HOMEWORK 4

JASON MEDCOFF

3. i) If $a+c=b+c$, take c' such that $c'+c=0$. Then

$$\begin{aligned} a+c &= b+c \\ (a+c)+c' &= (b+c)+c' \\ a+(c+c') &= b+(c+c') \\ a+(c'+c) &= b+(c'+c) \\ a+0 &= b+0 \\ a &= b. \end{aligned}$$

ii) If $a+b=0$ and $a+c=0$, then

$$b = b+0 = b+(a+c) = (b+a)+c = 0+c = c.$$

iii) Finally, if u is a unit in R, such that $ub=1$ and $uc=1$, then we have

$$b = 1b = (uc)b = (ub)c = 1c = c.$$

6. We know $\mathbb{I}_{11} = \{0, 1, \ldots, 9, 10\}$ and since 11 is prime, every nonzero element has a multiplicative inverse. Given a, we are looking for x such that $ax \equiv 1 \mod 11$, and the extended euclidean algorithm gives x and y such that $ax+by=1$. If we let $b=11$, then $by \equiv 0 \mod 11$, and so $ax \equiv 1 \mod 11$. Then x is the multiplicative inverse of a.

TABLE 1. Multiplicative inverses mod 11

a	1	2	3	4	5	6	7	8	9	10
a^{-1}	1	6	4	3	9	2	8	7	5	10

7. i) We know that the boolean group is abelian from page 130. So the boolean ring under its addition satisfies the first four axioms of commutative rings automatically. The rest of the axioms follow:

$$\begin{aligned} UV = U \cap V = V \cap U = VU \\ U(VW) = U \cap (V \cap W) = (U \cap V) \cap W = (UV)W \\ UX = U \cap X = U, \quad \text{since } U \subseteq X \\ U(V+W) = U \cap ((V-W) \cup (W-V)) &= (U \cap (V-W)) \cup (U \cap (W-V)) \\ &= [(U-V) \cap (U-W)] \cup [(U-W) \cap (U-V)] \\ &= (U \cap V) + (U \cap W) \\ &= UV + UW \end{aligned}$$

ii) In the boolean ring, we showed above that "1" is the set X itself. Thus X is automatically a unit. Now we want to show there are no other units. Suppose we have some U, $V \in \mathcal{B}(X)$

such that $UV = 1$, that is, $U \cap V = X$. Then U and V must be supersets of X, but they are subsets of X since they belong to $\mathcal{B}(X)$. Thus U and V are X itself, so X is the sole unit.

iii) We know from above that for any $\mathcal{B}(X)$, the multiplicative identity is X. Thus, for distinct X and Y, $\mathcal{B}(X)$ and $\mathcal{B}(Y)$ have different multiplicative identities and thus $\mathcal{B}(Y)$ is not a subring of $\mathcal{B}(X)$.

8. i) If $a^2 = a$, then $a^2 - a = 0$. We can factor $a(a-1) = 0$, and it must be that either $a = 0$ or $a - 1 = 0$. Thus, $a = 0$ or $a = 1$.

ii) Take f to be the unit step function, giving zero for negative input and one for nonnegative input. Then f is clearly not 0 or 1, but for all $x < 0$, $f(x)f(x) = 0(0) = 0 = f(x)$, and for all $x \geq 0$, $f(x)f(x) = 1(1) = 1 = f(x)$.

15. It is clear that R is a subset of $\mathbb{R}$, so we will begin by showing that R is a subring of $\mathbb{R}$. First, we note that R is nonempty; namely, it contains $0 = 0 + 0\sqrt{2}$. In addition, it is closed under subtraction:

$$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in R.$$

Finally, it is closed under multiplication:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + (bc + ad)\sqrt{2} + 2bd = (2bd + ac) + (bc + ad)\sqrt{2} \in R.$$

Thus R is a subring of $\mathbb{R}$. It can also be shown that since $\mathbb{R}$ is a domain, R is a domain. Consider some domain X and a subring Y of X. Suppose that Y is not a domain, meaning there exists a, $b \in Y$ such that neither equals zero, and $ab = 0$. But a and b are necessarily in X, and X is a domain, so $ab \neq 0$, a contradiction. Therefore a subring of a domain is also a domain, and therefore R is a domain.

19. i) Matrix addition is abelian in the general case, so it holds here as well.

ii) Matrix addition is commutative in general, and so holds here again.

iii) The zero matrix satisfies the additive identity; let a and b be 0.

Then $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} = \begin{bmatrix} 0+a & 0+b \\ 0+b & 0+a+b \end{bmatrix} = \begin{bmatrix} a & b \\ b & a+b \end{bmatrix}$.

iv) Take $A = \begin{bmatrix} a & b \\ b & a+b \end{bmatrix}$, $a,\ b \neq 0$; then the additive inverse $-A$ is $\begin{bmatrix} -a & -b \\ -b & -a-b \end{bmatrix}$ and is in $\mathbb{F}_4$ since $-a$ and $-b$ are in $\mathbb{F}_2$ as 2 is prime.

v) Matrix multiplication is associative in general, and associativity is inherited here.

vi) The identity matrix $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is in $\mathbb{F}_4$, since 1 and 0 are in $\mathbb{F}_2$.

