HOMEWORK 3 – MATH 392
January 26, 2018

ALEX THIES
athies@uoregon.edu

Problem 8.22. Prove Theorem 8.8.

Theorem 8. *Let K be a field and suppose $a(x), b(x) \in K[x]$ are associates. The polynomial $a(x)$ is irreducible over K if and only if $b(x)$ is irreducible over K.*

Proof. Let K, $a(x)$, and $b(x)$ be as above.

$\Rightarrow$) Assume $a(x)$ is irreducible over K, and suppose by way of contradiction that $b(x)$ is reducible over K. Then we know there exists polynomials $d(x)$,$f(x) \in K[x]$ such that $b(x) = d(x)f(x)$. And since $a(x)$ and $b(x)$ are associates we can write $a(x) = cb(x) = c[d(x)f(x)]\lightning$

This implies that $a(x)$, which we assumed to be irreducible over K, has factors in $K[x]$, a contradiction. A similar argument can be used to prove the converse. $\square$

Problem 8.23. Prove Theorem 8.9.

Theorem 9. *Let K be a field. Every polynomial in $K[x]$ of degree 1 is irreducible over K.*

Proof. Let K be a field and $a(x) \in K[x]$ such that $\deg a(x) = 1$. Since K is a field $K[x]$ is an integral domain and thus the degree of polynomials is additive in $K[x]$. We can write $a(x) = b(x)c(x)$, and since $\deg a(x) = 1$, we know that either $\beta = \deg b(x) = 1$ and $\gamma = \deg c(x) = 0$, or the other way around. This means that we can only factor $a(x)$ into associates, which is the definition of being irreducible.

Hence, for a field K, every polynomial in $K[x]$ of degree 1 is irreducible over K. $\square$

Problem 8.30. Complete the proof of Theorem 8.15.

Theorem 15. *Let K be a field and $a(x) \in K[x]$ with $a(x) \neq 0(x)$. The element $c \in K$ is a root of $a(x)$ if and only if $b(x) = -c + x$ is a factor of $a(x)$.*

Proof. Let K, $a(x)$ be as above.

$\Leftarrow$) Suppose that $b(x) = x - c$ is a factor of $a(x)$, we will show that $c \in K$ is a root of $a(x)$. Since $b(x)$ is a factor of $a(x)$, we can write $a(x) = b(x)d(x)$ for some polynomial $d(x)$. Further, since K is a field, $K[x]$ is an integral domain and the zero product property works like we'd like it to, so we have $a(c) = (c - c)d(c) = 0$, hence c is a root of $a(x)$. □

Problem 8.31. Use the PMI to prove Theorem 8.17, for any $n \geq 1$. In the inductive step when you have $a(x) = (-c_1 + x) \cdots (-c_k + x)q(x)$ be sure to show why $q(c_k + 1)$ must equal 0_K.

Theorem 17. *Suppose K is a field and $a(x) \in K[x]$ with $a(x) \neq 0(x)$. If the distinct elements $c_1, c_2, \ldots, c_n \in K$ are all roots of $a(x)$, then the product $b(x) = (-c_1 + x)(-c_2 + x) \cdots (-c_n + x)$ is a factor of $a(x)$.*

This one eluded me.

Problem 8.37. Prove Theorem 8.19.

Theorem 19. *Let K be a field. If $c_1, c_2, \ldots, c_n$ are distinct roots of the nonzero polynomial $a(x) \in K[x]$, then $\deg(a(x)) \geq n$.*

Proof. Let K, $a(x)$ be as above. By Theorem 8.17 we can write $a(x) = b(x)f(x)$ where $f(x) = \prod_{i=1}^{n}(x - c_i)$ for distinct roots $c_i \in K$. Since K is a field, $K[x]$ is an integral domain and degree is additive for elements of $K[x]$. Let $\deg a(x) = \alpha$, $\deg b(x) = \beta$, $\deg f(x) = \eta$. Its clear that $\eta = n$, and by the same reasoning that allows us to conclude that, we can also surmise $\alpha \geq \eta$, hence $\deg(a(x)) \geq n$, as desired. □

Problem 8.38. Complete the proof of Theorem 8.22.

Theorem 22. *Let K be a field and $a(x) \in K[x]$ with $\deg(a(x)) = 2$ or $\deg(a(x)) = 3$. The polynomial $a(x)$ is reducible over K if and only if $a(x)$ has a root in K.*

Proof. Let K, $a(x)$ be as above.

$\Leftarrow$) Assume $a(x)$ has a root $c \in K$, we will show that $a(x)$ is reducible over K. Since K is a field, $K[x]$ is an integral domain and the degree is additive. We'll proceed by cases.

Case 1: $\deg a(x) = 2$. When $\deg a(x) = 2$ we can write $a(x) = b(x)c(x)$ for polynomials $b(x), c(x) \in K[x]$. Let $\beta = \deg b(x)$ and $\gamma = \deg c(x)$, then we know $\beta + \gamma = 2$. But since $a(x)$ has a root, one of β or γ must be 1 since constant polynomials don't have roots. Hence, $\beta = \gamma = 1$, and we can write $a(x)$ as the product of non-constant polynomials, which defines $a(x)$ to be reducible.

Case 2: $\deg a(x) = 3$. When $\deg a(x) = 3$ we can write $a(x) = d(x)e(x)$ for polynomials $d(x), e(x) \in K[x]$. Let $\delta = \deg d(x)$ and $\varepsilon = \deg e(x)$, then we know $\delta + \varepsilon = 3$. But since $a(x)$ has a root, one of δ or ε must be 1 since constant polynomials don't have roots. And with one of δ or ε being 1, the other must be 2, again allowing $a(x)$ to satisfy the definition of being reducible over K.

