Math 113 Homework # 8 solutions

Fraleigh 19.14. If A and B are matrices such that the image of B is contained in the kernel of A, then $AB = 0$. This observation allows us to find that $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Fraleigh 19.17. (a) False, $n\mathbb{Z}$ is a subring of $\mathbb{Z}$ which has no zero divisors.

(b) True, proved in class and the book.

(c) False, $n\mathbb{Z}$ has characteristic zero since it is a subring of $\mathbb{Z}$.

(d) False, $n\mathbb{Z}$ has no multiplicative identity for $n > 1$.

(e) True, because if a ring is isomorphic to an integral domain then it is an integral domain.

(f) True. If it were finite then $m \cdot 1 = n \cdot 1$ for some $m \neq n$, so $(m - n) \cdot 1 = 0$, so the characteristic divides $m - n$.

(g) False: $(1, 0) \cdot (0, 1) = (0, 0)$.

(h) True. Suppose a is a zero divisor and has a multiplicative inverse. Then $a \neq 0$, there exists $b \neq 0$ with $ab = 0$, and there exists c with $ac = 1$. Then $0 = 0c = (ab)c = (ac)b = 1b = b$, contradiction.

(i) False, $n\mathbb{Z}$ is not a domain when $n > 1$ because it has no multiplicative identity.

(j) False, $\mathbb{Z}$ is not a field.

Fraleigh 21.2. $F = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. By a previous problem, F is a field, and F contains D. On the other hand every element of F is a quotient of two elements of D, because $p/q + (r/s)\sqrt{2} = (ps + qr\sqrt{2})/(qs)$.

Fraleigh 21.4. (a) True; this is essentially the definition of $\mathbb{Q}$.

(b) False. If $\mathbb{R}$ were a field of quotients of $\mathbb{Z}$, then there would be an injective ring homomorphism $f : \mathbb{Z} \to \mathbb{R}$, such that every element of $\mathbb{R}$ is the quotient of two elements of the image of f. As explained in class, an injective ring homomorphism $f : \mathbb{Z} \to \mathbb{R}$ must be the usual inclusion map. But not every element of $\mathbb{R}$ is a quotient of two elements of $\mathbb{Z}$; for example $\sqrt{2}$.

(c) True; any field is its own field of quotients.

(d) False. In general, if E is a field, and if F is a quotient field of E, that is if there is an injective ring homomorphism $f : E \to F$ such that every element of F is a quotient of elements of the image of f, then f must be an isomorphism, because any quotient of elements of E is in E. But $\mathbb{R}$ is not isomorphic to $\mathbb{C}$ because an isomorphism would have to send -1 to -1, and -1 has a square root in $\mathbb{C}$ but not in $\mathbb{R}$.

(e) True, see (c).

(f) True. For example we needed this to get an equivalence relation. And any construction of a field of quotients must use this fact; because if D has zero divisors then it is impossible to define an injective ring homomorphism from D to a field, since fields do not have zero divisors.

(g) False: 0 is not a unit in F.

(h) True, since every nonzero element of a field is a unit.

(i) True. If F is a field of quotients for D, then F' can be realized as the set of those elements in F that can be expressed as quotients of elements of D'.

(j) True, by the uniqueness of a field of quotients, since $\mathbb{Q}$ is a field of quotients for $\mathbb{Z}$.

Fraleigh 21.6. We compute that

$$\begin{aligned}([(a_1,b_1)]+[(a_2,b_2)])+[(a_3,b_3)] &= [(a_1b_2+b_1a_2,b_1b_2)]+[(a_3,b_3)]\\ &= [((a_1b_2+b_1a_2)b_3+b_1b_2a_3,b_1b_2b_3)]\\ &= [(a_1b_2b_3+b_1a_2b_3+b_1b_2a_3,b_1b_2b_3].\end{aligned}$$

Computing $[(a_1,b_1)]+([a_2,b_2]+[a_3,b_3])$ similarly, we obtain the same answer (so we do not have to check the equivalence relation in this step).

Fraleigh 22.17. By Fermat's theorem, $x^5 = x$ for all $x \in \mathbb{Z}_5$. This means that we can subtract multiples of 4 from the exponents of our polynomial, and as long as the exponents remain positive, then the polynomial has the same zeroes. Thus $2x^{219}+3x^{74}+2x^{57}+3x^{44}$ has the same zeroes as $2x^3+3x^2+2x+3x^4$. By simply trying all five possibilities, we find that the zeroes of the latter polynomial are $x = 0, 1, 2, 3$. (Alternatively you can use $x^4 = 1$ when $x \neq 0$ to say that the given polynomial is zero if and only if $2x^3 + 3x^2 + 2x + 3$ is, provided that $x \neq 0$, but then you have to check the case $x = 0$ separately.)