Then $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} = \begin{bmatrix} 1a+0b & 1b+0(a+b) \\ 0a+1b & 0b+1(a+b) \end{bmatrix} = \begin{bmatrix} a & b \\ b & a+b \end{bmatrix}$.

vii) Matrix multiplication is not commutative in general, so we look more closely here. Take $A = \begin{bmatrix} a & b \\ b & a+b \end{bmatrix}$ and $B = \begin{bmatrix} c & d \\ d & c+d \end{bmatrix}$. Then $AB = \begin{bmatrix} ac+bd & ad+bc+bd \\ bc+da+db & 2bd+ac+bc+ad \end{bmatrix} = \begin{bmatrix} ca+db & cb+da+db \\ da+cb+db & 2db+ca+da+cb \end{bmatrix} = BA$.

viii) Matrix multiplication is distributive over matrix addition in general and is inherited here.

To show this is a field with four elements, observe that there are two choices 0 or 1 for each of two variables a and b; thus there are four possible assignments of 0 and 1 to a and b. To show inverses for nonzero elements, we know already that a matrix is invertible if its determinant is

nonzero. Taking

$$\begin{vmatrix} a & b \\ b & a+b \end{vmatrix} = a(a+b) - b^2 = a^2 + ab - b^2$$

we can see that the determinant is nonzero as long as one of a or b is nonzero. Thus, each element except for the zero matrix is invertible.

20. Take some $a \in R$ such that $a \neq 0$. Then define a map $f : R \to R$ that sends $x \mapsto ax$. Consider the kernel of f,

$$\ker f = \{x \in R : f(x) = 0\} = \{x \in R : ax = 0\}$$

Then since R is a domain and $a \neq 0$, it must be that $x = 0$. Then the kernel is $\{0\}$ and f is injective. Then the image of f has at least $|R|$ elements, but the image of f is contained in R, so it must have exactly $|R|$ elements. Therefore f is surjective.

Since f is surjective and $1 \in R$, there must exist an x such that $f(x) = 1$, or $ax = 1$. Then x is the multiplicative inverse of a. Since a was arbitrary but nonzero, every nonzero element of R has a multiplicative inverse, and R is thus a field.

22. We already know from an above problem that since F is a subset of $\mathbb{R}$, if F is a subring, it is a domain. Then we need only show that every element has a multiplicative inverse. First, F is indeed a subring since

$$0 = 0 + 0\sqrt{2} \in F,$$
$$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in F,$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + (bc + ad)\sqrt{2} + 2bd = (2bd + ac) + (bc + ad)\sqrt{2} \in F.$$

Then F is also a domain. From prior experience, it is expected that the inverse of $a + b\sqrt{2}$ will be $\frac{1}{a+b\sqrt{2}}$. So we have

$$\frac{1}{a + b\sqrt{2}}\left(\frac{a - b\sqrt{2}}{a - b\sqrt{2}}\right) = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \left(\frac{a}{a^2 - 2b^2}\right) - \left(\frac{b}{a^2 - 2b^2}\right)\sqrt{2} \in F$$

since $\frac{a}{a^2-2b^2}$ and $\frac{b}{a^2-2b^2}$ are in $\mathbb{Q}$. Therefore, F is a field.

23. i) As above,

$$0 = 0 + 0i \in F,$$
$$(a + bi) - (c + di) = (a - c) + (b - d)i \in F,$$
$$(a + bi)(c + di) = ac + (bc + ad)i - bd = (ac - bd) + (bc + ad)i \in F.$$

Now, we want to find inverses:

$$\frac{1}{a + bi} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i \in F.$$

ii) Take $u \in F$. Write $u = a + bi$. Then we want to show that $u = \alpha\beta^{-1}$ for some α, $\beta \in F$. Write $\alpha = c + di$ and $\beta^{-1} = e + fi$.

$$a + bi = (c + di)(e + fi) = (ce - df) + (de + cf)i$$

So $a = (ce - df)$ and $b = (de + cf)$. Part i) already shows how to go from β to β^{-1} and vice versa.

24. i) Reflexive: $a \equiv b \implies b = ua \implies a = u^{-1}b \implies b \equiv a$ since the inverse of a unit is a unit.

Transitive: $a \equiv b,\ b \equiv c \implies b = ua,\ c = vb \implies c = uva \implies a \equiv c$ since the product of two units is a unit.

Symmetric: $a \equiv a \implies a = ua \implies u = 1$, trivially true as the multiplicative identity 1 is always a unit.

So $\equiv$ is an equivalence relation.

ii) $a \equiv b \implies b = ua$ for some unit u. Thus b is a multiple of a. It follows that any multiple of b is also a multiple of a. But since $a = u^{-1}b$, a is a multiple of b, as are all multiples of a. Therefore, the sets of multiples of a and b are the same, or $(a) = (b)$.

Conversely, say that $(a) = (b)$ in some domain R. Then we know that $ka = b$ and $\ell b = a$. Then it must be that $k\ell b = b$, so k and ℓ must be multiplicative inverses. Therefore, k and ℓ are units. Then we know that $b = ua$ for some unit u, and thus $a \equiv b$.