Math 55a, Fall 2004

Eighth Assignment, Solutions
Adapted from Andrew Cotton and George Lee

Problem 1.

Note: There are two possible definitions of "subring-with-unit." The usual notion says that D is a subring-with-unit of a ring $(R, +, \cdot)$ if $D \subset F$ and $(D, +|_D, \cdot|_D)$ is a ring with same multiplicative identity as R. Alternatively, one can say that D is a subring-with-unit of a ring R if it is *isomorphic* as a ring-with-unit to some D' which is a subring-with-unit of R in the usual sense. There is little difference between the two definitions; we use both in this solution at the sacrifice of some rigor but at the benefit of avoiding excessive notation.

Recall that in an integral domain (or in a field), addition and multiplication are commutative; and for $a, b, c \in D$, if $ac = bc$ then $(a - b)c = 0 \implies a = b$ or $c = 0$. Also, in this proof given a set S, we write $S^* = S - \{0\}$.

(a)

• *If K is a field with multiplicative inverse ν containing D as a subring-with-unit, then it is a quotient field of D iff $K = \{a \cdot \nu(b) \mid a, b \in D \times D^*\}$.*

Since K contains D as a subring-with-unit, its additive and multiplicative identities 0 and 1 are the same as the identities in D.

For $(a, b), (c, d) \in D \times D^*$, we have

$$a \cdot \nu(b) + c \cdot \nu(d) = (ad + bc) \cdot \nu(bd), \qquad a\nu(b) \cdot c\nu(d) = (ac) \cdot \nu(bd),$$
$$-a \cdot \nu(b) = (-a) \cdot \nu(b), \qquad \nu(a \cdot \nu(b)) = b \cdot \nu(a),$$
$$1 \cdot \nu(1) = 1.$$

Thus $K' = \{a \cdot \nu(b) \mid (a, b) \in D \times D^*\}$ is a subfield of K. And for each $d \in D$, K' also contains $d \cdot \nu(1) = d$ so it contains D as a subring-with-unit. So if K is a quotient field, K' cannot be a *proper* subfield and we must have $K = K'$.

Conversely, suppose $K = \{a \cdot \nu(b) \mid (a,b) \in D \times D^*\}$. If K' is a subfield of K containing D as a subring-with-unit, it is closed under multiplication and the multiplicative inverse; so it must contain $\{a \cdot \nu(b) \mid (a,b) \in D \times D^*\} = K$. Thus no proper subfield of K can contain D as a subring-with-unit, and K is a quotient field of D.

- *Any two quotient fields of D are isomorphic.*

Suppose we have two quotient fields K_1 and K_2 of D, where $\cdot$ and ν_1 represent multiplication and the multiplicative inverse in K_1; and $\times$ and ν_2 represent multiplication and the multiplicative inverse in K_2. From before, we know that $K_1 = \{a \cdot \nu_1(b) \mid (a,b) \in D \times D^*\}$ and that $K_2 = \{a \times \nu_2(b) \mid (a,b) \in D \times D^*\}$. Also, since D is a subring of both fields, $a \cdot b = a \times b$ for all $a, b \in D$.

Now consider the function $\phi : K_1 \to K_2$ defined by $\phi(a \cdot \nu_1(b)) = a \times \nu_2(b)$. ϕ is well-defined and injective because for $(a,b), (a',b') \in D \times D^*$,

$$\begin{aligned}
& a \cdot \nu_1(b) = a' \cdot \nu_1(b') \\
& \iff a \cdot \nu_1(b) \cdot b \cdot b' = a' \cdot \nu_1(b') \cdot b' \cdot b \\
& \iff a \cdot b' = a' \cdot b \\
& \iff a \times b' = a' \times b \\
& \iff a \times b' \times \nu_2(b') \times \nu_2(b) = a' \times b \times \nu_2(b) \times \nu_2(b') \\
& \iff a \times \nu_2(b) = a' \times \nu_2(b').
\end{aligned}$$

It is also surjective since every element of K_2 can be written in the form $a \times \nu_2(b)$ for $(a,b) \in D \times D^*$; thus, ϕ is a bijective map.

