Selected exercises from *Abstract Algebra* by *Dummit and Foote* (3rd edition).

Bryan Félix

Abril 12, 2017

Section 9.1

**Exercise 13.** Prove that the rings $F[x, y]/(y^2 - x)$ and $F[x, y]/(y^2 - x^2)$ are not isomorphic for any field $F$.

**Proof.** First, we show that $F[x, y]/(y^2 - x) \cong F[t]$. Let $\varphi : F[x, y] \to F[t]$ be an homomorphism given by $\varphi(x) = t^2$, $\varphi(y) = t$ and $\varphi(f) = f$ (for all $f \in F$). Note that the kernel of the homomorphism is precisely $(y^2 - x)$, therefore by the 1st isomorphism theorem $F[x, y]/(y^2 - x) \cong F[t]$. Furthermore since $F[t]$ is an integral domain, so is $F[x, y]/(y^2 - x)$. Now, we will show that $F[x, y]/(y^2 - x^2)$ has zero divisors, thus is not an integral domain and the conclusion will follow. Observe that $(y - x)(y + x) = y^2 - x^2 = 0$. We are done as neither $(y - x)$ nor $(y + x)$ is zero. 

**Exercise 14.** Let $R$ be an integral domain and let $i, j$ be relatively prime integers. Prove that the ideal $(x^i - y^j)$ is a prime ideal in $R[x, y]$. [Consider the ring homomorphism $\varphi$ form $R[x, y]$ to $R[t]$ defined by mapping $x$ to $t^j$ and mapping $y$ to $t^i$. Show that an element of $R[x, y]$ differs from an element in $(x^i - y^j)$ by a polynomial $f(x)$ of degree at most $j - 1$ in $y$ and observe that the exponents of $\varphi(x^i y^s)$ are distinct for $0 \leq s < j$.]

**Proof.** Taking the hint, it suffices to show that $R[x, y]/(x^i - y^j)$ is isomorphic to $R[t]$ by means of $\varphi$. Then, by Proposition 13, section 7.4 the ideal $(x^i - y^j)$ is prime since $R[t]$ is an integral domain.

First we show that the kernel of $\varphi$ is equal to $(x^i - y^j)$. If we take $r(x^i - y^j) \in (x^i - y^j)$, note that

$$\varphi(r(x^i - y^j)) = r\varphi(x^i - y^j) = r(t^i - t^j) = 0,$$

hence, $(x^i - y^j) \subset \ker(\varphi)$. For the reverse inclusion we write an element $g(x, y) \in R[x, y]$ as

$$f_0(x)y^0 + f_1(x)y^1 + \cdots + f_n(x)y^n.$$

Then, by doing ”long division” of between $g(x, y)$ and $x^i - y^j$ in the $y$ variable, we can write $g(x, y)$ as

$$g(x, y) = (x^i - y^j)(q(x, y)) + \sum_{n=0}^{j-1} h_n(x)y^n.$$
Now, we let \( g(x, y) \) be in the kernel of \( \varphi \), it follows that

\[
\varphi(g(x, y)) = \varphi((x^i - y^j)(q(x, y))) + \sum_{n=1}^{j-1} \varphi(h_n(x))\varphi(y^n)
\]

\[
= \sum_{i=1}^{j-1} \varphi(h_n(x))t^{ni}
\]

Note that the latter can be written as

\[
\sum_{i=1}^{j-1} \varphi \left( \sum_{m=0}^{k} r_m x^m \right) t^{ni},
\]

where \( r_m \) is an element of \( R \). Then,

\[
\varphi(g(x, y)) = \sum_{i=1}^{j-1} \varphi(h_n(x))t^{ni}
\]

\[
= \sum_{i=1}^{j-1} \varphi \left( \sum_{m=0}^{k} r_m x^m \right) t^{ni}
\]

\[
= \sum_{i=1}^{j-1} \left( \sum_{m=0}^{k} r_m \varphi(x^m) \right) t^{ni}
\]

\[
= \sum_{i=1}^{j-1} \left( \sum_{m=0}^{k} r_m t^{mj} \right) t^{ni}
\]

\[
= \sum_{i=1}^{j-1} \left( \sum_{m=0}^{k} r_m t^{mj+ni} \right)
\]

Now, we show that the exponents \( mj + ni \) are distinct for positive values of \( n, m \).
Assume \( mj + ni = m'j + n'i \). Taking the equation modulo \( j \) we have

\[
ni = n'i \mod j.
\]

Then, since \( \gcd(i, j) = 1 \) we have an inverse of \( i \) modulo \( j \), therefore

\[
n = n' \mod j.
\]

Furthermore since \( n \) only ranges from 0 to \( j - 1 \), it must be the case that \( n = n' \). Then we have \( mj + ni = m'j + ni \) if and only if \( mj = m'j \) and hence \( m = m' \) as desired. Thus the coefficients \( r_m \) above are all identically equal to 0 if \( g(x, y) \) is in the kernel of \( \varphi \). This "lifts" to the functions \( h_m(x) \), making them equal to 0 as well. It follows that \( g(x, y) \) is in the kernel if and only if it is in the ideal \( x^i - y^j \).

We conclude that \( R[x, y]/(x^i - y^j) \) is isomorphic to \( R[t] \) by the first isomorphism theorem and hence \( (x^i - y^j) \) is a prime ideal.

\[\square\]

**Section 9.2**

**Exercise 4.** Let \( F \) be a finite field. Prove that \( F[x] \) contains infinitely many primes.
Proof. Note that since $F$ is a field, then $F[x]$ is an euclidean domain. We will prove the exercise for an arbitrary euclidean domain mocking Eucli’s proof of the infinitude of primes. Let $R$ be an Euclidean domain and assume that $R$ has finitely many primes, $p_1, p_2, \ldots p_n$.

Consider the element $s = (p_1 \cdot p_2 \cdots p_n) + 1$ where 1 is the additive unit in the ring. Observe that $\deg(s) \geq 1$ as $p_i$ can not have degree 0 (otherwise it is a unit coming from $F$). This implies that $s$ is not a unit nor 0. Now, since there are finitely many primes in $R$, there must exist $p_i$ such that $s = p_i \cdot q$, in particular $p_i$ must divide 1 and hence it is a unit. Arriving at a contradiction since $p_i$ is a prime.

Exercise 7. Determine all the ideals of the ring $\mathbb{Z}[x]/(2, x^3 + 1)$.

Proof. Note that by the 3rd isomorphism theorem,

$$\mathbb{Z}[x]/(2, x^3 + 1) \equiv (\mathbb{Z}[x]/(2))/((2, x^3 + 1)/(2)) \equiv \mathbb{Z}/2\mathbb{Z}[x]/(x^3 + 1).$$

It follows that $\mathbb{Z}/2\mathbb{Z}$ is a field, then $\mathbb{Z}/2\mathbb{Z}[x]$ is a principal ideal domain. By the 4th isomorphism theorem there is a one to one correspondance with the ideals of $\mathbb{Z}/2\mathbb{Z}[x]/(p)$ and those ideals that contain $p$. Therefore, the ideals of $\mathbb{Z}/2\mathbb{Z}[x]$ have the form $(p)/(x^3 + 1)$. In order for the latter to be well defined $p$ must be a divisor of $x^3 + 1$. It follows that the ideals are are $(1)/(x^3 + 1)$, $(x + 1)/(x^3 + 1)$, $(x^2 - x + 1)/(x^3 + 1)$ and $(x^3 + 1)/(x^3 + 1)$.

\qed