**Math 342 Problem set 10 (due 22/11/011)**

**Working with polynomials**

1. For each pair of polynomials $f,g$ below, find $q,r \in \mathbb{Q}[x]$ such that $g = qf + r$ and $\deg r < \deg f$.
   (a) $g = 2x+4$, $f = 2$.
   (b) $g = 2x+4$, $f = x+1$.
   (c) $g = 2x+4$, $f = x^2-2$
   (d) $g = x^6+5x^4+3x^3+x+1$, $f = x^2+2$.

2. Same as problem 1, but reduce all coefficients modulu 5. Thus think of $f,g$ as elements of $\mathbb{F}_5[x]$ and find $q,r$ in $\mathbb{F}_5[x]$.

3. Simplify the products $(x+1)\cdot(x+1) \in \mathbb{F}_2[x]$, $(x+1)(x+1)(x+1) \in \mathbb{F}_3[x]$. Explain why $x^2+1$ is not irreducible in $\mathbb{F}_2[x]$ (even though it is irreducible in $\mathbb{Z}[x]$!)

4. The following transmissions were made using CRC-4. Decide whether the recieved message should be accepted. Write an identity of polynomials justifying your conclusion.
   (a) $(00000000, 0000)$
   (b) $(00000100, 0000)$
   (c) $(00101100, 0000)$
   (d) $(10110111, 1011)$

5. Over the field $\mathbb{F}_5$ we would like to encode the following three-digit messages by Reed-Solomon coding, evaluating at the 4 non-zero points $\{1,2,3,4\}$ modulu 5. For each message write the associated polynomial and encoded 4-digit transmission.
   (a) $\underline{m} = (1,2,3) \mod 5$ (here $m(x) = 1+2x+3x^2 \mod 5$).
   (b) $\underline{m} = (0,0,0) \mod 5$.
   (c) $\underline{m} = (1,4,2) \mod 5$.
   (d) $\underline{m} = (2,0,2) \mod 5$.

6. Working over the field $\mathbb{F}_5$, the sender has enocded two-digit messages by evaluating the associated linear polynomial at the 4 non-zero points in the same order as above. You receive the transmissions below, which may contained corrupted bits. For each 4-tuple find the linear polynomial which passes through as many points as possible.
   (a) $\underline{v}' = (1,2,3,3)$ .
   (b) $\underline{v}' = (4,1,3,0)$ .
   (c) $\underline{v}' = (2,4,3,1)$ .

**The general linear group**

7. Let $F$ be a field. Define $\mathrm{GL}_n(F) = \{g \in M_n(F) \mid \det(g) \neq 0\}$. Using the formulas $\det(gh) = \det(g)\det(h)$, $\det(I_n) = 1$ and the fact that if $\det(g) \neq 0$ then $g$ is invertible, show that $\mathrm{GL}_n(F)$ contains the identity matrix and is closed under multiplication and under taking of inverses.

(continued on the reverse)

8. Consider the vector space $V = \mathbb{F}_p^2$ over $\mathbb{F}_p$.
   (a) How many elements are there in $V$? In a 1-dimensional subspace of $V$?
   (b) How many elements in $V$ are non-zero? If $W$ is a given 1-dimensional subspace, how many elements are there in the complement $V \setminus W$?
   (c) Let $\underline{w} \in V$ be a non-zero column vector. How many $\underline{v} \in V$ exist so that the $2 \times 2$ matrix $(\underline{w}\,\underline{v})$ is invertible?
   (d) By multiplying the number of choices for $\underline{w}$ by the number of choices for $\underline{v}$, show that $\mathrm{GL}_2(\mathbb{F}_p)$ has $(p+1)p(p-1)^2$ elements.

## Supplementary Problems

A. (The field of rational functions) Let $F$ be a field.
   (a) Let $Q$ be the set of all formal expressions $\frac{f}{g}$ with $f, g \in F[x]$, $g \neq 0$. Define a relation $\sim$ on $Q$ by $\frac{f}{g} \sim \frac{f'}{g'}$ iff $fg' = gf'$. Show that $\sim$ is an equivalence relation.
   (b) Let $F(x)$ denote the set $Q/\sim$ of equivalence classes in $Q$ under $\sim$. Show that $F(x)$ has the structure of a field.
   *Hint*: Define operations by choice of representatives and show that the result is independent of your choices up to equivalence.
   (c) Show that the map $F[x] \to F(x)$ mapping $f \in F[x]$ to the equivalence class of $\frac{f}{1}$ is an injective ring homomorphism. Obtain in particular a ring homomorphism $\iota \colon F \to F(x)$.

B. (Universal properties of $F[x]$, $F(x)$) Let $E$ be another field, and let $\varphi \colon F \to E$ be a homomorphism of rings.
   (a) Show that $\varphi$ is injective.
   *Hint*: Assume $x \neq 0$ but $\varphi(x) = 0$ and show that $\varphi(1) = 0$.
   (b) Now let $\alpha \in E$. Show that there exists a ring homomorphism $\bar{\varphi} \colon F[x] \to E$ such that (i) $\bar{\varphi} \circ \iota = \varphi$ and (ii) $\bar{\varphi}(x) = \alpha$.
   (c) Show that there is at most one $\bar{\varphi}$ satisfying (i),(ii).
   *Hint*: By induction on the degree of the polynomial.
   (d) Assume that $\alpha$ is *transcendental* over $F$, that is that it is not a zero of any polynomial in $F[x]$. Show that $\bar{\varphi}$ extends uniquely to a field homomorphism $\tilde{\varphi} \colon F(x) \to E$.

C. (Degree valuation) For non-zero $f \in F[x]$ set $v_\infty(f) = -\deg f$. Also set $v_\infty(0) = \infty$.
   (a) For $\frac{f}{g} \in Q$ set $v_\infty\left(\frac{f}{g}\right) = v_\infty(f) - v_\infty(g)$. Show that $v_\infty$ is constant on equivalence classes, thus descends to a map $v_\infty \colon F(x) \to \mathbb{Z} \cup \{\infty\}$.
   (b) For $r, s \in F(x)$ show that $v_\infty(rs) = v_\infty(r) + v_\infty(s)$ and $v_\infty(r+s) \geq \min\{v_\infty(r), v_\infty(s)\}$ with equality if the two valuations are different (cf. Problem A, Problem Set 4).
   (c) Fix $q > 1$ and set $|r|_\infty = q^{-v_\infty(r)}$ for any $r \in F(x)$ ($|0|_\infty = 0$). Show that $|rs|_\infty = |r|_\infty |s|_\infty$, $|r+s|_\infty \leq |r|_\infty + |s|_\infty$.

REMARK. When $F$ is a finite field, it is natural to take $q$ equal to the size of $F$. Then $\mathbb{F}_p(x)$ with the absolute value $|\cdot|_\infty$ behaves a lot like $\mathbb{Q}$ with the $p$-adic absolute value $|\cdot|_p$.

D. ($F[x]$ is a Principle Ideal Domain) Let $I \subset F[x]$ be an ideal. Show that there exists $f \in F[x]$ such that $I = (f)$, that is $I = \{f \cdot g \mid g \in F[x]\}$.