Math 415B Midterm 2 Practice

Max von Hippel

April 15, 2019

Homework 5

Question 5

Assume $\mathbb{F}$ is a field and let $\mathbb{F}(X)$ be the field of fractions of the polynomial ring $\mathbb{F}[X]$. Show that there is no element of $\mathbb{F}(X)$ whose square is X.

Proof. Assume by way of contradiction that

$$\rho(X) = \sum_{i=0}^{n} \frac{\alpha_i}{\beta_i} X^i \in \mathbb{F}(X)$$

is such that $\rho(X)^2 = X$.

$$\iff (\sum_{i=0}^{n} \frac{\alpha_i}{\beta_i} X^i \in \mathbb{F}(X))^2 = (\frac{\alpha_n}{\beta_n})^2 X^{2n} + \text{ some coefficient } X^{2n-1}$$

$$+ ... + \text{ some other coefficient } X^2 + 2(\frac{\alpha_1}{\beta_1}\frac{\alpha_0}{\beta_0})X + (\frac{\alpha_0}{\beta_0})^2$$

Clearly all the coefficients except for

$$2(\frac{\alpha_1}{\beta_1}\frac{\alpha_0}{\beta_0}) = 1$$

must equal zero. So the leading coefficient,

$$\frac{\alpha_n}{\beta_n}$$

must equal zero. Since there are no zero divisors in a field it follows that $\alpha_n = 0$. Inductively, for each $n > 1$, $\alpha_n = 0$. So:

$$\rho(X) = \frac{\alpha_1}{\beta_1} X + \frac{\alpha_0}{\beta_0}$$

$$\implies \rho(X)^2 = (\frac{\alpha_1}{\beta_1})^2 X^2 + 2(\frac{\alpha_1}{\beta_1}\frac{\alpha_0}{\beta_0})X + (\frac{\alpha_0}{\beta_0})^2$$

By the same logic as before, it follows that

$$(\frac{\alpha_1}{\beta_1})^2 = 0$$

But then as there are no zero divisors in a field:

$$\implies \frac{\alpha_1}{\beta_1} = 0 \implies \alpha_1 = 0$$

So we can re-write $\rho(X)$:

$$\rho(X) = \frac{\alpha_0}{\beta_0}$$

Since the degree of $\rho(X)$ is zero, the degree of $\rho(X)^2$ is zero. So, $\rho(X)^2 \neq X$ because the degree of X is 1.

We have therefore proven by way of contradiction that there is no element of $\mathbb{F}(X)$ whose sequare is X. $\square$

Question 6

For every prime p show that

$$X^{p-1} - 1 = (X-1)(X-2)...(X-(p-1)) \text{ in } \mathbb{F}_p[X].$$

Proof. From Group Theory we know that $U(\mathbb{F}_p) = \{1, 2, ..., p-1\}$ is a cyclic group of order $p-1$, therefore the order $|j|$ must divide the group order $|U(\mathbb{F}_p)|$ for each $j \in 1, 2, ..., p-1$. So for each unit j, we have $j^{|U(\mathbb{F}_p)|} = j^{p-1} = 1$. Then $j^{p-1} - 1 = 0$ so j is a root of the polynomial $X^{p-1} - 1$; so every unit of $\mathbb{F}_p$ is a root of that polynomial. By the Factor Theorem it follows that $(X-1), ..., (X-(p-1))$ are all divisors of $X^{p-1} - 1$. Let $f'(X) \in \mathbb{F}_p[X]$ be such that $X^{p-1} - 1 = (X-1)f'(X)$. Note that $(X-2)$ does not divide $(X-1)$, $X-1$ is irreducible, and $X-2$ does divide $X^{p-1} - 1$ if $p > 2$. In this case we must hve that $X-2$ divides $f'(X)$; by induction it immediately follows that there exists some $f^*(X) \in \mathbb{F}_p[X]$ such that $X^{p-1} - 1 = (X-1)(X-2)...(X-(p-1))f^*(X)$. The degree of the left hand side is $p-1$ so this also must be the degree of the right hand side. So $p - 1 = deg((X-1)(X-2)...(X-(p-1))f^*(X)) = \deg((X-1)(X-2)...(X-(p-1))) + \deg(f^*(X)) = (p-1) + \deg(f^*(X)) \implies \deg(f^*(X)) = 0$; so $f^*(X)$ is a constant $c \in \mathbb{F}_p$. Then the leading coefficient is $1 * 1 * ... * 1 * c = 1 * c = 1$ so $c = 1^{-1} = 1$. So, $X^{p-1} - 1 = (X-1)(X-2)...(X-(p-1))$, and we are done. □

