403 HOMEWORK 1/6/06

If $q = p^n$ is a positive power of a prime p, write $\mathbb{F}_q$ for the field with q elements. For example, $\mathbb{F}_p = \mathbb{Z}_p$ with the addition and mulitplication given in Exercise 1.

Write $\mathbb{F}_q[x]$ for the ring of polynomials with coefficients in $\mathbb{F}_q$. An element in $\mathbb{F}_q[x]$ is simply a formal expression $a_0 + a_1x + a_2x^2 + + \cdots + a_nx^n$ where the a_i's are elements of $\mathbb{F}_q$ and we add and multiply these just as we would add and multiply polynomials with coefficients in $\mathbb{R}$ or $\mathbb{C}$ or $\mathbb{Z}$.

(1) Let m be an integer. Consider $(\mathbb{Z}, +)$ as a group and form the quotient group $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. Write elements in $\mathbb{Z}_m$ as $\bar{a} = a + m\mathbb{Z} = \{a + mn \mid n \in \mathbb{Z}\}$.
   (a) Recall that the addition in $\mathbb{Z}_m$ is defined by $\bar{a} + \bar{b} := \overline{a+b}$. Taking that for inspiration, define a multiplication on $\mathbb{Z}_m$ and show that your definition is unambiguous. In other words, give a formula for $\bar{a}.\bar{b}$ that depends on a and b and then, taking note of the fact that there are many integers a' such that $\bar{a} = \overline{a'}$, show that $\overline{a'}.\bar{b} = \bar{a}.\bar{b}$.
   (b) Prove that the multiplication in $\mathbb{Z}_m$ is associative.
   (c) Is your multiplication commutative? Explain.
   (d) Prove the distributive law: $\bar{a}.(\bar{b} + \bar{c}) = \bar{a}.\bar{b} + \bar{a}.\bar{c}$.
   (e) Show that $\mathbb{Z}_m$ has an identity element for multiplication.

(2) State and prove a result that begins: *An element $\bar{a} \in \mathbb{Z}_m$ has a multiplicative inverse if and only if a ....*

(3) State and prove a result that begins: *Every non-zero element in $\mathbb{Z}_m$ has a multiplicative inverse if and only if m ...*

(4) An element $f \in \mathbb{F}_q[x]$ is irreducible if the only possible factorizations of it are of the form $f = gh$ where either g or h is a constant. For example, in $\mathbb{F}_3[x]$, $x^3 + 1$ is NOT irreducible because it equals $(x + 1)^3$. List all the irreducible polynomials in $\mathbb{F}_2[x]$ of degrees 2, 3, and 4 and give a brief explanation as to why these are irreducible.

(5) A polynomial $f \in \mathbb{F}_q[x]$ is monic if its leading coefficient is 1, i.e., if $f = x^n$+lower degree terms. Write down all irreducible monic polynomials in $\mathbb{F}_3[x]$ of degrees 2 and 3 and give a brief explanation as to why these are irreducible.

(6) Rewrite the addition and multiplication tables for the field $\mathbb{F}_4$ as I presented them in class. Write down all monic irreducible quadratic polynomials in $\mathbb{F}_4[x]$. Also give an example of a monic irreducible cubic polynomial in $\mathbb{F}_4[x]$ and explain why it is irreducible.

(7) In $\mathbb{F}_p[x]$ show that $(x + 1)^p = x^p + 1$.

(8) Pick an irreducible cubic polynomial $f \in \mathbb{F}_2[x]$. Construct a field with eight elements (let's use the letter K to denote it) by adjoining a root α of f to $\mathbb{F}_2$, i.e.,
$$K = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{F}_2\}$$
and we add and multiply these in the obvious manner. What is α^3 equal to? Write out the addition and multiplication tables for K—please try to present these in a neat and tidy way so the grader can read them.

(9) Does every non-zero element in K have a multiplicative inverse? Explain.

(10) In the above exercises we are NOT thinking of a polynomial as a function, simply as a formal expression. However, every polynomial $f \in \mathbb{F}_q[x]$ can be thought of as a function $f : \mathbb{F}_q \to \mathbb{F}_q$ by defining $f(a)$ to be the element of $\mathbb{F}_q$ obtained by *plugging in* a and evaluating. Find a non-zero cubic polynomial $f \in \mathbb{F}_3[x]$ such that $f(a) = 0$ for all $a \in \mathbb{F}_3$. Find two distinct cubic polynomials f and g in $\mathbb{F}_3[x]$ such that $f(a) = g(a)$ for all $a \in \mathbb{F}_3$,

(11) Find another person in this class who has done Exercise 8 with a different polynomial f. Call the two different fields that the two of you have K_1 and K_2. Write down both addition and multiplication tables using different notations for the elements in K_1 and K_2, i.e., if you used α in Exercise 8 write β for the other person's α (otherwise α would have two different meanings!!). Write down an explicit isomorphism $\theta : K_1 \to K_2$. First define what you mean by an isomorphism in this context!! (Hint: in looking for θ don't tie your hands by insisting that $\theta(\alpha) = \beta$! Maybe it does, maybe not.)

403 Homework 1/14/06

(1) Let $f : R \to S$ be a bijective ring homomorphism. Show that its inverse is a ring homomorphism. We call such an f a ring isomorphism and say that R and S are isomorphic.

(2) Let I denote the kernel of a ring homomorphism $f : R \to S$. That is,

$$I = \ker f := \{x \in R \mid f(x) = 0\}.$$

Show that I is a subgroup of $(R, +)$ and that if $x \in I$ and $r \in R$, then xr and rx are in I also. A subset with these properties is called an ideal of R.

(3) Find all ideals in $\mathbb{Z}$, the ring of integers.

(4) Find all ideals in a field k.

(5) Suppose that I is an ideal in a ring R. Show that the quotient R/I can be given the structure of a ring. By R/I we mean the usual quotient of the abelian group R by the subgroup I; I is normal because $(R, +)$ is abelian.

(6) Write down an obvious map $\pi : R \to R/I$ and show that it is a ring homomorphism. Determine its kernel.

(7) Prove the first isomorphism theorem for rings: if $f : R \to S$ is a ring homomorphism, then the image of f is a subring of (i.e., a subset of S that forms a ring under the addition and multiplication in S and has the same identity as S), and that there is an isomorphism of rings

$$R/\ker f \cong \mathrm{im}(f).$$

(8) Let L, M, N be subspaces of a vector space and consider the vector space V/N. Show that

$$\left(\frac{L+N}{N}\right) \bigcap \left(\frac{M+N}{N}\right)$$

contains

$$\frac{(L \cap M) + N}{N}$$

but give an example to show that sometimes it is strictly bigger.