Finally, ϕ is a homomorphism because it preserves addition and multiplication:

$$\begin{aligned}
\phi(a \cdot \nu_1(b) + c \cdot \nu_1(d)) &= \phi((ad+bc) \cdot \nu_1(bd)) \\
&= (ad+bc) \times \nu_2(bd) \\
&= a \times \nu_2(b) + c \times \nu_2(b) \\
&= \phi(a \cdot \nu_1(b)) + \phi(c \cdot \nu_1(d))
\end{aligned}$$

and

$$\begin{aligned}
\phi\left((a \cdot \nu_1(b)) \cdot (c \cdot \nu_1(d))\right) &= \phi((ac) \cdot \nu_1(bd)) \\
&= (ac) \times \nu_2(bd) \\
&= (a \times \nu_2(b)) \times (c \times \nu_2(d)) \\
&= \phi(a \cdot \nu_1(b)) \times \phi(c \cdot \nu_1(d)).
\end{aligned}$$

Thus ϕ is an isomorphism between the quotient fields, as desired.

- *A quotient field of D exists.*

Define the relation $\sim$ on $D \times D^*$ as follows: $(a, b) \sim (c, d) \iff ad = cb$. Observe that

$$
\begin{aligned}
&(a,b) \sim (a,b);\\
&(a,b) \sim (c,d) \iff ad = cb \iff cb = ad \iff (c,d) \sim (a,b); \text{ and}\\
&(a,b) \sim (c,d), (c,d) \sim (e,f) \Longrightarrow ad = cb, cf = ed\\
&\quad \Longrightarrow \begin{cases} \text{(if } c = 0\text{)} & ad = ed = 0 \Longrightarrow a = e = 0 \\ \text{(if } c \neq 0\text{)} & (ad)(cf) = (cb)(ed) \Longrightarrow (af)(cd) = (eb)(cd) \end{cases}\\
&\quad \Longrightarrow af = eb \Longrightarrow (a,b) \sim (e,f),
\end{aligned}
$$

so $\sim$ is an equivalence relation.

Define $K = (D \times D^*)/\sim$, where $\frac{a}{b}$ is the equivalence class containing (a, b). We define addition and multiplication in K as follows in the left column.

$$
\begin{array}{ll}
\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, & (ab_1)d^2 + bb_1cd = (ba_1)d^2 + bb_1cd \Longrightarrow (ad + bc)(b_1d) = (bd)(a_1d + b_1c) \\
\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. & (ab_1)cd = (ba_1)cd \Longrightarrow (ac)(b_1d) = (bd)(a_1c)
\end{array}
$$

The column on the right shows that these operations are well-defined for different representatives $(a, b), (a_1, b_1) \in D \times D^*$ of the same equivalence class (and by the same logic, for different representatives of $\frac{c}{d}$). And all the resulting "fractions" are in K because bd and b_1d are nonzero as long as b, b_1, d are.

Because addition and multiplication are closed, associative, and commutative in D and D^*, it's easily seen that they are also closed, associative, and commutative in K. The distributive property in K also follows easily. It's also clear that $\frac{0}{1}$ and $\frac{1}{1}$ are additive and multiplicative identities. Because $\frac{0}{1} = \frac{0}{c}$ and $\frac{1}{1} = \frac{c}{c}$ for all $c\ inD^*$, we see that $\frac{-a}{b}$ is an additive inverse of $\frac{a}{b} \in K$ and that $\frac{b}{a}$ is a multiplicative inverse of $\frac{a}{b} \in K^*$. Therefore $(K, +, \cdot)$ satisfies the axioms for a field.