Question 7

Prove that $\mathbb{Z}[X]$ is not a PID.

Proof. Consider the ideal $\langle 3, X \rangle$.

$$\langle 3, X \rangle = \Big\{ 2f(X) + Xg(X) \mid f(X), g(X) \in \mathbb{Z}[X] \Big\}$$

Assume by way of contradiction that $\langle \gamma(X) \rangle = \langle 3, X \rangle$. Then $t(X)\gamma(X) = 1 \cdot 3 = 3$ for some $t(X) \in \mathbb{Z}[X]$; so by the division algorithm $\deg(\gamma(X)) = 0$. Since 3 is prime, we must have that $\gamma(X) = 1$ or $\gamma(X) = 3$. If $\gamma(X) = 3$ then $\langle \gamma(X) \rangle = \{3u(X) \mid u(X) \in \mathbb{Z}[X]\}$; this does not include $3(X^2 + X) + 11X$, which is included in $\langle 3, X \rangle$. If $\gamma(X) = 1$ then $\langle \gamma(X) \rangle = \{u(X) \mid u(X) \in \mathbb{Z}[X]\} = \mathbb{Z}[X]$; this includes 4 which is not included in $\langle 3, X \rangle$. So in all cases we reach a contradiction. We conclude that no such $\gamma(X)$ exists, and therefore specifically that $\langle 3, X \rangle$ is not principal. But in a principal ideal domain every ideal is principal; so $\mathbb{Z}[X]$ is not a PID and we are done. □

Question 8

Prove that $\mathbb{Q}[X]/\langle X^2 - 2 \rangle$ is isomorphic to $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$.

Proof. Define a natural evaluation map $\epsilon_{\sqrt{2}} : \mathbb{Q}[X] \to \mathbb{Q}$ to be $f(X) \mapsto f(\sqrt{2})$.

Let $f(X) \in \mathbb{Q}[X]$ arbitrarily. As $\sqrt{2} \notin \mathbb{Q}$ but $\sqrt{2}^2 \in \mathbb{Q}$ clearly $\epsilon_{\sqrt{2}}(f(X)) = 0 \implies f(X) = 0$ or $\deg(f(X)) > 1$. In the latter case, use the Division Algorithm to write $f(X) = q(X)(X^2 - 2) + r(X)$ where $q(X), r(X) \in \mathbb{Q}[X]$ and $\deg(r(X)) < \deg(X^2 - 2) = 2$. Observe that the evaluation map is a homormorphism $\mathbb{Q}[X] \to \mathbb{Q}[\sqrt{2}]$ (we've proven this in the general case in class), so $\epsilon_{\sqrt{2}}(f(X)) = \epsilon_{\sqrt{2}}(q(X))(\sqrt{2}^2 - 2) + \epsilon_{\sqrt{2}}(r(X)) = \epsilon_{\sqrt{2}}(r(X))$. $r(X)$ is of the form $aX + b$ (by our argument from before about its degree being bounded above by 2). $a\sqrt{2} + b = 0 \iff a = b = 0$ as $\sqrt{2} \notin \mathbb{Q}$. So, $\epsilon_{\sqrt{2}}(f(X)) = 0 \iff f(X) = q(X)(X^2 - 2)$ for some $q(X) \in \mathbb{Q}[X]$, which in turn holds iff $f(X) + \langle X^2 - 2 \rangle = 0 \in \mathbb{Q}[X]/\langle X^2 - 2 \rangle$. We conclude that $\mathrm{Ker}(\epsilon_{\sqrt{2}}) = \langle X^2 - 2 \rangle$. So then by the First Isomorphism Theorem, $\mathbb{Q}[X]/\mathrm{Ker}(\epsilon_{\sqrt{2}}) = \mathbb{Q}[X]/\langle X^2 - 2 \rangle \cong \mathrm{Im}(\epsilon_{\sqrt{2}}(\mathbb{Q}[X])) = \mathbb{Q}[\sqrt{2}]$ and we are done. □

Question 9

State and prove a version of Question 2 for arbitrary group rings $R[G]$ and $S[G]$.

