M 431: Assignment 10

Nathan Stouffer

Page 137 — Problem 40

Problem. Prove that a finite domain is a division ring. As a consequence, show that $\mathbb{Z}_p$ is a field if p is prime.

Proof. Let R be a finite domain. Then for any $a, b \in R$, we know that $ab = 0$ implies that $a = 0$ or $b = 0$. Equivalently, $a, b \neq 0$ means that $ab \neq 0$. Now we wish to show that R is a division ring. Since R is a domain, we only must verify that R contains a multiplicative identity and every non-zero element has an multiplicative inverse in R. That is we must show that $R' = R \backslash \{0\}$ is a group taken with the product in R.

Since R is finite, take $|R| = n \leq +\infty$, which means that $|R'| = n - 1$. Take any $r \in R'$ and consider the set of elements $\{r, r^2, \ldots, r^n\}$. We know $r^k \neq 0$ for all k becuase R is a domain and $r \neq 0$. Now since $|R'| = n-1$ we must have $r^i = r^j$ for some $0 \leq i < j \leq n$. Let $l = j - i > 0 \implies i = j + l = l + j$ and consider

$$r^l r^i = r^l r^j = r^{l+j} = r^i = r^{j+l} = r^j r^l = r^i r^l$$

Then if we take $1 = r^l$, we have a multiplicative identity: $1r^i = r^i 1 = r^i$. Furthermore, consider $r^{l-1}r = r^{l-1+1} = r^l = 1$ and $rr^{l-1} = r^{1+l-1} = r^l = 1$. So we have an inverse as well. By arbitrariness of r, we have shown that there is an identity and inverse for each $r \in R' = R \backslash \{0\}$, thus R is a division ring.

Let's think about $\mathbb{Z}_p$ for p prime. We already know $\mathbb{Z}_p$ to a finite, commutative ring so we need only verify that $\mathbb{Z}_p$ is a domain. Then the previous result in this problem tells us that $\mathbb{Z}_p$ is a division ring, then commutivity gives us that the $\mathbb{Z}_p$ is a field. To check that $\mathbb{Z}_p$ is a domain, suppose that we have some $a, b \neq 0$ where $ab = 0$. Then $ab \equiv 0 \mod p \implies p \mid (ab - 0) \implies p \mid ab$ which means that the prime factorization of ab must include p. But since p is prime, this means that p must divide either a, b but this is a contradiction. Thus we have shown that $a, b \neq 0 \in \mathbb{Z}_p \implies ab \neq 0$, which is equivalent to showing that $\mathbb{Z}_p$ is a division ring.

□

Page 134 — Problem 10

Problem. Let R be any ring with unit, and S the ring of 2×2 matrices over R.

(a) Check the associative law of multiplication in S.

(b) Show that $T = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \middle| \, a, b, c \in R \right\}$ is a subring of S.

(c) Show that $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ as an inverse in T if and only if a and c have inverses in R. In that case, write down $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}^{-1}$ explicitly.

Proof. **(a)** This amounts to just checking the equality of evaluating left to right and then right to left of three matrics in S. Let's start with left to right:

$$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{bmatrix} \right) \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a\bar{a} + b\bar{c} & a\bar{b} + b\bar{d} \\ c\bar{a} + d\bar{c} & c\bar{b} + d\bar{d} \end{bmatrix} \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$$

$$= \begin{bmatrix} (a\bar{a} + b\bar{c})a' + (a\bar{b} + b\bar{d})c' & (a\bar{a} + b\bar{c})b' + (a\bar{b} + b\bar{d})d' \\ (c\bar{a} + d\bar{c})a' + (c\bar{b} + d\bar{d})c' & (c\bar{a} + d\bar{c})b' + (c\bar{b} + d\bar{d})d' \end{bmatrix} = \begin{bmatrix} a\bar{a}a' + b\bar{c}a + a\bar{b}c' + b\bar{d}c' & a\bar{a}b' + b\bar{c}b' + a\bar{b}d' + b\bar{d}' \\ c\bar{a}a' + d\bar{c}a' + c\bar{b}c' + d\bar{d}c' & c\bar{a}b' + d\bar{c}b' + c\bar{b}d' + d\bar{d}d' \end{bmatrix}$$

