Field Theory HW
Ali Nesin
October 19, 2008

1. Let K be any field and $n, m \in \mathbb{N} \setminus \{0\}$. Show that the polynomial $X^m - 1$ divides $X^n - 1$ in $K[X]$ iff m divides n in $\mathbb{Z}$.

2. Find a relationship between the irreducible polynomials of $\mathbb{Z}[X]$ and the irreducible polynomials of $\mathbb{Q}[X]$.

3. Show that there is an algorithm that decides whether or not a polynomial in $\mathbb{Z}[X]$ is irreducible.

4. Let R be a commutative ring.

4a. Let $a \in R^*$ and $b \in R$. Show that the map $\varphi_{a,b}(f(X)) = f(aX + b)$ is a ring automorphism of $R[X]$ which is identity on R, i.e. $\varphi_{a,b} \in \mathrm{Aut}_R(R[X], +, .)$.

4b. Show that the set of all such automorphisms is a group isomorphic to $R^+ \rtimes R^*$ (under composition of course).

4c. Show that $\mathrm{Aut}_R(R[X], +, .) = \{\varphi_{a,b} : a \in R^* \text{ and } b \in R\}$.

5. Let $p \in \mathbb{Z}$ be a prime, $f, g, h \in \mathbb{Z}[X]$ and $n \in \mathbb{N}$ be such that $gh = X^n + pf$.

5a. Show that p divides $f(0)$ in $\mathbb{Z}$. (Hint: Work modulo p. This is Einsenstein's Criterion)

5b. Conclude that the polynomial $X^{p-1} + X^{p-2} + ... + X + 1$ is irreducible over $\mathbb{Q}$ and over $\mathbb{Z}$. (Hint: Make change of variable: $Y = X - 1$ and use #4 and #2).

6. Let n be a positive integer, d a divisor of n and ζ_d a primitive d^{th} root of unity.

6a. Show that the map φ_d from $\mathbb{Q}[X]/\langle X^n - 1\rangle$ into $\mathbb{Q}[\zeta_d]$ defined by $\varphi_d(\underline{f(X)}) = f(\zeta_d)$ is well-defined.

6b. Show that the map $\varphi = \oplus_{d|n}\varphi_d$ from $\mathbb{Q}[X]/\langle X^n - 1\rangle$ into $\oplus_{d|n}\mathbb{Q}[\zeta_d]$ defined by

$$\varphi(\underline{f}) = (\oplus_{d|n}\varphi_d)(\underline{f}) = (\varphi_d(\underline{f}))_{d|n}$$

is well-defined and an isomorphism of $\mathbb{Q}$-algebras.

6c. Show that $\varphi(\mathbb{Z}[X]/\langle X^n - 1\rangle) \le \oplus_{d|n}\mathbb{Z}[\zeta_d]$, but that the equality almost never arises.