Hence, for a field K and polynomial $a(x) \in K[x]$ such that $\deg(a(x)) = 2$ or $\deg(a(x)) = 3$, the polynomial $a(x)$ is reducible over K if and only if $a(x)$ has a root in K. $\square$

Problem 8.46. Prove Theorem 8.27.

Theorem 27. *Let K be a field and $a(x) \in K[x]$ with $a(x) \neq 0(x)$. If $\deg(a(x)) = n$ then there can be at most n distinct roots of $a(x)$ in K.*

Proof. Let K be a field and $a(x) \in K[x]$ with $a(x) \neq 0(x)$, and assume that $\deg a(x) = n$. Since $\deg a(x) = n$, we can write $a(x) = b(x)f(x)$ for some polynomials $b(x)$ and $f(x) = \prod_{i=1}^{n}(x - c_i)$, each of which is an element of $K[x]$, where $c_i \in K$ are the roots of $a(x)$. Notice that the linear factors that comprise $f(x)$ each has degree 1, thus $f(x) = \prod_{i=1}^{n}(x-c_i)$ has degree n, as K is a field and $K[x]$ and integral domain. That tells us that the only option for $b(x)$ is a constant polynomial with degree 0. This implies that $f(x)$ takes into account each of the distinct roots of $a(x)$, hence $a(x)$ has at most n distinct roots in K. $\square$

Problem 8.47. Let $a(x) = \frac{1}{3} + x + \frac{2}{3}x^2 + 3x^3 + \frac{1}{2}x^4$ in $\mathbb{Q}[x]$. Find an associate of $a(x)$ in $\mathbb{Z}[x]$ then determine the possible roots for $a(x)$ in $\mathbb{Q}$.

Proof. We proceed by finding a common denominator,

$$\begin{aligned} a(x) &= \frac{1}{3} + x + \frac{2}{3}x^2 + 3x^3 + \frac{1}{2}x^4, \\ &= \frac{2 + 3x + 4x^2 + 18x^3 + 3x^4}{6}, \\ &= \frac{1}{6}\left(2 + 3x + 4x^2 + 18x^3 + 3x^4\right). \end{aligned}$$

We can see that $b(x) = 2 + 3x + 4x^2 + 18x^3 + 3x^4 \in \mathbb{Z}[x]$ is an associate of $a(x)$ with $c = 1/6$. We now apply the rational roots theorem with $b(x)$. Since $a_0 = 2$ and $a_4 = 3$ are both prime, we have $s/t = 2/3$ as the only possible rational root of $a(x)$, and we can see that $a(2/3) \neq 0$, so $a(x)$ has no rational roots.

A quick trip to WolframAlpha shows that the roots of $a(x)$ are $c_1 \doteq -5.8$, $c_2 \doteq -0.44$, and that their exact forms are disgusting looking expressions involing lots of radicals, and are definitely not rational. $\square$

Problem 8.59. Use Eisenstein's Criterion to show that the polynomial $a(x) = \frac{2}{5} + \frac{8}{15}x + \frac{2}{3}x^2 + \frac{4}{5}x^3 + \frac{2}{15}x^4 + \frac{4}{15}x^5 + \frac{1}{3}x^6$ is irreducible over $\mathbb{Q}$.

Proof. Eisenstein's Criterion states that for an integral polynomial $a(x)$ with degree $n > 0$, if a prime number p that divides $a_0, a_1, \dots, a_{n-1}$, but not a_n, and p^2 does not divide a_0, then $a(x)$ is irreducible over $\mathbb{Q}$. We use the common denominator trick to find that $b(x) = 6 + 8x + 10x^2 + 12x^3 + 2x^4 + 4x^5 + 5x^6 \in \mathbb{Z}[x]$ is an associate of $a(x)$. Its fairly obvious that the only prime which satisfies the criterion is $p = 2$, as $b_0, \dots, b_5$ are even, b_6 is odd, and $p^2 \nmid 6$. The fact that $b_4 = 2$ sort of gives this one away. $\square$

Problem 8.66. Use Theorem 8.37 to prove that $a(x) = 56 + 36x + 29x^2 + x^3$ is irreducible over $\mathbb{Q}$.

Proof. Theorem 8.37 states that for a monic integral polynomial $a(x)$ with degree k, if there exists $n > 1$ so that $\bar{f}_n(a(x))$ is irreducible in $\mathbb{Z}_n$, then $a(x)$ is also irreducible in $\mathbb{Z}[x]$. Notice that $a(x)$ is monic, and that $\bar{f}_3(a(x)) = 2 + 2x^2 + x^3$. We have $\bar{f}_3(a(x)) \in \mathbb{Z}[x]$, by the rational roots theorem the only possible root for $\bar{f}_3(a(x))$ is $s/t = 2$, and it is obvious upon inspection that $2 + 2(4) + 8 \neq 0$. Thus by the rational roots theorem $\bar{f}_3(a(x))$ is irreducible over $\mathbb{Q}$, thus it is also irreducible over $\mathbb{Z}_3$. Hence, by Theorem 8.37 with $\bar{f}_3(a(x))$ irreducible over $\mathbb{Z}_3$, we have $a(x)$ is irreducible over $\mathbb{Z}$. By the rational roots theorem, since $a(x)$ is monic, its only rational roots are integers, and since we have shown $a(x)$ is irreducible over $\mathbb{Z}$, we can now claim that it is also irreducible over $\mathbb{Q}$, as desired. $\square$