David Beydler
MATH 540B
Due: 1/30/08

HW #2

$\boxed{9.1}$ 4) [Prove that the ideals (x) and (x,y) are prime ideals in $\mathbb{Q}[x,y]$ but only the latter ideal is a maximal ideal.]

Pf: <u>(x) is a prime ideal:</u> (by contradiction)
First note that $(x) \neq \mathbb{Q}[x,y]$, since $y \notin (x)$.
Now, suppose that $f(x,y)g(x,y) \in (x)$ for $f(x,y), g(x,y) \in \mathbb{Q}[x,y]$. Then $\exists h(x,y) \in \mathbb{Q}[x,y]$ s.t. $f(x,y)g(x,y) = h(x,y)x$. Suppose that $f(x,y) \notin (x)$ and $g(x,y) \notin (x)$. Then each polynomial would have a term with no x factor. Thus, when we multiply f and g, we would get a term with no x factor. This is a problem, since then $f(x,y)g(x,y) \notin (x)$, which is a contradiction. So, $f(x,y) \in (x)$ or $g(x,y) \in (x)$. Thus, (x) is a prime ideal.

<u>(x) is not a maximal ideal:</u>
Consider (x,y). We have $(x) \subseteq (x,y) \subseteq \mathbb{Q}[x,y]$. But since $y \in (x,y)$ and $y \notin (x)$, $(x) \neq (x,y)$. Also, since $2 \in \mathbb{Q}[x,y]$ and $2 \notin (x,y)$, $(x,y) \neq \mathbb{Q}[x,y]$. Thus, (x) is not maximal.

<u>(x,y) is a maximal ideal:</u>
(helped by Angelica)
Define $\phi: \mathbb{Q}[x,y] \to \mathbb{Q}$ by $\phi(f(x,y)) = f(0,0)$ for $f(x,y) \in \mathbb{Q}[x,y]$. In words, ϕ sends $f(x,y)$ to its constant term.
ϕ is a ring homomorphism since if $f(x,y), g(x,y) \in \mathbb{Q}[x,y]$ such that $\phi(f(x,y)) = a$ and $\phi(g(x,y)) = b$, then

$$\phi(f(x,y) + g(x,y)) = a + b = \phi(f(x,y)) + \phi(g(x,y)), \text{ and}$$
$$\phi(f(x,y)g(x,y)) = ab = \phi(f(x,y))\phi(g(x,y)).$$

The above argument makes sense since a and b are the constant terms of f and g, respectively. Also note that
$\ker\phi = \{f(x,y) \in \mathbb{Q}[x,y] \mid \phi(f(x,y)) = f(0,0) = 0\} = \{f(x,y) \mid f(x,y) \text{ has constant term } 0\} = (x,y)$
So, by the first iso thm, $\mathbb{Q}[x,y]/(x,y) \cong \phi(\mathbb{Q}[x,y]) = \mathbb{Q}$
So, (x,y) is a maximal ideal. ▨ (ϕ is onto since $\phi(q) = q$ for all $q \in \mathbb{Q}$)

(Also, since (x,y) is a maximal ideal, it is a <u>prime ideal</u>.)

DB2

$\boxed{9.2}$ 5) [Exhibit all the ideals in the ring $F[x]/(p(x))$, where F is a field and $p(x)$ is a polynomial in $F[x]$ (describe them in terms of the factorization of $p(x)$).]

The 1-1 correspondence is given by the map $\pi: F[x] \to F[x]/(p(x))$ where $\pi(f(x)) = f(x)+(p(x))$.

Since $F[x]$ is a ring, and $(p(x))$ is an ideal of $F[x]$, Thm 7.3.8 says that the ideals of $F[x]$ containing $(p(x))$ and the ideals of $F[x]/(p(x))$ are in 1-1 correspondence. Now, since F is a field, $F[x]$ is a Euclidean Domain, so all of its ideals are principal.

