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!

Solutions

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

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 $\{0, g, g^2, \ldots, g^7\}$ coincides with L.

Solution. 1) It was done in lectures.

2) We know (see lectures) that L is a field and moreover $L = \{a + bt + ct^2 \ : \ a, b, c \in \mathbb{F}_2\}$. Thus $|L| = 8$.

3) We have $g^2 = (t+1)^2 = t^2+1$ and $g^3 = t^3+3t^2+3t+1 = t^3+t^2+t+1 = t^2$, since we work in L. Thus $g^4 = t^3+t^2 = t^2+t+1$, $g^5 = t^3+1 = t$ and so on. Another argument: we can consider the set $L\setminus\{0\}$ as a (multiplicative) group and thus by Lagrange's theorem we know that the order of any element divides $|L \setminus \{0\}| = |L| - 1 = 7$. Since $g \neq 1$ and 7 is a prime number, it follows that $\{g, g^2, \ldots, g^7\} = L \setminus \{0\}$.

2 (15) Let K be a field and $p, q \in K[t]$ be irreducible polynomials over K, $(p) \neq (q)$. 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 $\mathbb{F}$.

Solution. The leading coefficient of g is not divisible by p, but all other coefficients are. Finally, pq is not divisible by p^2 (recall that q is an irreducible polynomial over K). Thus by Eisenstein's criterion and Gauss' lemma the polynomial g is irreducible over $\mathbb{F}$.

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

Solution. We need to check that the equation $(a + b\sqrt{5})^2 = 7$, where $a, b \in \mathbb{Q}$ has no solutions. One has $a^2 + 5b^2 + 2ab\sqrt{5} = 7$ and hence $ab = 0$ and $a^2 + 5b^2 = 7$. Thus either $a = 0$ or $b = 0$. If $a = 0$, then $b \notin \mathbb{Q}$ and vice versa. Thus, $t^2 - 7$ is irreducible.

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 $x^6 - 2$.

Solution. 1) The polynomial

$$x^6 - 2 = (x-\alpha)(x+\alpha)(x-\varepsilon_3\alpha)(x+\varepsilon_3\alpha)(x-\varepsilon_3^2\alpha)(x+\varepsilon_3^2\alpha)$$

is irreducible over $\mathbb{Q}$ by the Eisenstein criterion. Over $\mathbb{Q}(\alpha)$ the minimal polynomial of α is just $x - \alpha$, over $\mathbb{Q}(\alpha^2)$ it is $x^2 - \alpha^2$. Now thanks to $1 + \varepsilon_3 + \varepsilon_3^2 = 0$, we obtain

$$(x-\alpha)(x-\varepsilon_3^2\alpha) = x^2 - x\alpha(1+\varepsilon_3^2) + \alpha^2\varepsilon_3^2 = x^2 + x\alpha\varepsilon_3 + (\alpha\varepsilon_3)^2 \in \mathbb{Q}(\alpha\varepsilon_3) \qquad (1)$$

and it gives us the minimal polynomial of α over $\mathbb{Q}(\alpha\varepsilon_3)$.

2) (a) In this case we obviously have 6 conjugated elements $\{\pm\alpha, \pm\varepsilon_3\alpha, \pm\varepsilon_3^2\alpha\}$.

(b) Now $\{\alpha\}$, $\{-\alpha\}$ are conjugated to itself. Further

$$(x-\varepsilon_3\alpha)(x+\varepsilon_3\alpha)(x-\varepsilon_3^2\alpha)(x+\varepsilon_3^2\alpha) = (x^2 - \varepsilon_3^2\alpha^2) = (x^2 - \varepsilon_3\alpha^2) = x^4 + \alpha^2x^2 + \alpha^4 \in \mathbb{Q}[\alpha^2] \subset \mathbb{Q}[\alpha] \qquad (2)$$

and hence $\{\pm\varepsilon_3\alpha, \pm\varepsilon_3^2\alpha\}$ are conjugated to each other.

(c) It follows from part (a) and (2) that $\{\alpha, -\alpha\}$ and $\{\pm\varepsilon_3\alpha, \pm\varepsilon_3^2\alpha\}$ are two classes of conjugated elements.

(d) Finally, from (1) we see that $\{\alpha, \varepsilon_3^2\alpha\}$ and, similarly, $\{\alpha, \varepsilon_3\alpha\}$ are two conjugated pairs over $\mathbb{Q}(\varepsilon_3\alpha)$. The same computation but with minus gives us that $\{-\alpha, -\varepsilon_3^2\alpha\}$ and, similarly, $\{-\alpha, -\varepsilon_3\alpha\}$ are other two conjugated pairs over $\mathbb{Q}(\varepsilon_3\alpha)$.

5 Midterm exam is next Thursday!