Math 566 - Homework 6

Solutions

Prof Arturo Magidin

1. Let $R=\mathbb{Z}_6$, and $S=\{2,4\}$. Prove that S is a multiplicative subset of R, and that $S^{-1}R\cong\mathbb{Z}_3$.

   Proof. I will prove this without invoking the Universal Property of the ring of fractions first; I will give a proof invoking this property below.

   Since $6\mathbb{Z}\subseteq 3\mathbb{Z}$, we have a natural map $\psi\colon\mathbb{Z}_6\to\mathbb{Z}_3$ given by $\psi(a+6\mathbb{Z})=a+3\mathbb{Z}$. Note that under this homomorphism, $2+6\mathbb{Z}$ maps to $2+3\mathbb{Z}$, which is a unit; and $4+6\mathbb{Z}$ maps to $4+3\mathbb{Z}=1+4\mathbb{Z}$, which is a unit. In fact, each of them is its own inverse.

   This suggests defining $f\colon S^{-1}R\to\mathbb{Z}_3$ by

   $$\phi\left(\frac{r}{s}\right)=\psi(r)\psi(s)^{-1}=\psi(r)\psi(s)=\psi(rs)=rs+3\mathbb{Z}.$$

   We just need to verify this works.

   First, we check that this is well-defined. Recall that if $s\in S$, then $s^2+3\mathbb{Z}=1+3\mathbb{Z}$, and that $s+3\mathbb{Z}$ is not a zero divisor in $\mathbb{Z}_3$, so it can be cancelled.

   If $\frac{r}{s}=\frac{u}{t}$, then there exists $w\in S$ such that $w(rt-us)=0$. Therefore $wrt=usw$ in $\mathbb{Z}_6$. But this means that $\psi(wrt)=\psi(usw)$, and hence that $\psi(w)\psi(rs)=\psi(w)\psi(us)$. As $\psi(w)$ is not a zero divisor, then $\psi(rs)=\psi(us)$. Thus, $\phi(\frac{r}{s})=\phi(\frac{u}{t})$.

   Next, we have:

   $$\begin{aligned}\phi\left(\frac{r}{s}+\frac{u}{t}\right)&=\phi\left(\frac{rt+us}{st}\right)=(rt+us)(st)+3\mathbb{Z}\\&=(rst^2+uts^2)+3\mathbb{Z}=(rs+ut)+3\mathbb{Z}\\&=(rs+3\mathbb{Z})+(ut+3\mathbb{Z})=\phi\left(\frac{r}{s}\right)+\phi\left(\frac{u}{t}\right),\\\phi(\left(\frac{r}{s}\cdot\frac{u}{t}\right)&=\phi\left(\frac{ru}{st}\right)\\&=\psi(rust)=rust+3\mathbb{Z}\\&=(rs+3\mathbb{Z})(ut+3\mathbb{Z})=\phi\left(\frac{r}{s}\right)\phi\left(\frac{u}{t}\right).\end{aligned}$$

   Thus, we have a ring homomorphism. It is surjective, as $\frac{0}{2}$, $\frac{2}{2}$, and $\frac{4}{2}$ map to $0+3\mathbb{Z}$, $4+3\mathbb{Z}=1+3\mathbb{Z}$, and $8+3\mathbb{Z}=2+3\mathbb{Z}$, respectively.

   Finally, suppose that $\frac{r}{s}$ maps to $0+3\mathbb{Z}$. That means that $rs+3\mathbb{Z}=0+3\mathbb{Z}$, so $3|rs$. Since $s\in\{2,4\}$, then s is relatively prime to 3, so $3|r$. Thus, either $r+6\mathbb{Z}=0+6\mathbb{Z}$, or else $r+6\mathbb{Z}=3+6\mathbb{Z}$. But in the latter case, we have that $\frac{3}{s}=\frac{2(3)}{2s}=\frac{6}{2s}=\frac{0}{2s}$, so in either case we get $\frac{r}{s}=0_{S^{-1}R}$. Thus, ϕ is one-to-one, and hence an isomorphism.