and now right to left:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \left(\begin{bmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{bmatrix} \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \bar{a}a' + \bar{b}c' & \bar{a}b' + \bar{b}d' \\ \bar{c}a' + \bar{d}c' & \bar{c}b' + \bar{d}d' \end{bmatrix}$$

$$= \begin{bmatrix} a(\bar{a}a' + \bar{b}c') + b(\bar{c}a' + \bar{d}c') & a(\bar{a}b' + \bar{b}d') + b(\bar{c}b' + \bar{d}d') \\ c(\bar{a}a' + \bar{b}c') + d(\bar{c}a' + \bar{d}c') & c(\bar{a}b' + \bar{b}d') + d(\bar{c}b' + \bar{d}d') \end{bmatrix} = \begin{bmatrix} a\bar{a}a' + a\bar{b}c' + b\bar{c}a' + b\bar{d}c' & a\bar{a}b' + a\bar{b}d' + b\bar{c}b' + b\bar{d}d' \\ c\bar{a}a' + c\bar{b}c' + d\bar{c}a' + b\bar{d}c' & c\bar{a}b' + c\bar{b}d' + d\bar{c}b' + d\bar{d}d' \end{bmatrix}$$

Then each entry of the matrix is equal since R with $+$ is an abelian group.

(b) To show that set of upper diagonal matrices T over a ring R, we must show that for all $A, B \in T$ that $A \pm B \in T$ and $AB \in T$. Before doing so, note that since $a = a + 0$ for all $a \in R$, we must have $ba = b(a + 0) = ba + b0 \iff b0 = ba - ba = 0$ where b is arbitrary in R. Now consider $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}, B = \begin{bmatrix} \bar{a} & \bar{b} \\ 0 & \bar{c} \end{bmatrix} \in T$. $A \pm B$ is in T since each element in the sum will be the sum of two elements of R and the bottom left entry is $0 + 0 = 0$.

$$AB = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} \bar{a} & \bar{b} \\ 0 & \bar{c} \end{bmatrix} = \begin{bmatrix} a\bar{a} + b0 & a\bar{b} + b\bar{c} \\ 0\bar{a} + c0 & 0\bar{b} + c\bar{c} \end{bmatrix} = \begin{bmatrix} a\bar{a} & a\bar{b} + b\bar{c} \\ 0 & c\bar{c} \end{bmatrix} \in T$$

So T is a subing of S.

(c) We now discuss when $A \in T$ has an inverse. Suppose for some fixed $A \in T$ there exists $A^\star$ such that $AA^\star = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Then

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} \bar{a} & \bar{b} \\ 0 & \bar{c} \end{bmatrix} = \begin{bmatrix} a\bar{a} + b0 & a\bar{b} + b\bar{c} \\ 0\bar{a} + c0 & 0\bar{b} + c\bar{c} \end{bmatrix} = \begin{bmatrix} a\bar{a} & a\bar{b} + b\bar{c} \\ 0 & c\bar{c} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

which implies that $a\bar{a} = 1 = c\bar{c}$. If we instead multiply $A^\star A$ then we find that $\bar{a}a = 1 = \bar{c}c$ so both $a, c \in R$ have multiplicative inverses. Now going the other direction, suppose that $a, c \in R$ have multiplicative inverses $a^{-1}, c^{-1} \in R$. For $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ choose $A^\star = \begin{bmatrix} a^{-1} & a^{-1}(-bc^{-1}) \\ 0 & c^{-1} \end{bmatrix}$ Now consider the product

$$AA^\star = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} a^{-1} & a^{-1}(-bc^{-1}) \\ 0 & c^{-1} \end{bmatrix} = \begin{bmatrix} aa^{-1} + b0 & aa^{-1}(-bc^{-1}) + bc^{-1} \\ 0a^{-1} + c0 & 0a^{-1}(-bc^{-1}) + cc^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The commutation $A^\star A$ also equals I, thus $A \in T$ has an inverse when a^{-1}, c^{-1} exist in R.