Fraleigh 22.22. In $\mathbb{Z}_4[x]$, we have $(1 + 2x)(1 - 2x) = 1$, so $1 + 2x$ is a unit.

Fraleigh 22.23. (a) True by definition.

(b) True: if R is commutative and $f = \sum_i a_i x^i$ and $g = \sum_j b_j x^j$ are elements of $R[x]$ then we have

$$fg = \sum_{i,j} a_i b_j x^{i+j} = \sum_{i,j} b_j a_i x^{j+i} = gf.$$

(c) True; we proved this in class.

(d) True. Any divisor of zero in R can be regarded as a constant polynomial in $R[x]$, which is then a divisor of zero in $R[x]$.

(e) False. If f and g are nonzero elements of $R[x]$, then the highest exponent in the sum defining fg is the sum of the degrees of f and g. When R is not an integral domain, it is possible that $\deg(fg) < \deg(f)+\deg(g)$, see (f). But we always have $\deg(fg) \leq \deg(f)+\deg(g)$; and equality must hold when R is an integral domain.

(f) False. For example let $R = \mathbb{Z}_6$ and $f = 1 + 2x^3$, $g = 1 + 3x^4$. Then since $2 \cdot 3 = 0$ we have $fg = 1 + 2x^3 + 3x^4$ which has degree only 4.

(g) True since $h(\alpha) = f(\alpha)g(\alpha) = 0 \cdot g(\alpha) = 0$.

(h) True. A unit must have degree zero since degree of polynomials is additive under multiplication, and any unit of F, regarded as a constant polynomial, is also a unit in $F[x]$, with the same multiplicative inverse.

(i) True. Multiplying a polynomial by x simply increases each exponent by one, so if f is nonzero, i.e. f has some nonzero coefficient, then xf also has a nonzero coefficient so $xf \neq 0$.

(j) False. For example in $\mathbb{Z}_6[x]$ we have $(2x)(3x) = 0$ so $2x$ is a zero divisor in $\mathbb{Z}_6[x]$ which is not a zero divisor in $\mathbb{Z}_6$.

Fraleigh 22.26. Let $f = \sum_i a_i x^i$, $g = \sum_j b_j x^j$, and $h = \sum_k c_k x^k$. We then manipulate sums as follows:

$$\begin{aligned} f(g+h) &= \sum_i a_i x^i \left(\sum_j b_j x^j + \sum_k c_k x^k \right) \\ &= \sum_i a_i x^i \sum_j (b_j + c_j) x^j \\ &= \sum_{i,j} a_i (b_j + c_j) x^{i+j} \\ &= \sum_{i,j} (a_i b_j + a_i c_j) x^{i+j} \\ &= \sum_{i,j} a_i b_j x^{i+j} + \sum_{i,j} a_i c_j x^{i+j} \\ &= fg + fh. \end{aligned}$$

Here we have used the distributive law in R to get from the third line to the fourth, while to get between the other lines we use the definitions of addition and multiplication in $R[x]$.

Fraleigh 22.27. (a) If $f = \sum_i a_i x^i$ and $g = \sum_j b_j x^j$ then

$$\begin{aligned} D(f+g) = D \sum_i (a_i + b_i) x^i &= \sum_i i(a_i + b_i) x^{i-1} \\ &= \sum_i i a_i x^{i-1} + \sum_i i b_i x^{i-1} = Df + Dg \end{aligned}$$

so D is a homomorphism of additive groups. However D is *not* a ring homomorphism. We have $D(fg) = (Df)g + f(Df)$, which is usually not the same thing as $(Df)(Dg)$. For example take $f = g = x^2$; then $D(fg) = 4x^3$ while $(Df)(Dg) = 4x^2$.

(b) The kernel of D consists of the constant polynomials.

(c) The map $D : F[x] \to F[x]$ is surjective. We can define a formal integral $I : F[x] \to F[x]$ by

$$I\left(\sum_i a_i x^i \right) = \sum_i \frac{a_i}{i+1} x^{i+1}.$$

Here we use the fact that F has characteristic zero so that $1/(i+1) \in F$. Then I is a right inverse of D, that is $D \circ I = \mathrm{id} : F[x] \to F[x]$, which implies that D is surjective.