

## 1 Homework 9.

1. Suppose  $E/F$  is a field extension,  $\alpha \in E$ , and  $[F[\alpha] : F]$  is odd. Prove that  $F[\alpha^2] = F[\alpha]$ .
2. Suppose  $a_1, \dots, a_n$  are positive rational numbers. Prove that  $\sqrt[3]{2}$  is not in  $\mathbb{Q}[\sqrt{a_1}, \dots, \sqrt{a_n}]$ .
3. Given a set  $A$  of points, we say a line is 1-constructible with respect to  $A$  if it is passed through two points in  $A$ . We say a circle is 1-constructible with respect to  $A$  if its center is in  $A$  and its radius is the distance between two points in  $A$ . We say a point  $p$  is 1-constructible with respect to  $A$  if it is an intersection point of either two 1-constructible lines, or one 1-constructible line and one 1-constructible circle, or two 1-constructible circles. Let  $A_0 := \{(0, 0), (1, 0)\}$ . We say  $p := (\alpha, \beta)$  is a constructible point if there exists a sequence of points  $p_i := (\alpha_i, \beta_i)$  such that  $p_0 \in A_0$ ,  $p_n = p$ , and  $p_{i+1}$  is 1-constructible with respect to

$$A_i := A_0 \cup \{p_1, \dots, p_i\}.$$

- (a) Let  $F_i := \mathbb{Q}[\alpha_1, \beta_1, \dots, \alpha_i, \beta_i]$ . Justify it for yourself that

$$[F_{i+1} : F_i] \in \{1, 2, 4\}.$$

- (b) Prove that  $[F_n : \mathbb{Q}]$  is a power of 2.
- (c) Prove that  $\sqrt[3]{2}, \pi$  and  $\cos(20^\circ)$  are not constructible.
4. Suppose  $E \subseteq \mathbb{C}$  is a splitting field of  $x^p - 2$  over  $\mathbb{Q}$  where  $p$  is an odd prime number.
    - (a) Prove that  $E = \mathbb{Q}[\sqrt[p]{2}, \zeta_p]$  where  $\zeta_p := e^{2\pi i/p}$ .
    - (b) Prove that  $[E : \mathbb{Q}] = p(p-1)$ .
    - (c) Prove that  $\text{Gal}(E/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \ltimes (\mathbb{Z}/p\mathbb{Z})$  and the isomorphism is given by

$$\theta \mapsto (a_\theta, b_\theta), \text{ where } \theta(\zeta_p) = \zeta_p^{a_\theta} \text{ and } \theta(\sqrt[p]{2}) = \zeta_p^{b_\theta} \sqrt[p]{2}.$$

.(**Hint.** Note that  $[E : \mathbb{Q}]$  is a multiple of  $[\mathbb{Q}[\zeta_p] : \mathbb{Q}]$  and  $[\mathbb{Q}[\sqrt[p]{2}] : \mathbb{Q}]$ . Argue why  $[\mathbb{Q}[\zeta_p] : \mathbb{Q}] = p - 1$  and  $[\mathbb{Q}[\sqrt[p]{2}] : \mathbb{Q}] = p$ .

Show that the given map on  $\text{Gal}(E/\mathbb{Q})$  is a well-defined injective group homomorphism, and then compare the order of the domain and codomain.)

5. Suppose  $E$  is a splitting field of  $f(x) \in F[x]$  over  $F$ .

- (a) Prove that if  $\gcd(f, f') \neq 1$ , then  $E \otimes_F F[x]/\langle f \rangle$  has a non-zero nilpotent element.
- (b) Prove that if  $\gcd(f, f') = 1$ , then

$$E \otimes_F (F[x]/\langle f \rangle) \simeq \underbrace{E \oplus \cdots \oplus E}_{\deg f\text{-times}}.$$

6. Suppose  $F$  is a field,  $f(x) \in F[x]$  is a monic irreducible polynomial in  $F[x]$ . Let  $E$  be a splitting field of  $f$  over  $F$ . Suppose

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

for some  $\alpha_i$ 's in  $E$ .

- (a) Prove that for all  $\theta \in \text{Aut}_F(E)$  and  $i$ ,

$$\theta(\alpha_i) \in \{\alpha_1, \dots, \alpha_n\},$$

and deduce that we get a permutation  $\sigma(\theta)$  in the symmetric group of  $\{\alpha_1, \dots, \alpha_n\}$ .

- (b) Prove that

$$\sigma : \text{Aut}_F(E) \rightarrow S_{\{\alpha_1, \dots, \alpha_n\}}, \quad \theta \mapsto \sigma(\theta)$$

is an injective group homomorphism.

- (c) Prove that the action of  $\text{Aut}_F(E)$  on  $\{\alpha_1, \dots, \alpha_n\}$  is transitive.

