PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 1 (Jan 16 – Jan 24).

1 (10+10) 1) Using Vieta's trigonometric method, solve $x^3 - 3x + 1 = 0$.
2) Applying the cube of sum formula, solve $x^3 - 3 \cdot 2^{1/3} x - 3 = 0$.

2 (10) Let x_1, x_2, x_3 be the roots of the cubic $x^3 + ax^2 + bx + c = 0$. Compute $x_1^2 + x_2^2 + x_3^2 + x_1^{-1} + x_2^{-1} + x_3^{-1}$.

3 (10) Prove that the stabilizer of the polynomial $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$ is D_5, that is the subgroup of permutations $g \in S_5$ of the form $g : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ and $gx = \pm x + b$, where $b \in \mathbb{Z}/5\mathbb{Z}$.

4 (5+5) Let $H \le S_n$ be a subgroup and K be a field. Take any $f \in K[x_1, \dots, x_n]$ and form

$$F = F(f) = \sum_{h \in H} f(x_{h(1)}, \dots, x_{h(n)}) := \sum_{h \in H} h \cdot f \,,$$

where $h \cdot f$ and the natural action of S_n on $K[x_1, \dots, x_n]$ (i.e. $(h \cdot f)(x_1, \dots, x_n) := f(x_{h(1)}, \dots, x_{h(n)})$).
1) Prove that for any $h \in H$ one has $h \cdot F = F$.
2) Take $f = x_1 x_2^2 \dots x_n^n$ and prove that $h \cdot F = F$ iff $h \in H$.
3) *(for enthusiasts, does not affect the rating)* Is the second part true for any f?

5 (5+5+15) A complex polynomial $f(x_1, \dots, x_n)$ is called *skew–symmetric* if $h \cdot f = -f$ for any transposition h.
1) Prove that the ratio of any skew–symmetric polynomials is a symmetric rational function.
2) Let $D = D(x_1, \dots, x_n) = \prod_{i<j}(x_i - x_j)^2$ be the discriminant and $\Delta = \Delta(x_1, \dots, x_n) = \prod_{i<j}(x_i - x_j)$, $\Delta^2 = D$. Prove that Δ is a skew–symmetric polynomial.
3) Prove that any symmetric polynomial f is a product of Δ and another symmetric polynomial g.

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

prove that

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

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 $[L:K] < \infty$?

PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 3 (Jan 31 – Feb 13).

1 (5+10+15) 1) Show that $t^3 + t + 1$ is irreducible in $\mathbb{F}_2[t]$.

2) Consider the quotient ring $L := \mathbb{F}_2[t]/(t^3 + t + 1)$ and compute its size.

3) Take $g = t + 1$ and prove that the set $\{0, g, g^2, \dots, g^7\}$ coincides with L.

2 (15) Let K be a field and $p, q \in K[t]$ be irreducible polynomials over K, $(p) \neq (q)$ (this is equivalent to the statement that p is coprime to q). Consider the field $\mathbb{F} := K(t)$ and the polynomial $g(x) = x^n + px + pq \in \mathbb{F}[x]$. Prove that g is irreducible over $\mathbb{F}$.

3 (10) Prove that $t^2 - 7$ is irreducible over $\mathbb{Q}(\sqrt{5})$.

4 (5+5+5+10+20) 1) Let $\alpha = 2^{1/6}$ and $\varepsilon_3^3 = 1$, $\varepsilon_3 \neq 1$. Find the minimal polynomials of α over

a) $\mathbb{Q}$ b) $\mathbb{Q}(\alpha)$ c) $\mathbb{Q}(\alpha^2)$ d) $\mathbb{Q}(\alpha\varepsilon_3)$.

2) In each case (a—d), find the conjugate elements of all roots of $x^6 - 2$.

5 Midterm exam is next Thursday!

PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 4 (Feb 13 – Feb 21)

1 (5+5+15+20) For each of the following polynomials, construct a splitting field L over $\mathbb{Q}$ and compute the degree $[L : \mathbb{Q}]$.

1) $t^4 + 7t^2 + 12$
2) $t^4 + t^2 - 12$
3) $t^{2n} - 2^n$, where $n = 3, 4$.
4) $t^{14} - 1$.

2 (15) Let $K - L - M$ be a field extension and $K - L$, $L - M$ are algebraic extensions. Prove that $K - M$ is also an algebraic extension.

3 (15) Let α be transcendental over a field $K \subset \mathbb{C}$. Show that $K(\alpha)$ is not algebraically closed (hint: consider the polynomial $t^2 - \alpha$).

4 (15) Let $L : K$ be a splitting field extension for a non–constant polynomial $f \in K[t]$. Prove that $[L : K]$ divides $(\deg f)!$ (hint: at the very end look at some binomial coefficients).

PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 5 (Feb 21 – Feb 28)

1 (5+5+5+10+15) Which of the following field extensions are normal? Justify your answers.

1) $\mathbb{Q}(i) : \mathbb{Q}$
2) $\mathbb{Q}(2^{1/4}) : \mathbb{Q}$
3) $\mathbb{Q}(2^{1/4}, i) : \mathbb{Q}$
4) $\mathbb{Q}(2^{1/4}, i, \sqrt{5}) : \mathbb{Q}$
5) $\mathbb{Q}(3^{1/3}, i, \sqrt{3}) : \mathbb{Q}$.

2 (15) Let $\psi : L \to M$ be a homomorphism, suppose that L is algebraically closed. Prove that $\psi(L)$ is algebraically closed.

3 (20) Let $L : K$ be a field extension. Then $\overline{K}$ is isomorphic to $\overline{L}$. In addition, if $K \subset L \subseteq \overline{L}$, then $\overline{K} = \overline{L}$.

4 (15) Let $K - L$ be a normal extension, $K \subseteq L \subseteq \overline{K}$. Then for any K–homomorphism $\tau : L \to \overline{K}$ one has $\tau(L) = L$.

5 (25) Put $K = \mathbb{F}_2(t)$ and consider $L = K(t^{1/3})$. Prove that the extension $L : K$ is algebraic but not normal.

PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 6 (Feb 28 – Mar 7)

1 (5+10+10) Find Galois groups for the following polynomials f over $\mathbb{Q}$:
1) $(t^2-3)(t^2+1)$
2) t^4-t^2+1
3) t^4-2

2 (10+10) 1) Find $\mathrm{Gal}_{\mathbb{F}_3(t^2)}(\mathbb{F}_3(t))$.
2) Find $\mathrm{Gal}_{\mathbb{F}_2(t^2)}(\mathbb{F}_2(t))$.

3 (10+5) (a) Let $K-M-L$ be a field extension and $L:K$ is a normal extension. Prove that $L:M$ is also a normal extension.
(b) Give an example of three fields K, M, L such that $[L:K]=4$ and $[M:K]=[L:M]=2$ (hence $K-M$ and $M-L$ are normal extensions) but $L:K$ is not a normal extension.

4 (10) Let $L:K$ be a splitting field extension for a non–constant polynomial $f \in K[t]$. Prove that $|\mathrm{Gal}_L(K)|$ divides $(\deg f)!$.

5 (15+20) $a)$ Let $f=t^3+t+1 \in \mathbb{F}_2[t]$. Prove that $\mathrm{Gal}_{\mathbb{F}_2}(f)$ is isomorphic to $\mathbb{Z}_3$.
$b)$ Let $f=t^3+t^2+1 \in \mathbb{F}_2[t]$. Prove that $\mathrm{Gal}_{\mathbb{F}_2}(f)$ is isomorphic to S_3.

PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 7 (Mar 7 – Mar 14)

1 (10) Let $K = \mathbb{Q}$, $M = \mathbb{Q}(2^{1/3})$ and $L = \mathbb{Q}(2^{1/3}, \sqrt{3}, i)$. Prove that $L : K$ and $L : M$ are normal but $M : K$ is not normal.

2 (10+5) *a*) Let $K - L$ be algebraic, $\alpha \in L$ and $\sigma : K \to \overline{K}$ be a homomorphism. Prove that μ_α^K is separable over K iff $\sigma(\mu_\alpha^K)$ is separable over $\sigma(K)$.

b) Let $L : K$ be a splitting filed for $f \in K[t]$. Prove that if f is separable, then $L : K$ is separable.

3 (10) Let $L : K$ be a splitting field extension for a polynomial $f \in K[t]$. Then $L : K$ is separable iff f is separable over K.

4 (15) Let $K - M - L$ be an algebraic extension. Prove that $K - L$ is separable iff $K - M$ and $M - L$ are separable.

PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 8 (Mar 14 – Apr 4)

1 (5+5+5) Let $K \subseteq L$ be a splitting field extension for some $f \in K[t] \setminus K$. Then the following are equivalent:
(i) f has a repeated root over L;
(ii) $\exists \alpha \in L$ s.t. $0 = f(\alpha) = (\mathcal{D}f)(\alpha)$;
(iii) $\exists g \in K[t]$, $\deg g \geq 1$ s.t. g divides both f and $\mathcal{D}f$.

2 (5) Let K be a field, $\mathrm{char}(K) = p > 0$ and $f \in K[t^p]$ is an irreducible polynomial over K. Prove that f is inseparable.