Now, consider an ideal of $F[x]$ containing $(p(x))$, call it $(h(x))$. Since $p(x) \in (p(x)) \subset (h(x))$, we must have that there is an $f(x) \in F[x]$ such that $p(x) = f(x)h(x)$. Thus h divides p. So, h must be a factor of p.

With this knowledge, we conclude that the only ideals of $F[x]$ containing $(p(x))$ are $(p_1(x)), \ldots, (p_n(x))$, where $p_i(x)$ is a factor of $p(x)$. Thus, the ideals of $F[x]/(p(x))$ are the sets that look like $\{f(x)+(p(x)) \mid f(x) \in (p_i(x))\}$ for $i=1,\ldots,n$.

DB3

(handout) 1) a) [Find an irreducible polynomial of degree 2 over $\mathbb{Z}_3$. Prove that it is irreducible.]

Consider $f(x) = x^2+1$. Since $\deg(f) = 2$, f is irreducible over $\mathbb{Z}_3$ iff f has no roots in $\mathbb{Z}_3$. Let's check:

$f(0) = 0^2+1 = 1$
$f(1) = 1^2+1 = 2$
$f(2) = 2^2+1 = 2$

f has no roots in $\mathbb{Z}_3$, so f is irreducible over $\mathbb{Z}_3$.

b) [Construct a field $\mathbb{F}_9$ of size 9.]

Consider $\mathbb{Z}_3[x]/(x^2+1) = \{a+b\theta \mid a,b \in \mathbb{Z}_3\}$, where $\theta = x+(x^2+1)$ so that $\theta^2+1=0$. This is a field since $\mathbb{Z}_3$ is a field and x^2+1 is irreducible over $\mathbb{Z}_3$. It also has size 9, since

$$\mathbb{Z}_3[x]/(x^2+1) = \{0, 1, 2, \theta, 1+\theta, 2+\theta, 2\theta, 1+2\theta, 2+2\theta\}$$

So, just let $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$.

see next page

DB4

(handout cont) (1 cont)

c) [What is the prime subfield of $\mathbb{F}_q$?]

$\{0\} \subset \mathbb{F}_q$ is the prime subfield of $\mathbb{F}_q$.

d) [If $\mathbb{F}$ is a finite field, then it can be shown that $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ is a cyclic group under multiplication. Prove this for your finite field $\mathbb{F}_q$ in part (b).]

Pf: Consider $\theta + 1 \in \mathbb{F}_q^\times$. (Note $\theta^2 + 1 = 0$, so $\theta^2 = 2$)

$$(\theta+1)^2 = \theta^2 + 2\theta + 1 = \cancel{(\theta^2+1)}^{0} + 2\theta = 2\theta$$
$$(\theta+1)^3 = 2\theta(\theta+1) = 2\theta^2 + 2\theta = 2\cdot 2 + 2\theta = 2\theta + 1$$
$$(\theta+1)^4 = (2\theta+1)(\theta+1) = 2\theta^2 + \cancel{2\theta + \theta}^{0} + 1 = 2\theta^2 + 1 = 2\cdot 2 + 1 = 2$$
$$(\theta+1)^5 = 2(\theta+1) = 2\theta + 2$$
$$(\theta+1)^6 = (2\theta+2)(\theta+1) = 2\theta^2 + 2\theta + 2\theta + 2 = \theta$$
$$(\theta+1)^7 = \theta(\theta+1) = \theta^2 + \theta = \theta + 2$$
$$(\theta+1)^8 = (\theta+2)(\theta+1) = \theta^{2 \to 2} + \cancel{\theta + 2\theta}^{0} + 2 = 1$$

Since $|\theta+1| = 8$ in $\mathbb{F}_q^\times$ (and $|\mathbb{F}_q^\times| = 8$), we conclude that $\langle \theta+1 \rangle = \mathbb{F}_q^\times$, so $\mathbb{F}_q^\times$ is cyclic.