

Homework 8 due Wed, Nov 24th by 11am in Gradescope

Name: Sean Eva

GTID: 903466156

Collaborators:

Outside resources:

INSERT a “pagebreak” command between each problem (integer numbers). Problem subparts (letter numbered) can be on the same page.

REMOVE all comments (within “textit{ }” commands) before submitting solutions.

DO NOT include any identifying information (name, GTID) except on the first/cover page.

1. (a) Problem 4.6 # 1.

Let assumptions be as in the problem statement. This substitution of x to $x+1$ made in Example 5 is an automorphism of $f(x) \in \mathbb{Q}[x]$. If we define a function of $\phi : F[x] \rightarrow F[x]$ such that $\phi(f(x)) = f(x+1)$. We want to show that ϕ is an automorphism which is to say that it conserves addition and multiplication, is one to one, onto, and the codomain is equal to the domain. By the definition of ϕ the codomain is equal to the domain. Then we can see that $\phi(f(x) + g(x)) = \phi((a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n) = (a_0 + b_0) + (a_1 + b_1)(x+1) + \dots + (a_n + b_n)(x+1)^n = a_0 + a_1(x+1) + \dots + a_n(x+1)^n + b_0 + b_1(x+1) + \dots + b_n(x+1)^n = \phi(f(x)) + \phi(g(x))$, and similarly $\phi(f(x)g(x)) = \phi((fg)(x)) = (fg)(x+1) = f(x+1)g(x+1) = \phi(f(x))\phi(g(x))$. Therefore, ϕ preserves addition and multiplication in the field. Now in order to show that ϕ is one to one suppose we have two polynomials $f(x), g(x) \in F[x]$ such that $\phi(f(x)) = \phi(g(x))$. This means that $a_0 + a_1(x+1) + \dots + a_n(x+1)^n = b_0 + b_1(x+1) + \dots + b_m(x+1)^m$ and by polynomial equalities we then know that $n = m$ and $a_i = b_i$ for $0 \leq i \leq n$ and then this implies that $f(x) = g(x)$. Therefore, ϕ is one to one. Now we want to show that ϕ is onto. Let $f(x+1) = a_0 + a_1(x+1) + \dots + a_n(x+1)^n$ it is easy to see the preimage of this function is $f(x)$ where $\phi(f(x)) = f(x+1)$. Therefore, ϕ is onto. Since ϕ preserves addition and multiplication in the field, one to one, onto, and the codomain is equal to the domain we have that ϕ is an automorphism. This automorphism gives us a polynomial that is irreducible which implies that the polynomial we had before the automorphism is also irreducible.

(b) Explain how this generalizes to primes $p > 5$ (c.f. Problem 4.6 #5).

Let assumptions be as in the problem. Let us consider $f(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \dots + \binom{p}{1}$ by the binomial theorem to expand the polynomial. This then implies that each coefficient except the leading coefficient is divisible by p and that p^2 does not divide the constant term. By the Eisenstein Criterion, $f(x+1)$ is then irreducible and then $f(x)$ is irreducible too.

2. Problem 4.6 # 4.

Let assumptions be as in the problem statement. Let us assume to the contrary that $f(x)$ is not irreducible. Then that is to say that $f(x) = g(x)h(x)$ for some $g(x) = b_r x^r + b_{r-1} x^{r-1} + \dots + b_0, h(x) = c_s x^s + c_{s-1} x^{s-1} + \dots + c_0 \in \mathbb{Z}[x]$ where $r, s \geq 1$ and $r + s = n$. Since we have that $p|a_0$ and $p^2 \nmid a_0$ and since $a_0 = b_0 c_0$ then since $p|a_0$ then $p|b_0$ and $p|c_0$ but $p^2 \nmid b_0$ and $p^2 \nmid c_0$. Suppose then that $p|b_0$ but $p \nmid c_0$. By our assumption $p \nmid a_n$ and $a_n = b_r c_s$ so none of b_r and c_s can be divided by p . Thus, if a_r is the r th coefficient of reducible polynomial $f(x)$. Then, $a_r = b_r c_0 + b_{r-1} c_1 + \dots + b_0 c_r$ where $p \nmid b_r c_0$. Now we want to prove $p|b_0, b_1, \dots, b_{r-1}$. As $p|a_r$ then $b_r c_0 = a_r - (b_{r-1} c_1 + \dots + b_0 c_r)$ is divisible by p , which is a contradiction to our assumption. Since $p|b_0$ then $p|b_0 c_r$ and $p|a_1$. And since c_0 is not a multiple of p then $p|b_1$. Then by induction, b_i is a multiple of $p, \forall i < r$. Hence the statement is proved.