3 (10) Let K be a field, $\mathrm{char}(K) = p > 0$ and $f \in K[t^p]$ is an irreducible polynomial over K. Prove that there is $g \in K[t]$ and a non-negative n such that $f(t) = g(t^{p^n})$ and g is an irreducible and separable polynomial.

4 (10) Prove that $\prod_{\alpha \in \mathbb{F}_q^*} \alpha = -1$.

5 (5+5+5+5) a) Let $\alpha \in \mathbb{F}_q$ and $\alpha = \beta - \beta^p$ for some $\beta \in \mathbb{F}_q$. Prove that $\mathrm{Tr}(\alpha) = 0$.

b) Let $\alpha \in \mathbb{F}_q$ and $\alpha = \gamma^{1-p}$ for some nonzero $\gamma \in \mathbb{F}_q$. Prove that $\mathrm{Norm}(\alpha) = 1$.

c) Let $\alpha \in \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$. Prove that $\mathrm{Tr}(\alpha) = n\alpha$.

d) Let $\alpha \in \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$. Prove that $\mathrm{Norm}(\alpha) = \alpha^n$.

6 The midterm exam will be on Thursday the 27th!

PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 9 (Apr 4 – Apr 11)

1 (10+5) *a*) Let L be the splitting field of the polynomial $t^{13}-1$. Find all subgroups of $\mathrm{Gal}_{\mathbb{Q}}(L)$.
b) How many intermediate subfields are there in the extension $L:\mathbb{Q}$?

2 (10) Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{F}_3}(\mathbb{F}_{3^8})$. Find orders of all subgroups of $\mathrm{Gal}_{\mathbb{F}_3}(\mathbb{F}_{3^8})$.

3 (10) Prove Artin's theorem: let $[L:K]<\infty$, $G:=\mathrm{Gal}_K(L)$. Then $[L:L^G]$ is a Galois extension.

4 (10) Let $L:K$ be a finite Galois extension, $G:=\mathrm{Gal}_K(L)$. For any $\alpha\in L$ define

$$\mathrm{Tr}(\alpha)=\sum_{g\in G} g(\alpha) \qquad \text{and} \qquad \mathrm{Norm}(\alpha)=\prod_{g\in G} g(\alpha)\,.$$

Prove that for an arbitrary $\alpha\in L$ one has $\mathrm{Tr}(\alpha),\mathrm{Norm}(\alpha)\in K$.

5 (15+15) *a*) Find all of the subfields of $\mathbb{Q}(2^{1/3},e^{2\pi i/3})$.
b) Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(2^{1/3},e^{2\pi i/3}))$.

PURDUE UNIVERSITY
Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 10 (Apr 11 – Apr 18)

1 (10+10+5+5) Let $K, E, F \subseteq L$ be fields, $E : K$, $F : K$ be finite extensions. Prove:

a) if $E : K$ is separable, then $EF : F$ is separable;

b) if $E : K$ and $F : K$ are both separable, then $EF : K$ and $E \cap F : K$ are both separable;

c) if $E : K$ is Galois, then $EF : F$ is Galois;

d) if $E : K$ and $F : K$ are both Galois, then $EF : K$ and $E \cap F : K$ are both Galois.

2 (5+5+10) *a*) Find the splitting field L of the polynomial $f(t) = t^4 - 4t^2 + 5$.

b) Prove that $[L : \mathbb{Q}]$ is either 4 or 8.

c) Find 10 intermediate fields of the extension $L : \mathbb{Q}$ and their degrees.

d) (for enthusiasts) Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{Q}}(f)$.

3 (30) Draw the lattice of subfields and corresponding lattice of subgroups of $\mathrm{Gal}_{\mathbb{Q}}(t^6 + 3)$. *Hint*: Use the calculations (and the notation, if you like) from Lecture 18.

PURDUE UNIVERSITY

Department of Mathematics

GALOIS THEORY HONORS, MA 45401

Homework 11 (Apr 18 – Apr 25)

1 (5) Let $G = \mathbb{Z}/p^n\mathbb{Z}$, where p is a prime number. Construct a subnormal series G_j of subgroups of G such that $|G_{j-1}/G_j| = p$.

2 (5+5) *a*) Let G be a group. Prove that G' is a normal subgroup of G such that G/G' is abelian.
b) Prove that if N is any normal subgroup of G such that G/N is abelian, then $G' \leq N$.

3 (10) Let $\mathbb{F}$ be a field and

$$H := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \ : \ a, b, c \in \mathbb{F} \right\} \tag{1}$$

be the Heisenberg group. Prove that H is soluble.

4 (15) Prove that A_n, $n \geq 3$ is generated by 3–cycles.

5 (5+5+5) Let G be a group. Find G' for
a) $G = S_3$ *b*) $G = A_4$ *c*) $G = S_4$ (use the previous question).