HOMEWORK 6

JASON MEDCOFF

44. i) The inverse of a bijection is a bijection, so we need only show ψ is an homomorphism. Since $\varphi(a)\varphi(b) = \varphi(ab)$ and $\varphi(a^{-1}) = \varphi(a)^{-1}$,

$$\psi(\varphi(a)\varphi(b)) = \psi(\varphi(ab)) = ab = \psi(\varphi(a))\psi(\varphi(b)).$$

ii) The compositions of bijections is a bijection. Let $f : R \to S$ and $g : S \to T$, with $a, b \in R$. Then

$$(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)(g \circ f)(b).$$

iii) Say A, R, B belong to some set of commutative rings S. Then

- $A \cong R \implies R \cong A$ by (i) above,
- $A \cong A$ by the identity map $f : A \to A$, $a \mapsto a$ being an isomorphism,
- $A \cong R$, $R \cong B \implies A \cong B$ by (ii) above.

So isomorphism gives an equivalence relation on S.

46. $\eta(1) = 1$; that is, the constant polynomial 1 is taken to 1 in the ring R. In addition, for $f = \sum_i a_i x^i$, $g = \sum_j b_j x^j \in R[x]$,

$$\eta(f + g) = \eta(\sum_k (a_k + b_k)x^k) = a_0 + b_0 = \eta(f) + \eta(g)$$

and

$$\eta(fg) = \eta(\sum_i \Big(\sum_{j=0}^{i} a_j b_{i-j}\Big)x^i) = a_0 b_0 = \eta(f)\eta(g).$$

The kernel

$$\ker \eta = \{f \in R[x] : \eta(f) = 0\} = \{f \in R[x] : a_0 = 0\}$$

is the ideal of polynomials over R with a zero constant term. Thus the kernel can be described as those polynomials which have 0 as a root.

47. We can write

$$\psi^{-1}(J) = \{r \in R : \psi(r) = j \in J\}.$$

We know this contains zero since $\{0\} \subseteq J$ and

$$\psi^{-1}(\{0\}) = \ker \psi \subseteq \psi^{-1}(J).$$

Then let $a, b \in \psi^{-1}(J)$ with $a = \psi(x)$ and $b = \psi(y)$. Then

$$a - b = \psi(x) + \psi(y) = \psi(x - y)$$

and $x - y \in J$ so $\psi(x - y) \in \psi^{-1}(J)$. Similarly, for $r \in R$,

$$\psi(ra) = \psi(r)\psi(a)$$

and since $\psi(a) \in J$ and $J \in S$, $\psi(r)\psi(a) \in J$. So $\psi^{-1}(J)$ is an ideal in R.

49. Let $f : R \to \mathrm{Frac}(R)$, with $r \mapsto \frac{r}{1}$. This map is a homomorphism since for $r = 1$ we have $\frac{1}{1}$, and

$$f(r+s) = \frac{r+s}{1} = \frac{r}{1} + \frac{s}{1} = f(r) + f(s)$$

and furthermore

$$f(rs) = \frac{rs}{1} = \left(\frac{r}{1}\right)\left(\frac{s}{1}\right) = f(r)f(s).$$

We can demonstrate that f is bijective by observing $g : \mathrm{Frac}(R) \to R$, $\frac{a}{b} \mapsto ab^{-1}$. Then

$$(g \circ f)(r+s) = g(f(r+s)) = g(\frac{r}{1} + \frac{s}{1}) = g(\frac{r}{1}) + g(\frac{s}{1}) = r + s$$

and

$$(g \circ f)(rs) = g(f(rs)) = g(\frac{r}{1}\frac{s}{1}) = g(\frac{r}{1})g(\frac{s}{1}) = rs.$$

So g is the inverse of f and f is an isomorphism.

55.

- Closure under addition:
$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix} \in F$$
- Closure under multiplication:
$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} \in F$$
- Associativity of matrix addition: inherited.
- Commutativity of matrix addition: inherited.
- Additive identity: zero matrix.
$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} 0+a & 0+b \\ 0-b & 0+a \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$
- Additive inverse:
$$\begin{bmatrix} -a & -b \\ b & -a \end{bmatrix} + \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$
- Associativity of matrix multiplication: inherited.
- Commutativity of matrix multiplication:
$$\begin{bmatrix} c & d \\ -d & c \end{bmatrix} \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} ca-db & cb+da \\ -da-cb & -db+ca \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$
- Multiplicative identity: 2×2 identity matrix.
$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in F$$
since $0 = -0$.
- Distributive law: inherited.
- Nonzero elements have inverses: Consider $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$. We know A^{-1} exists since $\det A = a^2 + b^2 \neq 0$ as long as $a \neq 0$ and $b \neq 0$. Then
$$A^{-1} = \frac{1}{a^2+b^2} \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} \frac{a}{a^2+b^2} & -\frac{b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{bmatrix} \in F$$
since each entry in A^{-1} is in $\mathbb{R}$.

