined. We denote this map $\square$.

Solution: Assume $\left(a_{1}, s_{1}\right) E\left(a_{2}, s_{2}\right)$ and $\left(b_{1}, t_{1}\right) E\left(b_{2}, t_{2}\right)$, then there exists $x$ and $y \in S$ such that $x a_{1} s_{2}=x a_{2} s_{1}$ and $y b_{1} t_{2}=y b_{2} t_{1}$. It follows that $x y\left(a_{1} t_{1}+b_{1} s_{1}\right) t_{2} s_{2}=$ $x y a_{1} t_{1} s_{2} t_{2}+x y b_{1} s_{1} t_{2} s_{2}=x y a_{2} s_{1} t_{1} t_{2}+x y b_{2} t_{1} s_{1} s_{2}=x y\left(a_{2} t_{2}+b_{2} s_{2}\right) s_{1} t_{1}$, so $\square$ is welldefined.
4. Show that $\left(R_{S}, \square, \star\right)$ is a unitary commutative ring.

Solution: Let us start by showing associativity of $\square$. We have

$$
\begin{aligned}
(\overline{(a, s)} \square \overline{(b, t)}) \square \overline{(c, u)} & =\overline{(a t+b s, s t)} \square \overline{(c, u)} \\
& =\overline{((a t+b s) u+c s t, s t u)} \\
& =\overline{(a t u+b s u+c s t, s t u)} \\
& =\overline{(a t u+(b u+c t) s, s t u)} \\
& =\overline{(a, s)} \square \overline{(b u+c t, t u)} \\
& =\overline{(a, s)} \square(\overline{(b, t)} \square \overline{(c, u)}) .
\end{aligned}
$$

We have commutativity of $\square: \overline{(a, s)} \square \overline{(b, t)}=\overline{(a t+b s, s t)}=\overline{(b s+a t, t s)}=\overline{(b, t)} \square$ $\overline{(a, s)} ;(0,1)$ is the additive identity: $\overline{(a, s)} \square \overline{(0,1)}=\overline{(a \cdot 1+0 \cdot s, s \cdot 1)}=\overline{(a, s)}$ and we have an additive inverse: $\overline{(a, s)} \square \overline{(-a, s)}=\overline{\left(a s-a s, s^{2}\right)}=\overline{\left(0, s^{2}\right)}=\overline{(0,1)}$. The last equality comes from the fact that $1 \cdot 0 \cdot 1=0=1 \cdot 0 \cdot s^{2}$.

Let us now show associativity of $\star:(\overline{(a, s)} \star \overline{(b, t)}) \star \overline{(c, u)}=\overline{(a b, s t)} \star \overline{(c, u)}=$ $\overline{(a b c, s t u)}=\overline{(a, s)} \star \overline{(b c, t u)}=\overline{(a, s)} \star(\overline{(b, t)} \star \overline{(c, u)})$. Also $\star$ is commutative: $\overline{(a, s)} \star$ $\overline{(b, t)}=\overline{(a b, s t)}=\overline{(b a, t s)}=\overline{(b, t)} \star \overline{(a, s)}$ and $(1,1)$ is the multiplicative identity: $\overline{(a, s)} \star \overline{(1,1)}=\overline{(a \cdot 1, s \cdot 1)}=\overline{(a, s)}$.

Finally $\star$ distributes over $\square$ :

$$
\begin{aligned}
\overline{(a, s)} \star(\overline{(b, t)} \square \overline{(c, u)}) & =\overline{(a, s)} \star \overline{(b u+c t, t u)} \\
& =\overline{(a(b u+c t), s t u)} \\
& =\overline{(a b u+a c t, s t u)} \\
& =\overline{(a b s u+a c s t, s t s u)} \\
& =\overline{(a b, s t)} \square \overline{(a c, s u)} \\
& =\overline{(\overline{(a, s)} \star \overline{(b, t)}) \square(\overline{(a, s)} \star \overline{(c, u)})} .
\end{aligned}
$$

The fourth equality comes from the fact that $1 \cdot(a b s u+a c s t) s t u=1 \cdot(a b u+a c t) s^{2} t u$.
5. Show that the map $a \mapsto \overline{(a, 1)}$ is a unitary ring homomorphism from $\varphi: R \rightarrow R_{S}$.

Solution: Let us show it respects addition: $\varphi(a+b)=\overline{(a+b, 1)}=\overline{\left(a \cdot 1+b \cdot 1,1^{2}\right)}=$ $\overline{(a, 1)} \square \overline{(b, 1)}$; multiplication: $\varphi(a b)=\overline{(a b, 1)}=\overline{\left(a b, 1^{2}\right)}=\overline{(a, 1)} \star \overline{(b, 1)}$ and multiplicative identity: $\varphi(1)=\overline{(1,1)}$.
6. Show that if $S$ contains 0 then $R_{S}$ is the trivial ring.