$\square$

Page 135 — Problem 23

Problem. Define the map $*$ in the quaternions by taking

$$\alpha_0 + \alpha_1 i + \alpha_j + \alpha_3 k \mapsto \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$$

Then show that:

(a) $x^{**} = (x^*)^* = x$
(b) $(x+y)^* = x^* + y^*$
(c) $xx^* = x^*x$ is real an nonnegative
(d) $(xy)^* = y^*x^*$

Proof. **(a)** Take $x = \alpha_0+\alpha_1 i+\alpha_j+\alpha_3 k$ a quaternion. Let's begin with $(x^*)^* = ((\alpha_0+\alpha_1 i+\alpha_j+\alpha_3 k)^*)^* = (\alpha_0 - \alpha_1 i - \alpha_j - \alpha_3 k)^* = \alpha_0 + \alpha_1 i + \alpha_j + \alpha_3 k = x$.

(b) Now for quaternions x, y: $(x+y)^* = (\alpha_0 + \alpha_1 i + \alpha_j + \alpha_3 k + \beta_0 + \beta_1 i + \beta_j + \beta_3 k)^* = ((\alpha_0 + \beta_0) + (\alpha_1+\beta_1)i + (\alpha_2+\beta_2)j + (\alpha_3+\beta_3)k)^* = (\alpha_0+\beta_0) - (\alpha_1+\beta_1)i - (\alpha_2+\beta_2)j - (\alpha_3+\beta_3)k = \alpha_0 - \alpha_1 i - \alpha_j - \alpha_3 k + \beta_0 - \beta_1 i - \beta_j - \beta_3 k = x^* + y^*$

(c) For a quaterion $x = \alpha_0 + \alpha_1 i + \alpha_j + \alpha_3 k$, we can use the definition in the textbook for xx^* which gives

$$\begin{aligned}
\gamma_0 &= \alpha_0\alpha_0 + \alpha_1\alpha_1 + \alpha_2\alpha_2 + \alpha_3\alpha_3 \\
\gamma_1 &= 0 \\
\gamma_2 &= 0 \\
\gamma_3 &= 0
\end{aligned}$$

Since real numbers commute with multiplication this is also the value for x^*x. Further it is entirely real and a sum of squares is non-negative.

(d) For $(xy)^*$, we have

$$\begin{aligned}
\gamma_0 &= \alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3 \\
\gamma_1 &= -\alpha_0\beta_1 - \alpha_1\beta_0 - \alpha_2\beta_3 + \alpha_3\beta_2 \\
\gamma_2 &= -\alpha_0\beta_2 + \alpha_1\beta_3 - \alpha_2\beta_0 - \alpha_3\beta_1 \\
\gamma_3 &= -\alpha_0\beta_3 - \alpha_1\beta_2 + \alpha_2\beta_1 - \alpha_3\beta_0
\end{aligned}$$

which turns out to be the exact same as the formula for y^*x^*.

□

Page 135 — Problem 24

Problem. Use $*$, define $|x| = \sqrt{xx^*}$. Show that $|xy| = |x||y|$ for any two quaternions x and y, by using parts (c) and (d) of problem 23.

Proof. Before we show this, note that by the multiplication rule of quaternions, we have $xy = yx$ for any quaternion y when x is a real number (i, j, k components are 0). This can be check by hand with the multiplicatin rule. Now consider $|xy| = \sqrt{(xy)(xy)^*} = \sqrt{(xy)(y^*x^*)} = \sqrt{xyy^*x^*}$. Then since $yy^* \in \mathbb{R}$ we can say that $\sqrt{xyy^*x^*} = \sqrt{xx^*yy^*} = \sqrt{xx^*}\sqrt{yy^*} = |x||y|$ as desired.

□

Page 135 — Problem 25

Problem. Using the result of problem 24 to prove Lagrange's Identity.

