Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 20, 2020

Problems in Section 3.10.

1. Let D be a Euclidean ring, F its field of quotients. Prove the Gauss Lemma for polynomials with coefficients in D factored as products of polynomials with coefficients in F.

Proof. The proof is similar to that of Theorem 3.10.1. □

2. If p is a prime number, prove that the polynomial $x^n - p$ is irreducible over the rationals.

Proof. Apply Eisenstein's criterion. We see that $p \nmid a_n$, $p \mid a_i, i = 1, \cdots n-1$, $p \mid -p = a_0$ but $p^2 \nmid a_0$. Hence, $x^n - p$ is irreducible over the rationals. □

3. Prove that the polynomials $1 + x + \cdots + x^{p-1}$, where p is a prime number, is irreducible over the field of rational numbers.

Proof. Suppose $f(x) = 1 + x + \cdots + x^{p-1}$ was reducible then so does $f(x+1) = 1 + (x + 1) + \cdots + (x+1)^{p-1}$. With some calculations,

$$\begin{aligned} f(x+1) &= 1 + (x+1) + \cdots + (x+1)^{p-1} \\ &= \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{x^p + px^{p-1} + \binom{p}{2}x^{p-2} + \cdots + px}{x} \\ &= x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + p \end{aligned}$$

and by Eisenstein's criterion, $f(x+1)$ is irreducible over rationals. Hence its a contradiction. Therefore, $f(x) = 1 + x + \cdots + x^{p-1}$ is irreducible over rationals. □

4. If m and n are relatively prime integers and if

$$\left(x - \frac{m}{n}\right) \mid (a_0 + a_1 x + \cdots + a_r x^r),$$

where the a's are integers, prove that $m \mid a_0$ and $n \mid a_r$.

Proof. Let $f(x) = a_0 + a_1 x + \cdots + a_r x^r$. Then there exists $g(x) = b_0 + b_1 x + \cdots + b_{r-1} x^{r-1}$ such that

$$\begin{aligned}
&\left(x - \frac{m}{n}\right) g(x) = f(x) \\
&\iff \left(x - \frac{m}{n}\right)(b_0 + b_1 x + \cdots + b_{r-1} x^{r-1}) = a_0 + a_1 x + \cdots a_r x^r \\
&\iff -\frac{m}{n} b_0 + \left(b_0 - \frac{m}{n} b_1\right) x + \cdots + \left(b_{r-2} - \frac{m}{n} b_{r-1}\right) x^{r-1} + b_{r-1} x^r \\
&\qquad = a_0 + a_1 x + \cdots a_{r-1} x^{r-1} + a_r x^r \\
&\implies -\frac{m}{n} b_0 = a_0, \quad a_r = \frac{n}{m}(b_{r-2} - a_{r-1}) \\
&\implies n a_0 = -m b_0, \quad m a_r = n(b_{r-2} - a_{r-1})
\end{aligned}$$

so that $m \mid n a_0$ and $n \mid m a_r$. Since $(m, n) = 1$, $m \mid a_0$ and $n \mid a_r$. □

5. If a is rational and $x - a$ divides an integer monic polynomial, prove that a must be an integer.

Proof. We use the result of Problem 4. We can assume that $a = m/n$, where $(m, n) = 1$. As given polynomial is integer monic and n divides the coefficient of largest degree, that is, 1, $n \mid 1$ and hence $a = \pm m \in \mathbb{Z}$. Therefore, a is an integer. □