   Alternative solution. Under the homomorphism $\phi(a+6\mathbb{Z})=a+3\mathbb{Z}$ from $\mathbb{Z}_6$ to $\mathbb{Z}_3$, $\phi(2+6\mathbb{Z})=2+3\mathbb{Z}$ is a unit in $\mathbb{Z}_3$, and $\phi(4+6\mathbb{Z})=4+3\mathbb{Z}=1+\mathbb{Z}$ is a unit in $\mathbb{Z}_3$. By the universal property of the ring of fractions, there is a homomorphism $\varphi\colon S^{-1}R\to\mathbb{Z}_3$ induced by ϕ. This map will be given by $\varphi(\frac{r}{s})=\phi(r)\phi(s)^{-1}$. Since the inverse of $2+3\mathbb{Z}$ is $2+3\mathbb{Z}$ and the inverse of $4+3\mathbb{Z}$ is $4+3\mathbb{Z}$, in fact our homomorphism will be given by $\varphi(\frac{r}{s})=\phi(r)\phi(s)=\phi(rs)=rs+3\mathbb{Z}$.

   At this point, we can proceed as above; the universal property guarantees that this is indeed a ring homomorphism that is well-defined, so we can save ourselves the work of verifying these properties. □

2. Let $S = \{\pm 1001^k \mid k \text{ a positive integer}\}$. Let $\varphi\colon \mathbb{Z} \to S^{-1}\mathbb{Z}$ be the canonical map, $\varphi(a) = \frac{1001a}{1001}$. Describe the prime factorization of all $a \in \mathbb{Z}$ such that $\varphi(a)$ is a unit in $S^{-1}\mathbb{Z}$.

Proof. We claim that an integer $a \in \mathbb{Z}$ is mapped to a unit in $S^{-1}\mathbb{Z}$ if and only if a is of the form $a = \pm 7^r 11^s 13^t$, for nonnegative integers r, s, and t. (This is related to the fact that $1001 = 7 \times 11 \times 13$).

Indeed, first let us note that such an integer is indeed a unit in $S^{-1}\mathbb{Z}$: let $a = \pm 7^r 11^s 13^t$, and set $u = r + s + t$. If let $b = \pm 7^{u-r} 11^{u-s} 13^{u-t}$, then $ab = 1001^u$, so

$$\varphi(a)\left(\frac{b}{1001^u}\right) = \left(\frac{1001a}{1001}\right)\left(\frac{b}{1001^u}\right) = \frac{1001(ab)}{1001^{u+1}} = \frac{1001(1001)^u}{1001^{u+1}} = \frac{1001}{1001} = 1_{S^{-1}\mathbb{Z}}.$$

Thus, $\varphi(a)$ is a unit in $S^{-1}\mathbb{Z}$.

Conversely, suppose that $\varphi(a)$ is a unit, and let $\frac{x}{v1001^k}$ be the multiplicative inverse of x, with k a positive integer, $x \in \mathbb{Z}$, and $v = \pm 1$; by changing the sign of x if necessary, we may assume that $v = 1$. Then

$$\varphi(a)\left(\frac{x}{1001^k}\right) = \frac{1001ax}{1001^{k+1}} = 1_{S^{-1}R} = \frac{1001}{1001}.$$

That means that $1001^2(ax) = 1001^{k+2}$, hence $ax = 1001^k$. Thus, a divides $1001^k = 7^k 11^k 13^k$, and therefore $a = \pm 7^r 11^s 13^t$ for some nonnegative integers r, s, and t less than or equal to k. This proves the claim. □

3. Let P be a nonzero prime ideal of $\mathbb{Z}$, and let $\mathbb{Z}_P$ be the localization of $\mathbb{Z}$ at P; that is, $\mathbb{Z}_P = (\mathbb{Z} - P)^{-1}\mathbb{Z}$. Show that we can identify $\mathbb{Z}_P$ with the subring of $\mathbb{Q}$ consisting of the rationals that can be written as $\frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $b \notin P$.

