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 $r r^{l-1} = r^{1+l-1} = r^l = 1$. 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)

(c)

$\square$

Page 135 — Problem 23

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

$$\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 \mapsto \alpha_0 - \alpha_1 - \alpha_2 - \alpha_3$$

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.

$\square$

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.

$\square$

Page 135 — Problem 25

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

Proof.

□

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 $\mathbb{Q}$. Reserve the letter R for subrings with unity, $R \subset \mathbb{Q}$. Define the denominator primes associated to such rings by

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

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

Proof.

□