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 $[L:K] < \infty$?

Solutions

General remark. If there is a typo in any task, then the maximum score will be awarded for that task.

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 $\mathbb{F}_5$.

Solution: (a, i) The quotient is $t^2 + 3t - 2$ and the remainder is zero.
(a, ii) $f = g \cdot (t^2 + 3t - 2)$ and hence $gcd(f, g) = g$.
(a, iii) Take $a = 0$ and $b = 1$. Then $gcd(f, g) = g = 0 \cdot f + 1 \cdot g$.

(b, i) The quotient is $3t^4 - 4t^3 - 4t + 2$ and the remainder is 2.
(b, ii) We have $f = (3t^4 - 4t^3 - 4t + 2)g + 2$ and hence $gcd(f, g) = 2$ (or any other non–zero element of $\mathbb{F}_5$).
(b, iii) We have $f - (3t^4 - 4t^3 - 4t + 2)g = 2$. Take $a = 1$ and $b = -(3t^4 - 4t^3 - 4t + 2) = 2t^4 - t^3 - t - 2$.

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 $1, \alpha, \alpha^2$.

Solution: 1) In the lecture we showed that f is irreducible in $\mathbb{F}_2[t]$ and, therefore, in $\mathbb{Q}[t]$.

2) We have $\alpha^3 + \alpha^2 + 1 = 0$ and hence $\alpha^{-1} = -\alpha - \alpha^2$. Further by the Euclidean algorithm, we have $t^3 + t^2 + 1 = (t^2 - t)(t+2) + 2t + 1$ and hence $t^3 + t^2 + 1 = (t^2 - t)(t+2) + 2(t+2) - 3$. Substituting α, we obtain $0 = (\alpha+2)(\alpha^2 - \alpha + 2) - 3$. Hence $(\alpha + 2)^{-1} = (\alpha^2 - \alpha + 2)/3$.

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.

Solution: 1) This is a direct calculation.
2) The set of squares R in $\mathbb{F}_p$ is a subgroup of index two. Therefore, if $(2b - 2a), (-2a - 2b) \notin R$, then the product $4(a^2 - b^2)$ belongs to R. Hence $(a^2 - b^2) \in R$.
3) For $p = 2$ the polynomials x^4, $x^4 + 1 = (x + 1)^4$ are reducible. For $p > 2$ use the previous computations.
4) It is enough to show that $f(x)$ is irreducible over $\mathbb{Z}$. It has roots $(\pm 1 \pm i)/2$ and if $f(x) = g(x)h(x)$, where $g, h \in \mathbb{R}[x]$, then $g(x), h(x) = x^2 \pm \sqrt{2}x + 1$ (consider complex conjugation). But g, h do not belong $\mathbb{Z}[x]$.

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 $I + \frac{A}{1!} + \frac{A^2}{2!} + \ldots$. Using the isomorphism above and the Euler formula, prove that

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

Solution: 1) Let $\mathcal{M}$ be the set of our matrices. Consider the map $\varphi : \mathcal{M} \to \mathbb{C}$, namely, for $m \in \mathcal{M}$ one has $\varphi(m) = a + bi$. Clearly, $\varphi(I) = 1$ and $\varphi(m + m_*) = \varphi(m) + \varphi(m_*)$. We have

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} a_* & -b_* \\ b_* & a_* \end{pmatrix} = \begin{pmatrix} aa_* - bb_* & -(ba_* + ab_*) \\ ba_* + ab_* & aa_* - bb_* \end{pmatrix},$$

and

$$(a + ib)(a_* + ib_*) = (aa_* - bb_*) + i(ba_* + ab_*)$$

and hence φ preserves the multiplication. Finally, $\mathrm{Ker}(\varphi) = 0$. Thus φ is an isomorphism.

2) Thanks to the Euler formula one has (the convergence is obvious)

$$\exp \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \varphi^{-1}\varphi\left(\exp \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\right) = \varphi^{-1}(e^{a+ib}) = \varphi^{-1}(e^a(\cos b + i \sin b)) = \begin{pmatrix} e^a \cos b & -e^a \sin b \\ e^a \sin b & e^a \cos b \end{pmatrix}.$$

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 $[L : K] < \infty$?

Solution: 1) Consider $1, \alpha, \alpha^2, \dots$. Since $[L : K] < \infty$ it follows that these numbers are dependent over K. Hence there is $f \in K[t]$ such that $f(\alpha) = 0$ and therefore α is algebraic.

2) As we have seen α is algebraic and hence we know that $K[\alpha] = K(\alpha)$ (see lectures).

3) No. Take $K = \mathbb{Q}$ and let $L = \mathbb{A}$ be the field of all algebraic numbers. Then, clearly, $[L : K] = \infty$.