Proof. Take an element $\frac{a}{b} \in \mathbb{Z}_P$; then $b \notin P$ by construction of $\mathbb{Z}_P$, showing that all such elements lie in $\mathbb{Z}_P$. Conversely, let $q \in \mathbb{Q}$, and assume that $q \in \mathbb{Z}_P$. Then we can write $q = \frac{a}{b}$ with $a, b \in \mathbb{Z}$, $b \neq 0$, $\gcd(a, b) = 1$; and we have $q = \frac{r}{s}$ with $r \in \mathbb{Z}$ and $s \notin P$ because $q \in \mathbb{Z}_P$. Thus, $\frac{a}{b} = \frac{r}{s}$, so $sa = rb$. Since $b|as$ and $\gcd(a, b) = 1$, then $b|s$, and hence $b \notin P$ (since $s \notin P$), proving that when we write q in lowest terms, $q = \frac{a}{b}$, then $b \notin P$. □

4. Show that if we view $\mathbb{Z}_P$ as a subring of $\mathbb{Q}$ as in Problem 3, then

$$\bigcap_P \mathbb{Z}_P = \mathbb{Z},$$

where the intersection runs over all nonzero prime ideals of $\mathbb{Z}$.

Proof. Since $\mathbb{Z}$ is a domain and $\mathbb{Z} - P$ does not contain 0, $\mathbb{Z}$ is always identified with a subring of $\mathbb{Z}_P$. That means that $\mathbb{Z}$ is contained in the intersection.

Conversely, suppose that $q \in \mathbb{Q}$ lies in the intersection. Write q in lowest terms, $q = \frac{a}{b}$ with a and b integers, $b > 0$, and $\gcd(a, b) = 1$. If we can also write q as $q = \frac{r}{s}$, then $\frac{r}{s} = \frac{a}{b}$, so $br = as$. That is, $b|as$, and since $\gcd(a, b) = 1$, then $b|s$. Thus, every expression of q as a quotient of integers has denominator that is a multiple of b. Thus, $q \in \mathbb{Z}_P$ if and only if $b \notin P$; if $P = (0)$, this does not put any restrictions on b; if $P = (p)$ with $p > 0$ a prime, then b is not divisible by p. Thus, if q lies in the intersection, then when we express it as a quotient $\frac{a}{b}$ in lowest terms with $b > 0$, we have that b is not divisible by any primes. Thus, $b = 1$, so $q \in \mathbb{Z}$. This proves the intersection is equal to $\mathbb{Z}$. □

5. *Fractions of quotients.* Let R be a commutative ring, I be an ideal of R, and let $\pi\colon R \to R/I$ be the canonical projection onto the quotient.

   (i) Show that if S is a multiplicative subset of R, then $\pi S = \{\pi(s) \mid s \in S\}$ is a multiplicative subset of R/I.

   Proof. If $s, t \in S$, then $\pi(s)\pi(t) = \pi(st) \in \pi(S)$ (since S is multiplicative). □

(ii) Show that $\theta\colon S^{-1}R \to (\pi S)^{-1}(R/I)$ given by $\theta(\frac{r}{s}) = \frac{\pi(r)}{\pi(s)}$ is a well-defined surjective ring homomorphism.

Proof. Suppose that $\frac{r}{s} = \frac{a}{t}$. Then there exists $u \in S$ such that $u(rt - as) = 0$. Applying π we obtain $\pi(u)(\pi(r)\pi(t) - \pi(a)\pi(s)) = 0$, and since $\pi(u), \pi(s), \pi(t) \in \pi(S)$, then $\frac{\pi(r)}{\pi(s)} = \frac{\pi(a)}{\pi(t)}$ in $(\pi S)^{-1}(R/I)$. So θ is well-defined.

We then have

$$\begin{aligned}
\theta\left(\frac{r}{s}\right) + \theta\left(\frac{a}{t}\right) &= \frac{\pi(r)}{\pi(s)} + \frac{\pi(a)}{\pi(t)} = \frac{\pi(r)\pi(t) + \pi(a)\pi(s)}{\pi(s)\pi(t)} = \frac{\pi(rt+as)}{\pi(st)}\\
&= \theta\left(\frac{rt+as}{st}\right) = \theta\left(\frac{r}{s} + \frac{a}{t}\right).\\
\theta\left(\frac{r}{s}\right) \cdot \theta\left(\frac{a}{t}\right) &= \frac{\pi(r)}{\pi(s)} \cdot \frac{\pi(a)}{\pi(t)} = \frac{\pi(r)\pi(a)}{\pi(s)\pi(t)}\\
&= \frac{\pi(ra)}{\pi(st)} = \theta\left(\frac{ra}{st}\right) = \theta\left(\frac{r}{s} \cdot \frac{a}{t}\right).
\end{aligned}$$

Thus, θ is a well-defined homomorphism. Finally, if $\frac{a+I}{\pi(s)} \in (\pi S)^{-1}(R/I)$, then $\theta(\frac{a}{s}) = \frac{\pi(a)}{\pi(s)} = \frac{a+I}{\pi(s)}$, so θ is surjective.