7. Suppose  $p$  is an odd prime, and  $a \in \mathbb{F}_p^\times$ . Prove that  $x^p - x + a$  is irreducible in  $\mathbb{F}_p[x]$ .

(**Hint. First method.** Let  $E$  be a splitting field of  $x^p - x + a$  over  $\mathbb{F}_p$ . Let  $\alpha \in E$  be a zero of  $x^p - x + a$ . Prove that  $\alpha + i$  is a zero of  $x^p - x + a$  for every  $i \in \mathbb{F}_p$ , and deduce that

$$x^p - x + a = \prod_{i \in \mathbb{F}_p} (x - \alpha - i).$$

Notice that  $m_{\alpha, \mathbb{F}_p}(x)$  divides  $x^p - x + a$ , and consider the coefficient of  $x^{d-1}$  in  $m_{\alpha, \mathbb{F}_p}(x)$  and show that  $\deg m_{\alpha, \mathbb{F}_p} = p$ .

**Second method.** Let  $E$  be a splitting field of  $x^p - x + a$  over  $\mathbb{F}_p$ . Suppose  $\alpha \in E$  is a zero of  $x^p - x + a$ . Prove that  $E = \mathbb{F}_p[\alpha]$ . Note that  $\text{Aut}(E/\mathbb{F}_p)$  acts transitively on  $V_{m_{\alpha, \mathbb{F}_p}}(E)$  and it is generated by the Frobenius map  $\sigma: E \rightarrow E, \sigma(x) = x^p$ . Note that  $\sigma(\alpha) = \alpha - a$ , and so the orbit of  $\alpha$  has  $p$  elements. )

8. Let's recall that  $\mathbb{F}_q$  denotes a finite field of order  $q$  and for every prime power  $q$  there exists a unique field of order  $q$ , up to an isomorphism.

- (a) Prove that  $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$  if and only if  $m|n$ .
- (b) Let  $f(x) \in \mathbb{F}_p[x]$  be a monic irreducible polynomial of degree  $d$ . Prove that  $f(x) | x^{p^d} - x$ .
- (c) Suppose  $f(x) \in \mathbb{F}_p[x]$  is irreducible and  $f(x) | x^{p^n} - x$ . Prove that  $\deg f | n$ .
- (d) Let  $P_d$  be the set of all irreducible monic polynomials of degree  $d$  in  $\mathbb{F}_p[x]$ . Prove that

$$\prod_{d|n} \prod_{f \in P_d} f(x) = x^{p^n} - x.$$

- (e) Show that  $\sum_{d|n} d |P_d| = p^n$ .

(**Hint.** Notice that if  $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ , then by the tower formula,  $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}_p]$ . To show the converse, you can use the result that we proved last quarter:  $\mathbb{F}_{p^k}$  is the splitting field of  $x^{p^k} - x$  over  $\mathbb{F}_p$ , and it consists of all the zeros of this polynomial. Argue that if  $m|n$ , then  $x^{p^m} - x$  divides  $x^{p^n} - x$ .

For the second part, suppose  $E = F[\alpha]$  is an extension of  $F$  and  $f(\alpha) = 0$ . Argue why  $m_{\alpha, F} = f$ . Deduce that  $F[\alpha] \simeq \mathbb{F}_{p^d}$ , and so  $\alpha$  is a zero of  $x^{p^d} - x$ .

For the third part, notice that  $\mathbb{F}_{p^n}$  contains a zero  $\alpha$  of  $f$ . Notice that  $[\mathbb{F}_p[\alpha] : \mathbb{F}_p] = \deg f$  and use the first part.

To show the forth part, use the second and the third parts, and argue why  $x^{p^n} - x$  does not have multiple roots.

To show the last part, compare the degrees of polynomials given in the equation of the forth part. )

(Using the Möbius inversion, one can deduce that

$$|P_d| = \sum_{d|n} \mu(n/d)p^d,$$

and this can be used to show

$$\lim_{d \rightarrow \infty} \frac{|P_d|}{p^d/d} = 1,$$

which is the positive characteristic analogue of the prime number theorem.

In fact, we can use this result and deduce

$$|P_d| = \frac{p^d}{d} + O\left(\frac{p^{d/2}}{d}\right),$$

which is an analogue of the Riemann Hypothesis.)