Solution: Let $a \in R$ and $s \in S$, we have $0 \cdot a \cdot 1=1 \cdot 0 \cdot s$, it follows that $\overline{(a, b)}=\overline{(0,1)}$ and that $S$ contains only one element.
7. Show that $\varphi$ is not injective if and only if $S$ contains a zero-divisor.

Solution: Let us first assume that $S$ contains a zero divisor $s$. So there exists $y \in R$ such that $s y=0$. Now $s \cdot y \cdot 1=0=s \cdot 0 \cdot 1$. So $\varphi(y)=\overline{(y, 1)}=\overline{(0,1)}=\varphi(0)$. So $\varphi$ is not injective.

Conversely, assume $\varphi$ is not injective, then there exists $y \in \operatorname{ker}(\varphi) \backslash\{0\}$, i.e. $\varphi(y)=$ $\overline{(y, 1)}=\overline{(0,1)}$. Hence there exists $s, S$ such that $s \cdot y=s \cdot y \cdot 1=s \cdot 0 \cdot 1=0$. So $s \in S$ is a zero divisor.
8. Show that $R \backslash\{0\}$ is closed under multipication if and only if $R$ is an integral domain.

Solution: Let us assume that $R$ is an integral domain and let $s, t \in R \backslash\{0\}$. Then because neither $s$ or $t$ are zero divisors, st $\neq 0$ and $s t \in R \backslash\{0\}$.
Conversely, if $R \backslash\{0\}$ is closed under multiplication and $s, t \in R \backslash\{0\}$, then $s t \neq 0$, so $s$ is not a zero divisor and the only zero divisor in $R$ is $0: R$ is an integral domain (we already know it is unitary, commutative and non trivial).
9. Assume that $R$ is an integral domain. Show that $R_{(R \backslash\{0\})}$ is a field.

Solution: Let $\overline{(a, s)} \in R_{R \backslash\{0\}}$. If $a=0$, as we saw above, $\overline{(a, s)}=\overline{(0,1)}$. If follows that if $\overline{(a, s)} \neq \overline{(0,1)}$, we must have $a \neq 0$ and hence $\overline{(s, a)} \in R_{R \backslash\{0\}}$. We have $\overline{(a, s)} \star \overline{(s, a)}=\overline{(a s, a s)}=\overline{(1,1)}$. The last equality comes from the fact that $1 \cdot a s \cdot 1=$ $1 \cdot 1 \cdot a s$. So every non zero element in $R_{R \backslash\{0\}}$ is invertible, i.e. it is a field.
10. Show that $\mathbb{Z}_{(\mathbb{Z} \backslash\{0\})}$ is isomorphic (as a unitary ring) to $\mathbb{Q}$.

Solution: Let $\varphi(\overline{(m, n)})=m n^{-1}$. Let us show that $\varphi$ is well defined. If $\overline{(m, n)}=$ $\overline{(p, q)}$, then there exists $s \in \mathbb{Z} \backslash\{0\}$ such that $s m q=s n p$. But $\mathbb{Z}$ is an integral domain and $s \neq 0$ so we have $m q=n p$ and thus $m n^{-1}=p q^{-1}$.
$\underline{\text { Let us now show that } \varphi \text { is a unitary ring homomorphism. We have } \varphi(\overline{(m, n)}} \square$ $\overline{(p, q)})=\underline{\varphi(\overline{(m q}+p n, n q)})=\left(m q+\underline{\left.p n)(n q)^{-1}=m q q^{-1} \underline{n}^{-1}+p n q^{-1} n^{-1}=m n^{-1}+. .+{ }^{(m p)}\right)}=\right.$ $p q^{-1}=\varphi(\overline{(m, n)})+\varphi(\overline{(p, q)}) ;$ also $\varphi(\overline{(m, n)} \star \overline{(p, q)})=\varphi(\overline{(m p, n q)})=(m p)(n q)^{-1}=$ $m n^{-1} p q^{-1}=\varphi(\overline{(m, n)}) \varphi(\overline{(p, q)})$ and $\varphi(\overline{1,1})=1 \cdot 1^{-1}=1$.
If $m n^{-1}=\varphi(\overline{(m, n)})=0$ then, because $n \neq 0$, we have $m=0$ and $\overline{(m, n)}=\overline{(0,1)}$. So $\operatorname{ker}(\varphi)=\{\overline{(0,1)}\}$ and $\varphi$ is injective. Finally, pick any $q \in \mathbb{Q}$. We have $q=m n^{-1}=$ $\varphi(\overline{(m, n)})$ for some $m \in \mathbb{Z}$ and $n \in \mathbb{Z} \backslash\{0\}$ so $\varphi$ is surjective.