(iii) Recall that $S^{-1}I \triangleleft S^{-1}R$. Prove that $(S^{-1}R)/S^{-1}I \cong (\pi S)^{-1}(R/I)$.

Proof. We have a map from $S^{-1}R$ to $(\pi S)^{-1}(R/I)$, given by θ. So this suggests verifying that the kernel of this map is exactly $S^{-1}I = \{\frac{a}{s} \mid a \in I\}$.

If $\frac{a}{s} \in S^{-1}I$, with $a \in I$, then $\theta(\frac{a}{s}) = \frac{\pi(a)}{\pi(s)} = \frac{\overline{0}}{\pi(s)} = 0$, so $S^{-1}I$ is certainly contained in the kernel.

Now assume that $\frac{r}{s} \in \ker(\theta)$. Then $\frac{\pi(r)}{\pi(s)} = \frac{0}{\pi(s)}$. Therefore, there exists $\pi(t) \in \pi S$ such that $\pi(t)(\pi(r)\pi(s)) = 0 + I$. That means that $rst \in I$. But then we have that

$$\frac{r}{s} = \frac{rst}{sst} \in S^{-1}I,$$

which shows that $\ker(\theta) \subseteq S^{-1}I$.

This proves that $\ker(\theta) = S^{-1}I$, and the First Isomorphism Theorem yields $S^{-1}R/S^{-1}I \cong (\pi S)^{-1}(R/I)$. □

6. *Fractions of fractions.* Let R be a commutative ring, and S a multiplicative subset of R. Let T be the a multiplicative subset of $S^{-1}R$, and let

$$S_* = \left\{ r \in R \;\middle|\; \frac{r}{s} \in T \text{ for some } s \in S \right\}.$$

(i) Show that S_* is a multiplicative subset of R.

Proof. First, since T is a multiplicative subset of $S^{-1}R$, there is some element $\frac{r}{s} \in T$, and therefore there is some $r \in S_*$; thus, S_* is nonempty.

Let $a, b \in S_*$. We need to show that $ab \in S_*$. Since $a \in S_*$, there exists $s \in S$ such that $\frac{a}{s} \in T$; likewise, there exists $t \in S$ with $\frac{b}{t} \in T$. Since T is a multiplicative subset, $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \in T$. Since $st \in S$, it follows that $ab \in S_*$, as required. Thus, S_* is indeed a multiplicative subset. □

(ii) Prove that if $t \in S_*$ and $s \in S$, then $sr \in S_*$.

Proof. Since $t \in S_*$, there exists $u \in S$ such that $\frac{t}{u} \in T$. Since $s \in S$, we know that $\frac{st}{su} = \frac{t}{u} \in T$, and therefore there is an element $v \in S$ (namely $v = su$) such that $\frac{st}{v} \in T$; by definition of S_*, this means that $st \in S_*$, as claimed. □

(iii) Define $f\colon T^{-1}(S^{-1}R) \to S_*^{-1}R$ by $f(\frac{a/t}{b/u}) = \frac{au}{bt}$. Show that this is a well-defined ring homomorphism.

Proof. Apologies for the coming change of notation; the choice above is less than optimal, because we would be inclined to think that the element t lies in T, when in fact it lies in S. So I will switch to a denominator of the form $\frac{t}{u}$ as an element of T.

What is the intuition behind the isomorphism of $T^{-1}(S^{-1}R)$ and $S_*^{-1}R$ that we will establish in part (iv)? The first is a fraction ring of a fraction ring, so its elements will be "fractions of fractions." If we have a "fraction of fractions", then this ought to be expressible as a regular fraction (i.e., an element of $S_*^{-1}R$); so what we hope is that the usual identity

$$\frac{\frac{a}{s}}{\frac{t}{u}} = \frac{au}{st}$$

will hold, where $a \in R$, $s \in S$, and $\frac{t}{u} \in T$ (hence $t \in S_*$). Note that this makes sense, because $st \in S_*$ by part (ii).