To show F is isomorphic to $\mathbb{C}$, we construct the obvious map $f : F \to \mathbb{C}$, $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mapsto a + bi$. We can see that the identity matrix maps to $1 + 0i = 1$, and furthermore

$$f(\begin{bmatrix} a & b \\ -b & a \end{bmatrix})+f(\begin{bmatrix} c & d \\ -d & c \end{bmatrix}) = a+bi+c+di = (a+c)+(b+d)i = f(\begin{bmatrix} a+c & b+d \\ -b-d & a+c \end{bmatrix}) = f(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}+\begin{bmatrix} c & d \\ -d & c \end{bmatrix})$$

and

$$f(\begin{bmatrix} c & d \\ -d & c \end{bmatrix})f(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}) = (c+di)(a+bi) = ca-db+(da+cb)i = f(\begin{bmatrix} ca-db & cb+da \\ -da-cb & -db+ca \end{bmatrix}) = f(\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\begin{bmatrix} a & b \\ -b & a \end{bmatrix})$$

so f is a homomorphism. To show f is injective, choose $a+bi = c+di$. Then $a+bi = f(\begin{bmatrix} a & b \\ -b & a \end{bmatrix})$ and $c + di = f(\begin{bmatrix} c & d \\ -d & c \end{bmatrix})$ but since $a = c$ and $b = d$, the matrices are equal. To show f is surjective, take $z = a + bi$. Then there does exist $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ such that $f(A) = z$. Thus f is bijective and a homomorphism, so F and $\mathbb{C}$ are isomorphic.

58. Note that in $\mathbb{F}_5$, $x^2 - x - 2 = x^2 + 4x + 3$ and $x^3 - 7x + 6 = x^3 + 3x + 1$. Then using the extended euclidean algorithm,

$$\begin{aligned} x^2 + 4x + 3 &= (x^3 + 3x + 1)(0) + (x^2 + 4x + 3) \\ x^3 + 3x + 1 &= (x^2 + 4x + 3)(x + 1) + (x + 3) \\ x^2 + 4x + 3 &= (x + 3)(x + 1) + (0) \end{aligned}$$

so the gcd is $(x + 3)$. We can express this as

$$(x + 3) = (4x + 4)(x^2 + 4x + 3) + (1)(x^3 + 3x + 1).$$

59. By the division algorithm, we can write

$$f(x) = (x - a_1)q(x) + r(x)$$

but since a_1 is a root of f, $f(a_1) = 0$ so

$$f(a_1) = 0 = (0)q(a) + r(a)$$

and thus $r(a) = 0$. Furthermore, $\deg r = 0$ because if $\deg f = n$, $\deg(x-a_1)q(x) = n$. Thus $r(x)$ is the constant function 0. Suppose the statement is true for $a_1, \dots, a_{n-1}$ and we already have

$$f(x) = (x - a_1) \cdots (x - a_{n-1})q(x).$$

When we divide by $(x - a_n)$ we obtain

$$f(x) = (x - a_1) \cdots (x - a_n)q'(x) + r'(x)$$

and furthermore, a_n is a root so

$$f(a_n) = 0 = (a_n - a_1) \cdots (0)q'(a_n) + r'(a_n)$$

so once again $r'(a_n)$ is the zero constant function. The induction holds and the statement is true with g being q'.

60. If $n = 0$, f is a nonzero constant polynomial with no roots. Suppose the statement is true for all g with $\deg g < n$ and $\deg f = n$. If f has no roots in R, we are done; suppose f has a root $a \in R$. Then we know by problem **61** that we can write

$$f(x) = (x - a)g(x)$$

for some $g \in R[x]$. Then suppose $c \in R$ is an additional root of f not equal to a. Then since $f(c) = 0$ and $(a - c) \neq 0$, $g(c)$ must be zero since R is a domain. Therefore, the roots of f in R are a and the roots of g. Since $\deg g = n - 1$, g has at most $n - 1$ roots by the induction hypothesis. Thus, f has at most n roots in R.

61. By the division algorithm,

$$f(x) = (x - a)g(x) + r(x)$$

with g, $r \in R[x]$. Then since $f(a) = 0$,

$$f(a) = 0 = (a - a)g(a) + r(a) = r(a).$$

By the division algorithm, $\deg r < \deg(x - a)$, meaning $\deg r = 0$. Thus r is the constant zero polynomial and we write

$$f(x) = (x - a)g(x).$$

64. Since $k[x]$ is a euclidean domain, we can obtain prime factorizations of f and g. Each prime factor of f and g divides h, and f and g share no factors, since they are coprime. Therefore, the product of all these disjoint factors divides h, so fg divides h.

66. Suppose instead that $\sqrt{1 - x^2}$ is a rational function. Then we can write

$$\sqrt{1 - x^2} = \frac{p(x)}{q(x)}$$

assuming without loss of generality that p and q have no common factors. Then

$$1 - x^2 = \frac{p(x)^2}{q(x)^2}$$

which implies

$$p(x)^2 = (1 - x^2)q(x)^2$$

so $1 - x^2$ is a factor of p^2. Then it must be a factor of p, so p^2 is divisible by $(1 - x^2)^2$. Then

$$p(x)^2 = (1 - x^2)^2 p'(x) = (1 - x^2)q(x)^2$$

so

$$(1 - x^2)p'(x) = q(x)^2$$

thus $(1-x^2)$ is a factor of q^2 and therefore q. Then p and q have a common factor, a contradiction. Therefore it must be that $\sqrt{1 - x^2}$ is not a rational function.