9. Suppose  $p$  is a prime and  $\mathbb{F}_p(x, y)$  is a field of fractions of  $\mathbb{F}_p[x, y]$ .
  - (a) Prove that  $[\mathbb{F}_p(x) : \mathbb{F}_p(x^p)] = p$  and  $[\mathbb{F}_p(x, y) : \mathbb{F}_p(x^p, y^p)] = p^2$ .
  - (b) Prove that  $\phi : \mathbb{F}_p(x, y) \rightarrow \mathbb{F}_p(x^p, y^p), \phi(z) = z^p$  is an isomorphism.
  - (c) Prove that  $\mathbb{F}_p(x, y)/\mathbb{F}_p(x^p, y^p)$  is not a simple extension; that means there is no  $\frac{g}{h} \in \mathbb{F}_p(x, y)$  such that  $\mathbb{F}_p(x, y) = \mathbb{F}_p(x^p, y^p)\left[\frac{g}{h}\right]$ .
10. Suppose  $E$  is a splitting field of  $f \in F[x]$  over  $F$ .
  - (a) Prove that  $E/F$  is a normal extension.
  - (b) Prove that for every  $\alpha \in E$ ,  $\text{Aut}_F(E)$  acts transitively on  $V_{m_{\alpha;F}}(E)$ .

(**Hint.** For  $\alpha \in E$ , let  $E'$  be a splitting field of  $g(x) := f(x)m_{\alpha;F}(x)$  over  $F$ . Suppose  $\alpha' \in V_{m_{\alpha;F}}(E')$ . Then there exists an  $F$ -isomorphism  $\theta : F[\alpha] \rightarrow F[\alpha']$  such that  $\theta(\alpha) = \alpha'$ . Note that  $E'$  is a splitting field of  $g$  over  $F[\alpha]$  and a splitting field of  $g^\theta = g$  over  $F[\alpha']$ . Deduce that there exists  $\hat{\theta} \in \text{Aut}_\theta(E')$ . Note that  $\hat{\theta}$  permutes zeros of  $f$ , and so  $\hat{\theta}(E) = E$ . Therefore,  $\alpha' = \hat{\theta}(\alpha) \in E$ .)

11. Suppose  $n$  is a positive integer,  $F$  is a field, and either  $F$  is of characteristic 0 or it is of characteristic  $p > 0$  and  $\gcd(p, n) = 1$ . Let  $E$  be a splitting field of  $x^n - 1$  over  $F$ .

(a) Prove that  $E/F$  is a Galois extension.

**(Hint.** Argue why  $x^n - 1$  is separable.)

(b) Prove that  $\text{Gal}(E/F)$  can be embedded into  $(\mathbb{Z}/n\mathbb{Z})^\times$ .

**(Hint.** Argue why  $Z := \{\zeta \in E \mid \zeta^n = 1\}$  is a cyclic group of order  $n$ . Observe that the restriction gives us an embedding of  $\text{Gal}(E/F)$  into  $\text{Aut}(Z)$ .)

12. (Kummer theory: cyclic) Suppose  $n$  is a positive integer,  $F$  is a field, and  $x^n - 1$  has  $n$  distinct zeros in  $F$ . By the previous problem, you know  $\mu_n(F) := \{\zeta \in F \mid \zeta^n = 1\}$  is a cyclic group of order  $n$ . Suppose  $\zeta_n$  is a generator of  $\mu_n(F)$ . Suppose  $a \in F^\times \setminus (F^\times)^n$ , and let  $E$  be a splitting field of  $x^n - a$  over  $F$ .

(a) Prove that  $E/F$  is a Galois extension and  $E = F[\sqrt[n]{a}]$  where  $\sqrt[n]{a} \in E$  is a zero of  $x^n - a$ .

**(Hint.** Show that  $x^n - a = (x - \sqrt[n]{a})(x - \zeta_n \sqrt[n]{a}) \cdots (x - \zeta_n^{n-1} \sqrt[n]{a})$ .)

(b) Prove that  $\text{Gal}(E/F) \rightarrow \mu_n(F)$ ,  $\sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$  is a well-defined injective group homomorphism. Deduce that  $\text{Gal}(E/F)$  is cyclic and its order is a divisor of  $n$ .

13. (Kummer theory: cyclic) Suppose  $\mathbb{Q}[\zeta_n] \subseteq F \subseteq \mathbb{C}$  is a tower of fields where  $\zeta_n = e^{2\pi i/n}$ . For  $a \in \mathbb{C}$ , let  $\sqrt[n]{a} \in \mathbb{C}$  be a zero of  $x^n - a$ .