Consider the map $\varphi : D \to K$ defined by $d \mapsto \frac{d}{1}$. This map is a homomorphism because $\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1}$ and $\frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1}$; also, it maps the multiplicative identity in D to the multiplicative identity in K. Hence, φ is a homomorphism of rings-with-unit, and $D' = \varphi(D)$ is a subring-with-unit of K (in the usual sense). For $d \neq 0$, $\frac{d}{1} \neq \frac{0}{1}$, so $\varphi : D \to \varphi(D)$ is actually an *isomorphism* of rings-with-unit. Therefore, D is a subring-with-unit of K (in the modified sense).

And since $K = \{r \cdot \nu(s) \mid r, s \in R \times R^*\}$, from our first claim it is a quotient field. Thus K is a quotient field of R, or equivalently, D.

(b) Construct the quotient field K of $D = \mathbb{Z}$ as in part (a), and consider the map $\Phi : \mathbb{Q} \to K$ defined by $\frac{a}{b} \mapsto \frac{a}{b}$ for $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. (What suggestive notation!) Because $\frac{a}{b} = \frac{c}{d}$ in $\mathbb{Q}$ iff $ad = bc$, Φ is well-defined. Because $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ in both $\mathbb{Q}$ and K, Φ is a field homomorphism. Finally, nonzero elements of $\mathbb{Q}$ are mapped to nonzero elements of K, implying that Φ must actually be an isomorphism. Hence $\mathbb{Q} \cong K$, as desired.

(c) The quotient field is the set of equivalence classes of "rational functions" $\frac{P}{Q}$ where $P, Q \in K[x]$, Q is nonzero. Without having to describe it in terms of equivalence classes, we could instead say the quotient field is the set of expressions $\frac{P}{Q}$ in "simplest terms": that is, where $P, Q \in K[x]$, Q is nonzero and monic, and P and Q share no common "nonconstant" (i.e., with degree less than one) polynomial divisor.

Problem 2.

(solution due to Gabriel Carroll, Andy Cotton, and George Lee)

Products $\prod$, sums $\sum$, and direct sums $\bigoplus$ in this solution refer to products, sums, and direct sums taken over all $\alpha \in A$. Let (f_α) denote the element $f \in \prod \mathrm{Hom}(M_\alpha, N)$ whose α-coordinate is f_α. For $\beta \in A$, let p_β denote the projection from $\bigoplus M_\alpha$ to M_β. In addition, let $i_\beta : M_\beta \to \bigoplus M_\alpha$ be the map such that $i_\beta(m)$ has α-coordinate 0 for $\alpha \neq \beta$ and β-coordinate m. It is easy to verify that i_β and p_β are homomorphisms of N-modules. Also, for $x \in \bigoplus M_\alpha$ observe that $x = \sum i_\alpha(p_\alpha(x))$.

Define

$$\begin{aligned} \psi \quad : \quad \prod \mathrm{Hom}(M_\alpha, N) &\to \mathrm{Hom}(\bigoplus M_\alpha, N), \\ f \quad &\mapsto \quad \psi_f, \end{aligned}$$

where if $f = (f_\alpha)$ then $\psi_f(x) = \sum f_\alpha(p_\alpha(x))$ for all $x \in \bigoplus M_\alpha$. We claim this is an isomorphism. We must check four properties: (i) ψ is well-defined; (ii) ψ is injective; (iii) ψ is surjective; (iv) ψ is a homomorphism of N-modules.

