

# Galois Theory Problem Set 2

Austin Mohr

November 5, 2009

## 1 Problem 10

**Proposition 1.1.** *Let  $p$  be a prime and let  $H$  be a subgroups of  $S_p$ . If  $H$  has a transposition and an element of order  $p$ , then  $H = S_p$ .*

*Proof.* Let  $a, b \in H$  with  $a$  of order  $p$  and  $b$  a transposition. Without loss of generality, let  $b = (0\ 1)$ . As  $a$  has order  $p$  and  $p$  is prime, we have that  $a$  is a  $p$ -cycle. Therefore,  $a^k = (0\ 1\ \dots)$  for some  $k$ . We can re-index the other elements so that we have  $a^k = (0\ 1\ \dots\ p-1)$ . Let  $c = a^k$ . Then  $cbc^{-1} = (0\ 1\ \dots\ p-1)(0\ 1)(p-1\ \dots\ 0\ 1) = (0)(1\ 2)(3)\dots(p-1) = (1\ 2)$ . By induction, we have  $c^kbc^{-k} = c(c^{k-1}bc^{-(k-1)})c^{-1} = (k+1\ k+2)$ . Therefore, we have that  $(0\ 1), (1\ 2), \dots, (p-2\ p-1)$  are generated by  $\{a, b\}$ . Let  $(xy)$  be a transposition. Then  $(x\ x+1)(x+1\ x+2)\dots(y-1\ y) = (x\ y)$  and  $(x\ y)$  is also generated by  $\{a, b\}$ . As every permutation can be decomposed into transpositions we conclude that  $\{a, b\}$  generates  $S_p$ .  $\square$

## 2 Problem 11

**Proposition 2.1.** *The polynomial  $f(x) = x^5 - 2x^3 - 8x + 2$  is not solvable by radicals over the field of rational numbers.*

*Proof.* Observe first that, by Eisenstein's Criterion,  $f(x)$  is irreducible over  $\mathbb{Q}$ . Next, notice that

$$\begin{aligned} f'(x) &= 5x^4 - 6x^2 - 8 \\ &= (5x^2 + 4)(x^2 - 2). \end{aligned}$$

Let  $a_0, a_1$ , and  $a_2$  be the distinct real roots of  $f(x)$ . We also have complex roots  $a_3$  and  $a_4$  with  $a_3 = \overline{a_4}$ . Let  $E$  be the splitting field over  $\mathbb{Q}$  of  $f(x)$ . It must be that  $\text{Gal}(E/\mathbb{Q})$  contains a 2-cycle (there is an automorphism transposing  $a_3$  and  $a_4$  but fixing every other element). We also have that  $|\text{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}]$ , which implies that  $5 \mid [E : \mathbb{Q}]$ . This in turn gives that  $\text{Gal}(E/\mathbb{Q})$  contains an element of order 5. By problem 10 above, we have that  $\text{Gal}(E/\mathbb{Q}) \cong S_5$ , which is not solvable. Hence,  $f(x)$  is not solvable by radicals.  $\square$

### 3 Problem 12

**Proposition 3.1.** *Let  $F$  be a finite field. The product of all the nonzero elements of  $F$  is equal to  $-1$ .*

*Proof.* Let  $|F| = p^k$ . Evidently,  $|F^\times| = p^k - 1$ . Furthermore,  $F^\times$  is cyclic (and so abelian). Let  $\sigma$  be a generator for  $F^\times$ . We have that  $\sigma^{p^k-1} = 1$  and  $\sigma^m \neq 1$  for  $m < p^k - 1$ .

Suppose  $p = 2$ . For any  $k$ ,  $2^k - 1$  is odd. Here, the only self-inverse element is 1, so the product  $1 \cdot \sigma \cdot \dots \cdot \sigma^{2^k-2}$  can be arranged such that inverse pairs are group together. Hence, the product is equal to 1, which is congruent to  $-1$  modulo 2.

Suppose  $p$  is an odd prime. For any  $k$ ,  $p^k - 1$  is even. Here, the self-inverse elements are 1 and  $\sigma^{\frac{p^k-1}{2}}$ , so the product  $1 \cdot \sigma \cdot \dots \cdot \sigma^{p^k-2}$  can be arranged such that inverse pairs are group together. Hence, the product is equal to  $\sigma^{p^k-2}$ , which is congruent to  $-1$  modulo  $p$ .  $\square$

**Corollary 3.2.** *(Wilson's Theorem) For every prime number  $p$ ,  $(p - 1)! \equiv -1 \pmod{p}$ .*

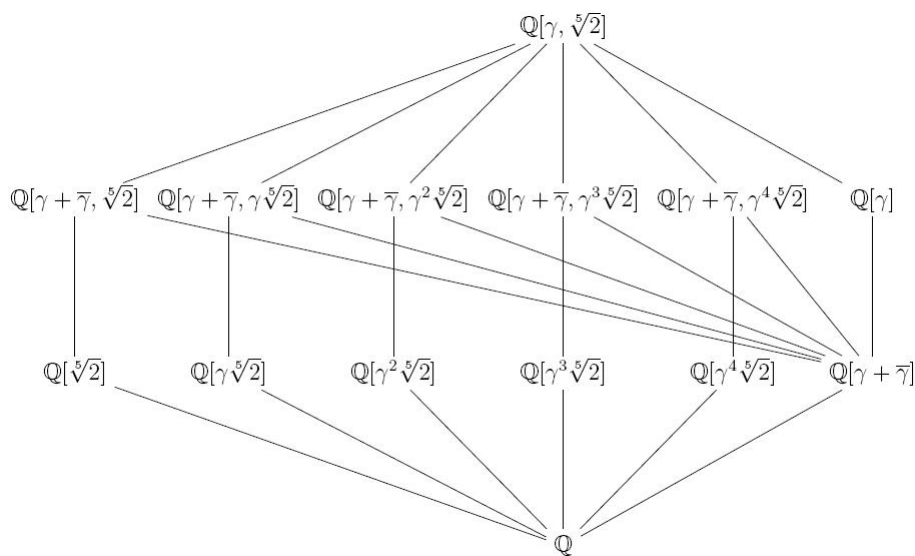
*Proof.* The elements of  $F_p^\times$  are precisely  $1, \dots, p - 1$ , and so by the proposition above gives