(a) For  $a_1, a_2 \in F^\times$ , prove that

$$F[\sqrt[n]{a_1}] = F[\sqrt[n]{a_2}] \quad \text{if and only if} \quad \langle a_1(F^\times)^n \rangle = \langle a_2(F^\times)^n \rangle.$$

**(Hint.**  $(\Rightarrow)$  Recall that

$$\psi_i : \text{Gal}(F[\sqrt[n]{a_i}]/F) \rightarrow \langle \zeta_n \rangle, \quad \psi_i(\sigma) := \frac{\sigma(\sqrt[n]{a_i})}{\sqrt[n]{a_i}}$$

is an injective group homomorphism. Since  $\langle \zeta_n \rangle$  has a unique subgroup of order  $[F[\sqrt[n]{a_i}] : F]$ , we have that  $\text{Im}(\psi_1) = \text{Im}(\psi_2)$ . Suppose  $\sigma_0$  is a

generator of  $\text{Gal}(F[\sqrt[n]{a_1}]/F)$ ; then  $\sigma_0(\sqrt[n]{a_1})/\sqrt[n]{a_1} = (\sigma_0(\sqrt[n]{a_2})/\sqrt[n]{a_2})^i$  for some  $i$ . This implies that  $\sigma_0(\sqrt[n]{a_1}/\sqrt[n]{a_2}^i) = \sqrt[n]{a_1}/\sqrt[n]{a_2}^i$ ; deduce that  $a_1(F^\times)^n \in \langle a_2(F^\times)^n \rangle$ .

- (b) Prove that  $\text{Gal}(F[\sqrt[n]{a}]/F) \simeq \langle a(F^\times)^n \rangle$  for every  $a \in F^\times$ .

(**Hint.** Suppose  $\sigma_0$  is a generator of  $\text{Gal}(F[\sqrt[n]{a}]/F)$ . Since

$$\psi : \text{Gal}(F[\sqrt[n]{a}]/F) \rightarrow \langle \zeta_n \rangle, \quad \psi(\sigma) := \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$$

is an injective group homomorphism,

$$\sigma_0^d = \text{id} \Leftrightarrow (\sigma_0(\sqrt[n]{a})/\sqrt[n]{a})^d = 1 \Leftrightarrow \sqrt[n]{a}^d \in F^\times \Leftrightarrow a^d \in (F^\times)^n.)$$

14. Prove that  $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle$  where  $\sigma_p : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ ,  $\sigma_p(x) = x^p$ .
15. Let  $\Phi_n(x)$  be the  $n$ -th cyclotomic polynomial. Suppose  $p$  is an odd prime which does not divide  $n$ . Let  $\Phi_{n,p} \in \mathbb{F}_p[x]$  be  $\Phi_n(x) \pmod{p}$ . Let  $\overline{\mathbb{F}}_p$  be an algebraic closure of  $\mathbb{F}_p$  and  $E \subseteq \overline{\mathbb{F}}_p$  is a splitting field of  $\Phi_{n,p}(x)$  over  $\mathbb{F}_p$ .

- (a) Suppose  $\zeta \in E$  is a zero of  $\Phi_{n,p}(x)$ . Prove that  $\zeta$  is not a zero of  $\Phi_{d,p}(x)$  for any  $d|n$  and  $d \neq n$ . Deduce that the multiplicative order  $o(\zeta)$  of  $\zeta$  is  $n$ .

(**Hint.**  $x^n - 1$  does not have multiple zeros in  $\overline{\mathbb{F}}_p$ .)

- (b) Prove that  $\Phi_{n,p}(x) = \prod_{1 \leq i \leq n, \gcd(i,n)=1} (x - \zeta^i)$  where  $\zeta \in E$  is a zero of  $\Phi_{n,p}(x)$ . Deduce that  $E = \mathbb{F}_p[\zeta]$  and

$$\theta : \text{Gal}(\mathbb{F}_p[\zeta]/\mathbb{F}_p) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \theta(\sigma) = a_\sigma \pmod{n}$$

is an injective group homomorphism where  $\sigma(\zeta) = \zeta^{a_\sigma}$ .

- (c) Suppose  $\theta$  is as in the previous problem. Prove that

$$\theta(\text{Gal}(E/F)) = \langle p \rangle.$$

(**Hint.** Use the fact that  $\text{Gal}(E/F) = \langle \sigma_p \rangle$ , where  $\sigma_p(a) = a^p$  is the Frobenius map.)

- (d) Prove that if  $\Phi_{n,p}(x)$  has a zero in  $\mathbb{F}_p$ , then  $n|p-1$ .

- (e) Use the previous problem to show there are infinitely many primes of the form  $\{nk + 1\}_{k=1}^{\infty}$ .

**(Hint.** Suppose  $p_1, \dots, p_r$  are primes of the form  $nk + 1$ . Consider

$$f(x) := \Phi_n\left(2n \prod_{i=1}^r p_i x\right);$$

for some value of  $a \in \mathbb{Z}$ ,  $f(a)$  has a prime factor  $\ell$ . Argue why  $\ell \nmid n$  and  $\ell \neq p_i$ . Use the previous problem to deduce that  $n \mid \ell - 1$ .)

- (f) Prove that  $\Phi_{n,p}(x)$  is irreducible in  $\mathbb{F}_p[x]$  if and only if  $\langle p \rangle = (\mathbb{Z}/n\mathbb{Z})^\times$ .