(i) Fix $f = (f_\alpha) \in \prod \mathrm{Hom}(M_\alpha, N)$. For $x \in \bigoplus M_\alpha$, $p_\beta(x) \neq 0$ for finitely many $\beta \in A$, so $\sum f_\alpha(p_\alpha(x))$ is well-defined. However, we must verify that ψ_f is actually in $\mathrm{Hom}(\bigoplus M_\alpha, N)$. Indeed, suppose we have

$r, s \in N$ and $x, y \in \bigoplus M_\alpha$. Because p_α and f_α are homomorphisms of N-modules for each $\alpha \in A$, we have

$$\begin{aligned} \psi_f(rx+sy) &= \sum f_\alpha(p_\alpha(rx+sy)) \\ &= \sum f_\alpha(rp_\alpha(x)+sp_\alpha(y)) \\ &= \sum (rf_\alpha(p_\alpha(x))+sf_\alpha(p_\alpha(y))) \\ &= r\sum f_\alpha(p_\alpha(x)) + s\sum f_\alpha(p_\alpha(y)) \\ &= r\psi_f(x)+s\psi_f(y), \end{aligned}$$

where we may separate the sums because $f_\alpha(p_\alpha(x))$ and $f_\alpha(p_\alpha(y))$ are nonzero for only finitely many $\alpha \in A$. Hence, ψ_f is indeed a homomorphism of N-modules.

(ii) Next we prove that ψ is injective. Suppose that $f = (f_\alpha)$ and $g = (g_\alpha)$ are elements in $\prod \mathrm{Hom}(M_\alpha, N)$ such that $\psi_f = \psi_g$. Then

$$f_\alpha(m) = \psi_f(m) = \psi_g(m) = g_\alpha(m).$$

But this is true for *all* $m \in M_\alpha$, so $f_\alpha = g_\alpha$. And this is true for *all* $\alpha \in A$, so we must have $f = g$, as desired.

(iii) Third, we prove ψ is surjective. Given any $\sigma \in \mathrm{Hom}(\bigoplus M_\alpha, N)$, for each $\alpha \in A$ define $f_\alpha : M_\alpha \to N$ by $f_\alpha = \sigma \circ i_\alpha$. Because σ and i_α are both homomorphisms of N-modules, so is f_α. Writing $f = (f_\alpha)$, for any $x \in \bigoplus M_\alpha$ we have

$$\begin{aligned} \psi_f(x) &= \textstyle\sum f_\alpha(p_\alpha(x)) \\ &= \textstyle\sum \sigma(i_\alpha(p_\alpha(x))) \\ &= \sigma\left(\textstyle\sum i_\alpha(p_\alpha(x))\right) && \text{since } \sigma \text{ preserves addition of finitely many nonzero terms} \\ &= \sigma(x). && \text{from our initial observations} \end{aligned}$$

Hence, $\psi_f = \sigma$, as needed.

(iv) Finally, we prove that ψ is a homomorphism of N-modules. Suppose we have $f = (f_\alpha)$ and $g = (g_\alpha)$ in $\prod \mathrm{Hom}(M_\alpha, N)$, and scalars r and s in N. By the definition of addition and scalar multiplication in each $\mathrm{Hom}(M_\alpha, N)$, we have $(rf_\alpha + sg_\alpha)(m) = rf_\alpha(m) + sg_\alpha(m)$ for all $m \in M_\alpha$. Similarly, $(r\psi_f + s\psi_g)(x) = r\psi_f(x) + s\psi_g(x)$ for all $x \in \bigoplus M_\alpha$. Therefore, for all such x, we have

$$\begin{aligned}
\psi_{rf+sg}(x) &= \sum (rf_\alpha + sg_\alpha)(p_\alpha(x)) \\
&= \sum \left(rf_\alpha(p_\alpha(x)) + sg_\alpha(p_\alpha(x))\right) \\
&= r\sum f_\alpha(p_\alpha(x)) + s\sum g_\alpha(p_\alpha(x)) \\
&= r\psi_f(x) + s\psi_g(x) \\
&= (r\psi_f + s\psi_g)(x),
\end{aligned}$$

where again we may separate the sums because $f_\alpha(p_\alpha(x))$ and $g_\alpha(p_\alpha(x))$ are nonzero for only finitely many $\alpha \in A$. Hence ψ is indeed a homomorphism of N-modules. This completes the proof.