Algebra II: Tutorial 3

February 26, 2022

Problem 1. Determine whether or not the following polynomials are irreducible over $\mathbb{Q}$:

1. $f(x) = 2x^9 + 12x^4 + 36x^3 + 27x + 6$,
2. $f(x) = x^4 + 25x + 7$.

Solution. 1. It is irreducible by applying Eisenstein's criterion with $p = 3$.
2. By the rational root test, if it has a root over $\mathbb{Q}$, the root is either ± 1 or ± 7. A direct computation shows that none of these are roots of f, and therefore $f(x)$ has no roots in $\mathbb{Q}$. Thus, the only possibility is to factor into two quadratic polynomials. By Gauss's lemma, we can assume that the quadratic polynomials are $x^2 + \alpha x \pm 7$ and $x^2 + \beta x \pm 1$ where $\alpha, \beta \in \mathbb{Z}$. Thus, $\alpha = -\beta$, $\pm(\alpha + 7\beta) = 25$ and $\alpha\beta \pm 8 = 0$, which admits no integral solution. Thus, $f(x)$ is irreducible.

Problem 2. Use Eisenstein's criterion to show that $x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible over $\mathbb{Q}$.

Solution. We can not apply Eisenstein's criterion directly. We first change the variable x to $x + 1$. Then, by noticing that

$$x^{p-1} + x^{p-2} + \cdots + 1 = \frac{x^p - 1}{x - 1},$$

the polynomial becomes

$$\frac{(x+1)^p - 1}{x} = \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-1}x}{x} = x^{p-1} + px^{p-2} + \cdots + p.$$

Recall the fact that these binomial coefficients are divisible by p. Then you can apply Eisenstein's criterion.

Problem 3 (Follow-up question from tutorial 2: ACCPI domains)**.** Let R be an integral domain, and suppose that R satisfies the ACCPI condition. For this question, we will call such rings ACCPI domains.

1. Show that any non-zero element in $R\backslash R^\times$ admits a factorisation into a product of finitely many irreducible elements.

Consider the ring of algebraic integers $\overline{\mathbb{Z}}$.

1. Show that $2^{\frac{1}{2^n}} \in \overline{\mathbb{Z}}$.

2. Show that there are no irreducible elements in $\overline{\mathbb{Z}}$. (Hint: consider the square root of an algebraic integer).

3. Show that, $\forall n \mathbb{N}, (2^{\frac{1}{2^n}}) \subset (2^{\frac{1}{2^{n+1}}})$. Does this chain terminate? Deduce that $\overline{\mathbb{Z}}$ does not have the ACCPI property.

Solution. We show this by contradiction. Suppose there exists a non-zero non-unit element a which does not admit a product into finitely many irreducible elements. In particular, such an element must be reducible, i.e. there exist non-units $a_1, b_1 \in R$ such that $a = a_1 b_1$. In particular, $aR \subset a_1 R$ and $aR \subset b_1 R$. Furthermore, $aR \neq a_1 R$ since a and a_1 are not associates in R (and similarly, $aR \neq b_1 R$). If a_1, b_1 are both irreducible, this contradicts our assumption on a. Therefore, at least one of the two is reducible, say $b_1 = a_2 b_2$, with a_2, b_2 non-zero non-units. Then, $a = a_1 a_2 b_2$, and $aR \subset a_1 a_2 R \subset a_2 R$, with $aR \neq a_1 a_2 R$ (since b_2 non-unit) and $a_1 R \neq a_1 a_2 R$ (again, since a_2 non-unit). Once again, the assumption on a means that one of the three terms a_1, a_2, b_2 must be reducible. By repeating this procedure, we see that, for any $n \in \mathbb{N}$, there exists a chain (under inclusion) of principal ideals all containing aR, of length n, with no two ideals equal. Since $\mathbb{N}$ is unbounded from above, this implies the existence of a chain of principal ideals which does not terminate, contradicting the assumption that R satisfies the ACCPI condition.
2. For $n \in \mathbb{N}$, the element $2^{\frac{1}{2^n}}$ is a root of the monic polynomial $f_n(x) = x^{2^n} - 2$ in $\mathbb{Z}[x]$.
3. Suppose that $\overline{\mathbb{Z}}$ has an irreducible element a. By definition, a is non-zero and a non-unit, and is the root of a monic polynomial $f \in \mathbb{Z}[x]$. Note that the polynomial $f(x^2) \in \mathbb{Z}[x]$ is again monic, with root $a^{\frac{1}{2}}$. Suppose that $a^{\frac{1}{2}}$ is a unit in $\overline{\mathbb{Z}}$. This would imply a is a unit, which is a contradiction. Hence, $a^{\frac{1}{2}}$ is not a unit, and $a = a^{\frac{1}{2}} a^{\frac{1}{2}}$, which shows that a is not irreducible.
4. The fact that $(2^{\frac{1}{2^n}}) \subseteq (2^{\frac{1}{2^{n+1}}})$ is obvious from the fact that $2^{\frac{1}{2^{n+1}}}$ is the square root of $2^{\frac{1}{2^n}}$. The proof of 2. alluded to the fact that if an element a is not a unit and $a = b^2$, then b is not a unit. We know that 2 is not a unit in $\overline{\mathbb{Z}}$ (since $\frac{1}{2}$ is not an algebraic integer), and so by induction, $\forall n \in \mathbb{N}, 2^{\frac{1}{2^n}}$ is not a unit in $\overline{\mathbb{Z}}$. In particular, the equality $\subseteq$ is in fact a proper inclusion. It is clear that such a chain does not terminate, and therefore $\overline{\mathbb{Z}}$ does not have the ACCPI property. By the theorem in the notes characterising UFDs, we deduce that $\overline{\mathbb{Z}}$ is not a UFD.

Problem 4. Let K be a field, and denote by 1 the multiplicative identity in K. Show that the subfield of K generated by $\{1\}$ is the prime subfield of K. Deduce that the

prime subfield of K is $\mathbb{Q}$ (resp. is $\mathbb{F}_p$) if and only if K has characteristic zero (resp. has characteristic p).

Solution. The field generated by $\{1\}$ certainly contains the prime subfield, since the prime subfield is the intersection of all subfields of K. Furthermore, any subfield of K contains 1, and therefore contains the field generated by $\{1\}$. This proves our first claim. On the other hand, the field generated by $\{1\}$ is precisely $\mathbb{Q}$ when K has characteristic zero and $\mathbb{F}_p$ when K has characteristic p. ■