Proof. For two quaterions x, y and their product xy, Lagrange's identity is

$$(\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)(\beta_0^2 + \beta_1^2 + \beta_2^2 + \beta_3^2) = (\gamma_0^2 + \gamma_1^2 + \gamma_2^2 + \gamma_3^2)$$

Here the LHS is $xx^*yy^* = |x|^2|y|^2 = (|x||y|)^2$ and the RHS is $(xy)(xy)^* = |xy|^2$ but the previous problem told us that $|x||y| = |xy|$ so the LHS equals the RHS and we have proved Lagrange's identity.

□

Subrings of $\mathbb{Q}$

Problem. The rationals are our best friends. Let's then try to understand all subrings (with unity) of $\mathbb{Q}$. Denote by $\mathbb{P}$ the set of all the primes in $\mathbb{N}$. Given a subset $P \subset \mathbb{P}$, set

$$\mathbb{Q}_P := \{m/n \mid \text{ prime factors of } n \text{ are in } P\}$$

with m/n being a reduce fraction: $(m, n) = 1$.

(i) Show that $\mathbb{Q}_P$ is a subring with unity of $\mathbb{Q}$. **(ii)** Reserve the letter R for subrings with unity, $R \subset \mathbb{Q}$. Define the denominator primes associated to such rings by

$$P_R := \{p \in \mathbb{P} \mid 1/p \in R\}$$

Show that if $P = P_R$ then $R = \mathbb{Q}_P$.

Proof. **(i)** We wish to show that $\mathbb{Q}_P$ is a subring with unity of $\mathbb{Q}$. First we show that it is a subring. Consider $m/n, m'/n' \in \mathbb{Q}_P$ and the sum/difference:

$$\frac{m}{n} \pm \frac{m'}{n'} = \frac{mn'}{nn'} \pm \frac{m'n}{nn'} = \frac{mn' \pm m'n}{nn'}$$

Certainly the far RHS is a number in $\mathbb{Q}$. If we reduce it so the numerator and denominator are coprime, then we have a candidate for a member of $\mathbb{Q}_P$. Every factor of n, n' is a member P so every factor of their product is also a member of P. Also reducing nn' does not add any factors so every factor of the reduction of nn' is a member of P, therefore the sum on the far RHS is a member of $\mathbb{Q}_P$.

Now we show the product:

$$\frac{m}{n} * \frac{m'}{n'} = \frac{mm'}{nn'}$$

The product is a member of $\mathbb{Q}_P$ by the same reasoning as before with nn'. So $\mathbb{Q}_P$ is a subring, is it a subring with unity? This is equivalent to asking if $1/1 = 1 \in \mathbb{Q}_P$. It really seems like 1 should be prime but then that would mess up some unique factorization theorems so I am thinking maybe 1 is not a prime. I am going to roll with the following line of reasoning: I think 1 has no prime factors the requirement that the prime factors of 1 be in the set P is vacuously true and $1 \in \mathbb{Q}_P$!

(ii) Show that if $P = P_R$ then $R = \mathbb{Q}_P$. We wish to show that R and $\mathbb{Q}_P$ are subsets of each other. Going to the left, pick $m/n \in R$ a subring with unity of $\mathbb{Q}$. Consider the prime factorization of $n : p_1^{j_1} * p_2^{j_2} * \cdots * p_k^{j_k}$. Then each $p_*^{j_*} \in P_R$ but since $P_R = P$ each $p_*^{j_*}$ is also a member of P. But then by very definition of $\mathbb{Q}_P$, we must have $m/n \in \mathbb{Q}_P$.

Now going to the right, pick any $m/n \in \mathbb{Q}_P$. Then every prime factor of n is in the set P, by $P_R = P$ it is also true that every prime factor of n is in the set P_R. Let a be a prime factor of n, then $1/a \in R$ Thus $1/n$ is product of members of R and since R is a ring $1/n \in R$. Then we can add $1/n$ to itself m times and we still have a member of R. This member is $m/n \in R$. Thus we have shown the inclusion in both directions and $R = \mathbb{Q}_R$.

$\square$