Let $f\colon T^{-1}(S^{-1}R) \to S_*^{-1}R$ be given by

$$f\left(\frac{\frac{a}{s}}{\frac{t}{u}}\right) = \frac{au}{st},$$

where $a \in R$, $s, u \in S$, and $\frac{t}{u} \in T$. By part (ii), this at least makes some sense as $st \in S_*$, so $\frac{au}{st}$ is indeed an element of $S_*^{-1}R$. We do need to show that this is well-defined.

To show this is well defined we are going to have to unwind a couple of definitions. Suppose that

$$\frac{\frac{a}{s}}{\frac{t}{u}} = \frac{\frac{b}{r}}{\frac{v}{w}} \text{ in } T^{-1}(S^{-1}R);$$

we want to show that $\frac{au}{st} = \frac{bw}{rv}$ in $S_*^{-1}R$.

To say that

$$\frac{\frac{a}{s}}{\frac{t}{u}} = \frac{\frac{b}{r}}{\frac{v}{w}} \text{ in } T^{-1}(S^{-1}R)$$

means that there exists $\frac{q}{z} \in T$ such that $\frac{q}{z}\left(\frac{av}{sw} - \frac{bt}{ru}\right) = 0_{S^{-1}R}$. Doing the operations, we obtain that $\frac{qavru - qbtsw}{zswbt} = 0_{S^{-1}R}$. Thus, there exists $s' \in S$ such that $s'(qavru - qbtsw) = 0$, or $s'q(avru - btsw) = 0$. Now, note that since $\frac{q}{z} \in T$, we have $q \in S_*$, and therefore $s'q \in S_*$. Thus, $s'q(avru - btsw) = 0$ is exactly the condition we need for $\frac{au}{st} = \frac{bw}{rv}$ to hold in $S_*^{-1}R$, so the the map is indeed well defined.

To show f is a ring homomorphism, we have:

$$\begin{aligned} f\left(\frac{\frac{a}{s}}{\frac{t}{u}} + \frac{\frac{b}{r}}{\frac{v}{w}}\right) &= f\left(\frac{\frac{av}{sw} + \frac{bt}{ru}}{\frac{tv}{uw}}\right) = f\left(\frac{\frac{avru+btsw}{swru}}{\frac{tv}{uw}}\right) = \frac{(avru + btsw)(uw)}{(swru)(tv)}. \\ f\left(\frac{\frac{a}{s}}{\frac{t}{u}}\right) + f\left(\frac{\frac{b}{r}}{\frac{v}{w}}\right) &= \frac{au}{st} + \frac{bw}{rv} = \frac{aurv + bwst}{strv}. \end{aligned}$$

Note that the two answers are equal, since the crossproducts are equal:

$$(avru + btsw)(uw)(strv) = (swru)(tv)(aurv + bwst).$$

Thus, f is additive. To show f is multiplicative, we have:

$$\begin{aligned} f\left(\frac{\frac{a}{s}}{\frac{t}{u}} \cdot \frac{\frac{b}{r}}{\frac{v}{w}}\right) &= f\left(\frac{\frac{ab}{sr}}{\frac{tv}{uw}}\right) = \frac{abuw}{srtv}. \\ f\left(\frac{\frac{a}{s}}{\frac{t}{u}}\right) \cdot f\left(\frac{\frac{b}{r}}{\frac{v}{w}}\right) &= \frac{au}{st} \cdot \frac{bw}{rv} = \frac{aubw}{strv}. \end{aligned}$$

Thus, f is also multiplicative, and so is a ring homomorphism. □

(iv) Prove that $T^{-1}(S^{-1}R) \cong S_*^{-1}R$.

