# 1 Homework 1.

1. Suppose $K/F$ is a field extension, and $K_1$ and $K_2$ are two intermediate subfields; that means $F \subseteq K_i \subseteq K$. Let $K_1K_2$ be the subfield of $K$ which is generated by $K_1 \cup K_2$. We say $K_1K_2$ is a composite of $K_1$ and $K_2$. Suppose $[K_i : F] < \infty$ for $i = 1, 2$.

   (a) Prove that
   $$K_1K_2 = \{\sum_{i=1}^{m} a_i b_i \mid m \in \mathbb{Z}^+, a_i \in K_1, b_i \in K_2\}.$$

   (b) Prove that there exists a surjective $F$-algebra homomorphism
   $$m : K_1 \otimes_F K_2 \to K_1K_2$$
   such that $m(x \otimes y) = xy$.

   (c) In the setting of the previous part, prove that the following statements are equivalent

      i. $K_1 \otimes_F K_2$ is a field.

      ii. $\phi$ is an isomorphism.

      iii. $[K_1K_2 : F] = [K_1 : F][K_2 : F]$.

   (d) Prove that $\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Q}} \mathbb{Q}[\sqrt{3}] \simeq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

2. 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

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

which is the positive characteristic analogue of the prime number theorem. In fact, we can use this result and deduce

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

which is an analogue of the Riemann Hypothesis.)

3. Prove that $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ are not isomorphic.

4. 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 $\phi : \mathbb{F}_p(x, y) \to \mathbb{F}_p(x^p, y^p), \phi(z) = z^p$ 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 $\mathbb{F}_p(x,y) = \mathbb{F}_p(x^p,y^p)[\frac{g}{h}]$.

5. Suppose $\alpha, \beta \in \mathbb{C}$ are algebraic over $\mathbb{Q}$. Let $f := m_{\alpha,\mathbb{Q}}$ and $g := m_{\beta,\mathbb{Q}}$. Prove that $f$ is irreducible in $(\mathbb{Q}[\beta])[x]$ if and only if $g$ is irreducible in $(\mathbb{Q}[\alpha])[x]$.

   (**Hint.** Prove that both of these conditions are equivalent to

$$[\mathbb{Q}[\alpha,\beta] : \mathbb{Q}] = \deg f \deg g.)$$

6. 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-contructible 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

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

   (a) Let $F_i := \mathbb{Q}[\alpha_1,\beta_1,\ldots,\alpha_i,\beta_i]$. 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 $\cos(20°)$ are not constructible.

7. 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 $E$. Let $\mathrm{Aut}(E/F)$ be the set of isomorphisms $\theta : E \to E$ such that $\theta(a) = a$ for all $a \in F$.

(a) Prove that for all $\theta \in \mathrm{Aut}(E/F)$ 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

$$\sigma : \mathrm{Aut}(E/F) \to S_{\{\alpha_1,\dots,\alpha_n\}}, \quad \theta \mapsto \sigma(\theta)$$

is an injective group homomorphism.

(c) Prove that the action of $\mathrm{Aut}(E/F)$ on $\{\alpha_1, \dots, \alpha_n\}$ is transitive.

(For this problem, you should only write the details for the last part. But you have to know why the other parts are correct.)