NEPAL ALGEBRA PROJECT 2017
MODULE 2 — HOMEWORK #2: SOLUTIONS
WEDNESDAY, 31 MAY, 2017

ROGER AND SYLVIA WIEGAND

1. Let F be a finite field. Prove that $|F|$ is a power of p.

The prime subfield k has p elements, and F is a vector space over k. If F has dimension d over k, then, as a vector space, $F \cong \mathsf{k}^d$, which has p^d elements.

2. Let $f(X) = X^5 - 3$, and let $\zeta = e^{\frac{2\pi \mathrm{i}}{5}}$.
   (a) Show that ζ is a root of $g(X) = X^4 + X^3 + X^2 + X + 1$.

   ζ is a root of $X^5 - 1 = (X-1)g(X)$, so $(\zeta - 1)g(\zeta) = 0$. Since $\zeta - 1 \neq 0$ it follows that $g(\zeta) = 0$.

   (b) Prove that $g(X)$ is irreducible in $\mathbb{Q}[X]$. (Hint: First prove that $g(X+1)$ is irreducible.)

   Since $g(X) = \frac{X^5-1}{X-1}$, we have $g(X) = \frac{(X+1)^5-1}{X} = X^4 + 5X^3 + 10X^2 + 10X + 5$. This is irreducible, by Eisenstein. If $g(X) = p(X)q(X)$, with neither p nor q constant, we would have $g(X+1) = p(X+1)q(X+1)$, contradiction.

   (c) Show that $E = \mathbb{Q}(\sqrt[5]{3}), \zeta)$ is the splitting field of $f(X)$ over $\mathbb{Q}$.

   The roots of $f(X)$ are $\alpha = \sqrt[5]{3}$, $\zeta^{\pm 1}\alpha$, $\zeta^{\pm 2}\alpha$, and clearly $\mathbb{Q}(\sqrt[5]{3}) = \mathbb{Q}(\alpha,\ \zeta^{\pm 1}\alpha,\ \zeta^{\pm 2}\alpha)$.
   (d) Describe $\mathrm{Aut}(E/\mathbb{Q}(\zeta))$.
   (e) Describe $\mathrm{Aut}(E/\mathbb{Q}(\sqrt[5]{3}))$.
   (f) What is $|\operatorname{Aut} E|$?

Since E contains both $\mathbb{Q}(\zeta)$ and $\mathbb{Q}(\alpha)$, which have degrees 4 and 5 over $\mathbb{Q}$, $[E : \mathbb{Q}]$ must be a common multiple of 4 and 5 and hence a multiple of 20. But since ζ has degree at most 4 over $\mathbb{Q}(\alpha)$ it follows that $[E : \mathbb{Q}] = 20$. We know $E/\mathbb{Q}$ is Galois, being the splitting field of a separable polynomial. Therefore $|\operatorname{Aut}(E/\mathbb{Q})| = [E : \mathbb{Q}]$. This answers (f).

(d) Since $E/\mathbb{Q}(\zeta)$ is Galois, the order of the group is 5; therefore the group must be cyclic. An automorphism is determined by what it does to α, and α can be sent to any of the roots. Therefore $\mathrm{Aut}(E/\mathbb{Q}(\zeta))$ is generated by the automorphism $\alpha \mapsto \zeta\alpha$ (for example).

(e) The order of the group is 4, since the extension is Galois. An automorphism is determined by what it does to ζ, and ζ can be sent to any of the roots $\zeta^{\pm 1}$, $\zeta^{\pm 2}$ The map $\zeta \mapsto \zeta^2$ does this: $\zeta \mapsto \zeta^2 \mapsto \zeta^{-1} \mapsto \zeta^{-2} \mapsto \zeta$, so it has order 4. Thus the group is cyclic.

3. Let $\alpha \in \mathbb{C}$ be a root of $f(X) = X^3 - 3X - 1$. Prove that $\sqrt{2} \notin \mathbb{Q}(\alpha)$.

Since neither 1 nor -1 is a root of $f(X)$, there are no rational roots, and since the degree is 3 we know $f(X)$ is irreducible over $\mathbb{Q}$. Therefore $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $2 \nmid 3$, $\sqrt{2} \notin \mathbb{Q}(\alpha)$.

4. Let $\alpha = \sqrt{3 + 2\sqrt{2}} \in \mathbb{C}$.
   (a) Find the minimal polynomial $f(X)$ of α over $\mathbb{Q}$.

   Well, I wasted a lot of time trying to show that α has degree 4. But in fact $\alpha = 1 + \sqrt{2}$. So the minimal polynomial is $X^2 - 2X - 1$. Funny, huh?

   (b) Find the splitting field E of $f(X)$ over $\mathbb{Q}$.

   $\mathbb{Q}(\alpha)$.

   (c) Describe the group $\mathrm{Aut}(E/\mathbb{Q})$.

   It's cyclic of order 2 generated by $\alpha \mapsto 1 - \sqrt{2}$.

5. Describe the field $\mathbb{F}_2[X]/(X^2 + X + 1)$ by giving
   (a) a list of elements,
   (b) the addition table, and
   (c) the multiplication table.

Let x denote the coset of X. The field has four elements: $0, 1, x, x+1$ The addition table is trivial: Just use the relation $2 = 0$. For multiplication, use the rule $x^2 = x + 1$, and the rest falls out. (I'm too lazy to build tables in LaTeX, so I will settle for 75% credit on this problem.)

