PURDUE UNIVERSITY
Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 2 (Jan 23 – Jan 31).

1 (20+20) For each of the following pairs of polynomials f and g:
(i) find the quotient and remainder on dividing f by g;
(ii) use the Euclidean Algorithm to find $gcd(f, g)$;
(iii) find polynomials a and b with the property that $gcd(f, g) = af + bg$.

a) $f = t^3 + 4t^2 + t - 2$, $g = t + 1$ over $\mathbb{Z}$.
b) $f = t^7 - 3t^6 + t + 4$, $g = 2t^3 + 1$ over $\mathbb{F}_5$.

2 (5+15) 1) Prove that $f(t) = t^3 + t^2 + 1$ is irreducible in $\mathbb{Q}[t]$.
2) Suppose that $\alpha \in \mathbb{C}$ is a root of f. Express α^{-1} and $(\alpha + 2)^{-1}$ as linear combinations, with rational coefficients, of $1, \alpha, \alpha^2$.

3 (5+10+5+10) 1) Let $p > 2$ be a prime number and consider $P(x) = x^4 + 2ax^2 + b^2$, where $a, b \in \mathbb{Z}$. Show that

$$P(x) = (x^2 + a)^2 - (a^2 - b^2) = (x^2 + b)^2 - (2b - 2a)x^2 = (x^2 - b)^2 - (-2a - 2b)x^2 .$$

2) Noticing $(2b-2a)(-2a-2b) = 4(a^2-b^2)$, derive that one of the numbers $(a^2-b^2), (2b-2a), (-2a-2b)$ is a square modulo p.
3) Prove that $P(x) = x^4 + 2ax^2 + b^2$, $a, b \in \mathbb{Z}$ is reducible over $\mathbb{F}_p[x]$ for any prime p.
4) Prove that $f(x) = x^4 + 1$ is irreducible over $\mathbb{Z}$ but reducible over $\mathbb{F}_p$ for any prime p.

4 (10+10) 1) Prove that $\mathbb{C}$ is isomorphic to the set of matrices $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, where $a, b \in \mathbb{R}$.

2) Given a matrix A denote by $\exp A$ the matrix $I + \frac{A}{1!} + \frac{A^2}{2!} + \dots$. Using the isomorphism above and the Euler formula,

prove that

$$\exp \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} e^a \cos b & -e^a \sin b \\ e^a \sin b & e^a \cos b \end{pmatrix}.$$

5 (5+5+10) 1) Let $[L : K] < \infty$ be a finite extension. Prove that $L : K$ is an algebraic extension, that is any $\alpha \in L$ is algebraic over K.

2) Let $\alpha \in L/K$ and $[L : K] < \infty$. Then $K[\alpha] = K(\alpha)$.

3) Suppose that $L : K$ is an extension and any $\alpha \in L$ is algebraic. Is it true that $[L : K] < \infty$?