Proof. We show that the map f from part (iii) is in fact an isomorphism. To show that f is one-to-one, suppose that

$$f\left(\frac{\frac{a}{s}}{\frac{t}{u}}\right) = \frac{au}{st} = \frac{0}{t}$$

(we can use $\frac{0}{t}$, since $t \in S_*$), which means that there exists $v \in S_*$ such that $vaut = 0$. We want to show that $\frac{(a/s)}{(t/u)}$ is the zero element of $T^{-1}(S^{-1}R)$. Indeed, since $vt \in S_*$, there exists $z \in S$ such that $\frac{vt}{z} \in T$. Then $\frac{vt}{z}\left(\frac{a}{s}\right) = \frac{vat}{zs} = 0_{S^{-1}R}$, because $u \in S$ satisfies $uvat = 0$. Thus, there is an element of T which, multiplied by $\frac{a}{s}$, is equal to zero, so the element $\frac{a/s}{t/u}$ is the zero element of $T^{-1}(S^{-1}R)$, as claimed. Thus f is indeed one-to-one

Finally, to show f is onto, let $\frac{a}{t} \in S_*^{-1}R$. That means that there exists $s \in S$ such that $\frac{t}{s} \in T$. Then we can look at

$$f\left(\frac{\frac{a}{s}}{\frac{t}{s}}\right) = \frac{as}{ts} = \frac{a}{t}.$$

Thus, f is a ring isomorphism, as desired. □

NOTE: This means that one can realize a ring of quotients of a ring of quotients of R as a ring of quotients of R; this is analogous to the fact that a quotient of a quotient of R can be realized as a quotient of R (the Third Isomorphism Theorem).

Remark: In fact, there is a "fancy proof" that $S_*^{-1}R \cong T^{-1}(S^{-1}R)$, using the universal property of the ring of fractions.

We have the maps $\varphi_S\colon R \to S^{-1}R$ and $\varphi_T\colon S^{-1}R \to T^{-1}(S^{-1}R)$. Composing them, we get a map $f\colon R \to T^{-1}(S^{-1}R)$. It is now straightforward to check that if $t \in S_*$, then $f(t)$ is a unit in $T^{-1}(S^{-1}R)$: there exists $s \in S$ such that $\frac{t}{s} \in T$, and so $\varphi_S(t) = \frac{ts}{s} = \frac{t}{s}\frac{ss}{s}$ is an element of T times a unit of $S^{-1}R$. Since φ_T maps units to units, and elements of T to units, $f(t) = \varphi_T(\varphi_S(t))$ is a unit in $T^{-1}(S^{-1}R)$. By the universal property of the ring of fractions, there is a unique homomorphism $\psi\colon S_*^{-1}R \to T^{-1}(S^{-1}R)$ such that $\psi(r) = f(r)$ for all $r \in R$. Now let $t \in S_*$, and define the map $g\colon S^{-1}R \to S_*^{-1}R$ by mapping $\frac{a}{s}$ to $\frac{at}{st}$; this makes sense, since $st \in S_*$. It is a ring homomorphism:

$$\begin{aligned} g\left(\frac{a}{s} + \frac{b}{s'}\right) &= g\left(\frac{as' + bs}{ss'}\right) = \frac{(as' + bs)t}{ss't}, \\ g\left(\frac{a}{s}\right) + g\left(\frac{b}{s'}\right) &= \frac{at}{st} + \frac{bt}{s't} = \frac{as'tt + bstt}{ss'tt} = \frac{as't + bst}{ss't}. \\ g\left(\frac{a}{s}\cdot\frac{b}{s'}\right) &= \frac{abt}{ss't} = \frac{abtt}{ss'tt} = \frac{at}{st}\cdot\frac{bt}{s't} = g\left(\frac{a}{s}\right)g\left(\frac{b}{s'}\right). \end{aligned}$$

And if $\frac{u}{s} \in T$, then $g(\frac{u}{s}) = \frac{ust}{st}$ is a unit in $S_*^{-1}R$, because $u, t \in S_*$ and $s \in S$, so $ust \in S_*$. Thus, g is a ring homomorphism from $S^{-1}R$ to $S_*^{-1}R$ that sends every element of T into a unit. This induces a homomorphism $\phi\colon T^{-1}(S^{-1}R) \to S_*^{-1}R$ such that $\phi(\frac{r}{s}) = \frac{rt}{st}$ for all $\frac{r}{s} \in S^{-1}R$.

It is now an easy computation to show that ψ and ϕ are inverses of each other, so they are isomorphisms. □