$$\begin{aligned} (p - 1)! &= 1 \cdot \dots \cdot (p - 1) \\ &= -1 \pmod{p}. \end{aligned}$$

In other words,  $(p - 1)! \equiv -1 \pmod{p}$ .  $\square$

### 4 Problem 13

Let  $E$  be the splitting field of  $x^5 - 2$  over  $\mathbb{Q}$ . The lattice of all fields intermediate between  $\mathbb{Q}$  and  $E$  is pictured below, where  $\gamma$  represents a primitive fifth root of unity.



(Many thanks to K. Brown for the image.)

## 5 Problem 14

Let  $F$  be a field of prime characteristic  $p$ . Let  $E$  be a field extending  $F$ . The field  $E$  is a normal separable extension of  $F$  of dimension  $p$  if and only if  $E$  is the splitting field over  $F$  of an irreducible polynomial of the form  $x^p - x - a$  for some  $a \in F$ .

*Proof.* ( $\Rightarrow$ ) Let  $E$  be a normal, separable extension of  $F$  having dimension  $p$ . We have that  $|\text{Gal}(E/F)| = p$ , and so  $\text{Gal}(E/F)$  is cyclic. Let  $\sigma$  generate  $\text{Gal}(E/F)$ . The automorphisms of  $E$  are  $1, \sigma, \sigma^2, \dots, \sigma^{p-1}$ . Define

$$t = 1 + \sigma + \sigma^2 + \dots + \sigma^{p-1}.$$

We know that these automorphisms are linearly independent, so there is  $v \in E$  such that

$$t(v) = v + \sigma(v) + \sigma^2(v) + \dots + \sigma^{p-1}(v) = u \neq 0.$$

Apply  $\sigma$  to  $u$  to get

$$\begin{aligned} \sigma(u) &= \sigma(v) + \sigma^2(v) + \sigma^3(v) + \dots + \sigma^{p-1}(v) + \sigma^p(v) \\ &= 1 + \sigma(v) + \sigma^2(v) + \dots + \sigma^{p-1}(v). \end{aligned}$$

Hence,  $\sigma(u) = u$ . As  $u$  is fixed by  $\sigma$ , it must be that  $u \in F$ , and so  $v \in (E \setminus F)$ . Let now  $v' = vu^{-1}$ . We have that  $t(v') = 1$ , so assume (without loss of generality) that  $t(v) = 1$ .

Let

$$w = v + 2\sigma(v) + 3\sigma^2(v) + \dots + (p-1)\sigma^{p-2}(v).$$

We have that

$$\begin{aligned} w - \sigma(w) &= v + 2\sigma(v) + 3\sigma^2(v) + \dots + (p-1)\sigma^{p-2}(v) \\ &\quad - (\sigma(v) + 2\sigma^2(v) + 3\sigma^3(v) + \dots + (p-1)\sigma^{p-1}(v)) \\ &= v + \sigma(v) + \sigma^2(v) + \dots + \sigma^{p-1}(v) \\ &= 1. \end{aligned}$$

Hence,  $\sigma(w) = w - 1$ . Now, let  $\gamma = -w$  to obtain

$$\sigma(\gamma) = \sigma(-w) = -\sigma(w) = -(w - 1) = -w + 1 = \gamma + 1.$$

This entails that  $\gamma = -w \in (E \setminus F)$ , and so  $F[\gamma]$  has dimension  $p$  over  $F$ . As  $\sigma(\gamma^p) = \sigma(\gamma)^p = (\gamma + 1)^p = \gamma^p + 1$ , we have that

$$\sigma(\gamma^p - \gamma) = (\gamma + 1)^p - (\gamma + 1) = \gamma^p - \gamma.$$

Hence,  $\gamma^p - \gamma \in F$ . Let now  $a = \gamma^p - \gamma$ . We see that  $x^p - x - a$  has roots  $\gamma, \gamma + 1, \gamma + 2, \dots, \gamma + (p-1)$ , and so  $E$  is the splitting field of  $f(x) = x^p - x - a$ .

( $\Leftarrow$ ) Let  $E$  be the splitting field over  $F$  of the irreducible polynomial  $f(x) = x^p - x - a$ . As  $f'(x) = -1$ , we have that  $f(x)$  and  $f'(x)$  share no common roots, and so  $f(x)$  is separable.

Now, let  $u \in E$  be a root of  $f(x)$ . It follows that

$$\begin{aligned} f(u+1) &= (u+1)^p - (u+1) - a \\ &= u^p + 1^p - u - 1 - a \\ &= u^p - u - a \\ &= 0. \end{aligned}$$

Hence,  $u+1$  is also a root of  $f(x)$ . Proceeding inductively,  $u, u+1, u+2, \dots, u+(p-1)$  are the  $p$  distinct roots of  $f(x)$ . Hence,  $E$  is a normal separable extension of  $F$  of dimension  $p$ . □