3. Problem 4.6 # 6.

Let assumptions be as in the problem statement. Given that ϕ is an automorphism such that $\phi(a) = a \forall a \in F$. Let $f(x)$ be irreducible, then let $g(x) = \phi(f(x))$ is nonzero and have nonunit. Let $g(x) = \phi(f(x)) = u(x)v(x)$ where $u(x), v(x) \in F[x]$. Then, $f(x) = \phi^{-1}(u(x))\phi^{-1}(v(x))$ and either $\phi^{-1}(u(x))$ or $\phi^{-1}(v(x))$ is a unit. This implies that $u(x)$ or $v(x)$ is a unit and then $g(x)$ is irreducible. Now let $\phi(f(x))$ be irreducible. Then $\phi(f(x))$ is nonzero and not a unit. This implies then that $f(x)$ is nonzero and not a unit. Let $f(x) = r(x)s(x)$ where $r(x), s(x) \in F[x]$. Then $g(x) = \phi(r(x))\phi(s(x))$ is a unit. Which implies that either $r(x)$ or $s(x)$ is a unit since ϕ is an automorphism. So $f(x)$ is irreducible.

4. Problem 4.6 # 9.

Let assumptions be as in the problem statement. In order to prove that ϕ is an automorphism we need to show that ϕ preserves both addition and multiplication, is onto, is one to one, and the codomain is the same as the domain. The codomain is the same as the domain by the definition of ϕ from the problem statement. Then suppose we have $f(x) = a_0 + a_1(x) + \dots + a_n(x)^n, g(x) = b_0 + b_1(x) + \dots + b_n(x)^n \in F[x]$, then we have that $\phi(f(x)) = a_0 + a_1(bx + c) + \dots + a_n(bx + c)^n, \phi(g(x)) = b_0 + b_1(bx + c) + \dots + b_n(bx + c)^n$, then $\phi(f(x)) + \phi(g(x)) = a_0 + a_1(bx + c) + \dots + a_n(bx + c)^n + b_0 + b_1(bx + c) + \dots + b_n(bx + c)^n = (a_0 + b_0) + (a_1 + b_1)(bx + c) + \dots + (a_n + b_n)(bx + c)^n = \phi(f(x) + g(x))$. Similarly, $\phi(f(x)g(x)) = \phi((fg)(x)) = (fg)(bx + c) = f(bx + c)g(bx + c) = \phi(f(x))\phi(g(x))$. Therefore, ϕ preserves addition and multiplication in the field which makes it a homomorphism. Now we will show that ϕ is one to one. Let us say $\phi(f(x)) = \phi(g(x))$ then identically to the process used in problem one of this homework assignment, $f(x) = g(x)$. Therefore, we know that ϕ is one to one. Again similarly to the process used in number one of this homework assignment, ϕ is onto. Therefore, since ϕ preserves addition and multiplication, is one to one, is onto, and the codomain is equal to the domain then ϕ is an automorphism. It is also simple to see that if $f(x) = a$ then $\phi(f(x)) = a$ which implies that $\phi(a) = a$.

5. Problem 4.6 # 11.

Let assumptions be as in the problem statement. Let $g(x) = \phi(x)$. Then it is easy to see that $\phi(f(x)) = f(g(x))$ for all $f(x) \in F[x]$, this follows from the given fact that ϕ is a ring automorphism which is a ring homomorphism. Suppose that $\deg(g(x)) \geq 2$, then $\deg(\phi(f(x))) \neq 1$. It follows then that ϕ is not surjective because there is no $f(x)$ such that $\phi(f(x)) = x$ since the latter side has degree 1. But then ϕ is not an automorphism which is a contradiction to our assumption that ϕ is an automorphism. Finally, suppose that $\deg(g(x)) = 0$ but then $\deg(\phi(f(x))) = \deg(f(g(x))) = 0$ for all $f \in F[x]$. Again, this implies that ϕ is not surjective and not an automorphism which is again a contradiction. Thus, $\deg(g(x)) = 1$, therefore $g(x) = bx + c$ where $b \neq 0$ and $b, c \in F$. Thus, $\phi(f(x)) = f(bx + c)$.

6. Problem 4.7 # 4.

Let assumptions be as in the problem statement. If we recall that $F = \{\frac{a}{b} | a, b \in D, b \neq 0\}$. Let $\frac{a}{b} \in F$ where $a, b \in D$ and $b \neq 0$. Since $a, b \in D$, therefore $b^{-1} \in D$ and then $ab^{-1} \in K$. Hence, $\frac{a}{b} \in K$ so $F \subset K$. Hence F is the smallest field containing D .