6. Find the splitting field E of $f(X) = X^4 + X^2 + 1$ over $\mathbb{Q}$, and describe the group $\mathrm{Aut}(E/\mathbb{Q})$.

See the solution to Problem #8 on Module 2, Homework set 1. The roots are $\zeta^{\pm 1}$ and $\zeta^{\pm 2}$, where ζ is a primitive 6^{th} root of unity. The splitting field is $\mathbb{Q}(\zeta)$, since this contains all the roots. The degree $[E : \mathbb{Q}]$ is 2, since the minimal polynomial of ζ over $\mathbb{Q}$ is $X^2 - X + 1$. [How, you ask, can a polynomial of degree 2 have four roots? It doesn't: $\zeta^{\pm 1}$ are the roots of $X^2 - X + 1$ and $\zeta^{\pm 2}$ are the roots of $X^2 + X - 1$. Note that $f(X)$ is the product of these two polynomials.] Anyway, the automorphism is cyclic of order 2, generated by $\zeta \mapsto \zeta^{-1}$.

7. (This is essentially Milne Exercise 4-4 (page 57).) Find an extension $E/\mathbb{Q}$ of degree 4 such that there does not exist a proper intermediate field $\mathbb{Q} \subset F \subset E$. For this problem you may use the following results (which are true, by the way) without proving them:
   (A) There exists a polynomial $f(X) \in \mathbb{Q}[X]$ of degree 4 whose splitting field has degree 24 over $\mathbb{Q}$.
   (B) The group A_4 consisting of even permutations of $\{1, 2, 3, 4\}$ is the only subgroup of order 12 in S_4.

First we observe that $f(X)$ must be irreducible over Q. For it $f(X)$ had a linear factor then the splitting field would be of degree at most $3! = 6$, and if it were the product of two quadratics, the degree of the splitting field would be at most 4. In particular, $f(X)$ is separable, since irreducible polynomials are always separable over a field of characteristic 0. Now, when we think of the Galois group G as permutations of the roots, we see that the G is the full symmetric group S_4.

Let r_1, r_2, r_3, r_4 be the roots of $f(X)$ in the splitting field K over $\mathbb{Q}$. Let H be the subgroup of G consisting of automorphism that fix r_4. Then H consists of all permutations of r_1, r_2, r_3 and in particular contains the transposition $r_1 \mapsto r_2 \mapsto r_1$, $r_3 \mapsto r_3$, $r_4 \mapsto r_4$. Transpositions are odd permutations and so do not belong to A_4. By (B), the subgroup H, which has index 4 in G, is not contained in any subgroup of index 2 in G. By FTGT, $K^H/\mathbb{Q}$ is an extension of degree 4 that does not contain an intermediate field of degree 2 over $\mathbb{Q}$. So $E = K^H$ is the field we want!

8. Milne Exercise 4-9 (page 57) [Let $f(X)$ be an irreducible polynomial in $\mathbb{Q}[X]$ with both real and nonreal roots. Show that its Galois group is nonabelian. Can the condition that f is irreducible be dropped?]

We regard the splitting field E of $f(X)$ over $\mathbb{Q}$ as a subfield of $\mathbb{C}$. First we observe that if r is a complex root of a polynomial $g(X) \in \mathbb{Q}[X]$, then its complex conjugate $\overline{r}$ is also a root. To see this, write $g(X) = a_n X^n + \cdots + a_0$, with the $a_i \in \mathbb{Q}$. We have $g(\overline{r}) = a_n \overline{r}^n + \cdots + a_0 = \overline{a_n}\ \overline{r}^n + \cdots + \overline{a_0} = \overline{a_n r^n + \cdots + a_0} = \overline{0} = 0$, because congugation is a field automorphism. Since E is generated over $\mathbb{Q}$ by the roots of $f(X)$, it follows that E is stable under conjugation.

Now let α be a real root of $f(X)$ and β be a non-real root. Then $\overline{\beta}$ is another root. Choose an automorphism $\sigma \in G$ (the Galois group) taking α to β. (Here is where we use the assumption that f is irreducible.) Let τ denote the automorphism of E given by complex conjugation. Now compute: $\tau\sigma(\alpha) = \tau(\sigma(\alpha)) = \tau(\beta) = \overline{\beta}$, whereas $\sigma\tau(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha) = \beta$. Since $\overline{\beta} \neq \beta$, we see that $\tau\sigma \neq \sigma\tau$.

The assumption that $f(X)$ is irreducible cannot be dropped. Take, for example, $f(X) = (X^2 + 1)(X - 1)$. The splitting field is $\mathbb{Q}(i)$, which has degree 2, so the Galois group is cyclic of order 2.

These problems are due Tuesday, 30 May, 2017, at 10 pm Nepal time. They must be sent to nap@rnta.eu (copy to rwiegand1unl.edu and swiegand1unl.edu) by 10 pm Nepal time. You may discuss problems with other students in the class, but you must do the write-up completely by yourself, without consulting anyone else. You may refer, by number, to theorems, propositions, etc., in Milne's book, provided that they are results that were covered in NAP Module 1 or Module 2: up to 25 May). If you are ambitious, you can write your solutions in TeX and send them as an attachment. Alternatively, you can write them out (legibly, please), scan them, and send as an attachment. A less desirable option would be to photograph your solutions and send the photo; this will probably be harder to read, so the first two options are preferable.

You can download Milne's book at http://www.jmilne.org/math/CourseNotes/FT.pdf The NAP website is: http://www.rnta.eu/nap/ Feel free to email us anytime with questions.