# HOMEWORK 7

JASON MEDCOFF

**93.** We can use the isomorphism theorem by showing that there is a homomorphism $f : R[x]/ \to R$, demonstrating the kernel of $f$ to be $(x)$, and showing that the image of $f$ is $R$ itself. So first, choose $f$ such that $r(x) = r_0 + \ldots + r_n x^n \mapsto r_0$; in other words, $f$ is the evaluation function that sends polynomials $r(x)$ to $r(0)$.

This map is well defined since equality of polynomials is defined by equality of coefficients. The map is a homomorphism since

$$f(r(x) + s(x)) = r_0 + s_0 = f(r(x)) + f(s(x))$$

and

$$f(r(x)s(x)) = r_0 s_0 = f(r_0)f(s_0),$$

and furthermore, the zero polynomial obviously maps to zero in $R$. Thus $f$ is a homomorphism.

The kernel of $f$ is given by

$$\begin{aligned} \ker f &= \{r(x) \in R[x] : f(r(x)) = 0\} \\ &= \{r_1 x + \ldots + r_n x^n\} \\ &= (x) \end{aligned}$$

since polynomials without constant terms are divisible by $x$ without remainder. Finally, the image of $f$ is clearly the entirety of $R$ since one can choose any constant polynomial $r(x) = r_0$ with $r_0 \in R$. Thus by the first isomorphism theorem, there exists an isomorphism between $R[x]/(x)$ and $R$.

**97.**

**Lemma.** In a finite field of prime order $n$, $(a + b)^n = a^n + b^n$. By binomial coefficients,

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

where

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

but for $n > k$, $n$ divides $n!$ but not $k!$. Then the coefficients of all terms but the first and the last are divisible by the characteristic. All that is left is $a^n + b^n$.

i) $F$ obeys the additive homomorphism rule since

$$F(a + b) = a^p + b^p = (a + b)^p = F(a) + F(b)$$

since by binomial coefficients,

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$$

where

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

but since

**100.** i) By the lemma in 97, we can write $x^4 + 1 = x^4 + 1^4 = (x + 1)^4$.

ii) We can write

$$\begin{aligned}(x^2 + ax + b)(x^2 + cx + d) &= x^4 + cx^3 + dx^2 + ax^3 + acx^2 + adx + bx^2 + bcx + bd \\ &= x^4 + (c + a)x^3 + (d + ac + b)x^2 + (ad + bc)x + (bd) \\ &= x^4 + 1\end{aligned}$$

and by equating coefficients, clearly $bd = 1$, $c+a = 0$ or $c = -a$, $d+ac+b = 0$, and $ad+bc = 0$. The latter two can be written as $d + b - a^2 = 0$ and $ad - ab = 0$ or $a(d - b) = 0$.

iii) Suppose $b^2 \equiv -1 \mod p$.

**2.** Since $\mathcal{F}(k)$ is already a commutative ring, we know that it is an abelian group under addition. According to the given definition of scalar multiplication, we have

$$\alpha(f(a) + g(a)) = \alpha f(a) + \alpha g(a)$$
$$(\alpha + \beta)f(a) = \alpha f(a) + \beta f(a)$$
$$(\alpha\beta)f(a) = \alpha(\beta f(a))$$
$$1f(a) = f(a)$$

thus we have a vector space.

If we take the subset of polynomial functions, we can show this is a subspace by

$$0f(a) = 0 \in \mathcal{PF}(k),$$
$$f(a) + g(a) = (f_0 + g_0) + (f_1 + g_1)x + (f_2 + g_2)x^2 + \cdots \in \mathcal{PF}(k),$$
$$\alpha f(a) = (\alpha f_0) + (\alpha f_1)x + (\alpha f_2)x^2 + \cdots \in \mathcal{PF}(k).$$

**7.** Suppose $Ax = 0$ with $x \neq 0$. Then it must be that for every column $i$ of $A$, $\sum a_i x_i = 0$ with at least one $x_i$ nonzero. This is a linear combination, and we know that a linear combination has a nontrivial solution if and only if the vectors are linearly dependent. Thus, the null space has a nontrivial solution if and only if the matrix column vectors are linearly dependent.

**8.** If the given list is linearly dependent, then we can write

$$0 = a_0 + a_1 x + a_2 x^2 + \ldots + a_{100} x^{100} = f(x)$$

with at least one $a_i$ nonzero. This would mean that this degree 100 polynomial $f(x)$ evaluates to zero for all $x \in k$. However, a degree 100 polynomial has at most 100 roots by the fundamental theorem of algebra. Thus, it must be that $f(x)$ is in fact the zero polynomial with $a_i = 0$. Thus, the list is linearly independent.

With a similar argument, $V_n$ must be linearly independent, simply by replacing 100 above with $n$. Then $1, x, \ldots, x^n$ is a basis of $V_n$ because it clearly spans $V_n$ and is linearly independent. Furthermore, the basis contains all $x^i$ for $0 \leq i \leq n$, so it is obvious that there are $n+1$ elements in the basis and so $\dim V_n = n + 1$.

**11.** Let $E_{ij}$ designate the $m \times n$ matrix with 1 at position $ij$ and zero elsewhere. Clearly, for an $m \times n$ matrix, there are $mn$ such $E$. These matrices are also linearly independent, for if we rearrange the entries as a vector of length $mn$, we have the standard basis of $k^{mn}$, which is a linearly independent set. Thus, the set of all $E_{ij}$ is a basis for the $m \times n$ matrices of size $mn$. So, the dimension of that vector space is $mn$.

If we consider the subspace of symmetric matrices, we can similarly think about rearranging the basis matrices as vectors. For a symmetric matrix, everything below the diagonal is already given by what is above the diagonal, so we need only consider the diagonal of length $n$, the $n-1$ superdiagonal elements, etc. giving $\frac{n(n+1)}{2}$ elements total. Then we need vectors of this length to uniquely define the elements of the basis, and so the dimension of this subspace of symmetric $n \times n$ matrices is $\frac{n(n+1)}{2}$.

**15.** We know that the space of $n \times n$ matrices has dimension $n^2$. Consider $m > n^2$. Then the set $I, A, A^2, \ldots, A^m$ must be linearly dependent. If that were the case, there exists a linear combination $c_0 I + c_1 A + \ldots + c_m A^m = 0$. Take $f(x) = c_0 + c_1 x + \ldots c_m x^m \neq 0$ and $f(A) = 0$ gives the result.

**18.** We know $As = b$ and $Au = 0$, so for some solution $x' = s + u$ write

$$\begin{aligned} Ax' &= b \\ A(s+u) &= b \\ As + Au &= b \\ b + 0 &= b \end{aligned}$$

Thus, all solutions $x'$ are of the form $s + u$ with $u \in U$, which is precisely the definition of a coset of $U$ with respect to $s$.