TODO

If $\phi : G \to H$ is a group homomorphism and R is a ring then can you get a ring homomorphism $R[G] \to R[H]$?

TODO

What about $R[H] \to R[G]$?

TODO

Homework 7

Question 5

Let R be an integral domain and $\mathbb{F}$ its field of fractions. We will consider $R \subseteq \mathbb{F}$ to be the subring $\{x/1 \mid x \in R\}$. Hence, we naturally have $R[X] \subseteq \mathbb{F}[X]$. Assume $f, g \in R[X]$ are polynomials with $g \neq 0$. Then by the division algorithm there exist unique polynomials $q, r \in \mathbb{F}[X]$ such that $f = qg + r$ and either $r = 0$ or $\deg(r) < \deg(g)$.

Show that if $g = b_m X^m + ... + b_0$ and $b_m \in U(R)$ is a unit then $q, r \in R[X]$.

TODO

Question 6

Assume $\mathbb{F}$ is a finite field with $|\mathbb{F}| = q$. If $n > 0$ is an integer then let $\sigma(n, q)$ denote the number of monic irreducible polynomials $f \in \mathbb{F}[X]$ with $\deg(f) = n$, i.e., the leading term is X^n. Give a formula for $\sigma(2, q)$ and $\sigma(3, q)$ as a function of q.

TODO

Are there more or less irreducible polynomials than reducible polynomials?

TODO

Question 7

Assume $\mathbb{F}$ is a field. Explain why, when looking for irreducible polynomials, it suffices to consider monic polynomials, i.e., polynomials of the form $X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0 \in \mathbb{F}$.

Proof. Assume that $f(X) = a_n X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0$ is irreducible. So whenever $f(X) = g(X)h(X)$ either $g(X)$ is a unit or $h(X)$ is a unit. But $f(X) = a_n(f(X)/a_n) = a_n(X^n + (a_{n-1}a_n^{-1})X^{n-1} + (a_{n-2}a_n^{-1})X^{n-2} + ... + (a_0 a_n^{-1}))$ □

Question 8

Find all monic irreducible polynomials of degree 2 over $\mathbb{F}_3$.

Proof. For it to be monic and of degree 2 it must be of the form $f(X) = X^2 + a_1 X + a_0$. By the Reducibility Test for degrees 2 and 3, $f(x)$ is reducible if and only if it has a 0. Our possible polynomials are

- X^2 has root 0
- $X^2 + X$ has root 0
- $X^2 + 2X$ has root 0
- $X^2 + 1$ has no root, because $1 \neq 0, 1^2 + 1 = 2 \neq 0, 2^2 + 1 = 5 = 2 \bmod 3 \neq 0$. So this is an irreducible.
- $X^2 + 2$ has root 1.
- $X^2 + X + 1$ has root 1.

- $X^2 + X + 2$ has no root, because $2 \neq 0$, $1^2 + 1 + 2 = 1 + 3 = 4 = 1 \bmod 1 \neq 0, 2^2 + 2 + 2 = 8 = 2 \bmod 3 \neq 0$. So this is an irreducible.
- $X^2 + 2X + 1$ has root 2.
- $X^2 + 2X + 2$ has no root, because $2 \neq 0, 1 + 2 + 2 = 5 = 2 \bmod 3 \neq 0, 2^2 + 2(2) + 2 = 1 \neq 0$. So this is an irreducible.

So the irreducible monic polynomials of degree 2 over $\mathbb{F}_3$ are exactly $X^2 + 1, X^2 + X + 2$, and $X^2 + 2X + 2$. $\square$