Algebra Homework

March 26, 2017

1 Week 1

Ex 1.1.

1. Prove that if $[K(\alpha):K]$ is odd, then $K(\alpha)=K(\alpha^2)$.
2. Given L_1/K and L_2/K with $L_1, L_2 \subseteq L$, show that

$$L_1 \otimes_K L_2 \text{ is a field } \iff [L_1L_2 : K] = [L_1 : K][L_2 : K]$$

Ex 1.2.

1. Prove that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
2. Determine $\left[\mathbb{Q}\left(\sqrt{3+2\sqrt{2}}\right) : \mathbb{Q}\right]$, $\left[\mathbb{Q}\left(\sqrt{3+4i}+\sqrt{3-4i}\right) : \mathbb{Q}\right]$, $\left[\mathbb{Q}\left(\cos\frac{\pi}{6}+i\sin\frac{\pi}{6}\right) : \mathbb{Q}\right]$.

Ex 1.3. Let R be a PID and $a \in R$. TFAE:

1. a is an irrducible element.
2. $\langle a \rangle$ is a maximal ideal.
3. $\langle a \rangle$ is a prime ideal.
4. a is a prime element.

Ex 1.4. Let L/K be algebraic and $\tau : L \to L$ be a monomorphism fixing K. Show that τ is onto. (so τ is isom.)

Ex 1.5.

1. Determine the splitting field L for x^4+2 over $\mathbb{Q}$, $[L:\mathbb{Q}]$ and $\mathrm{Aut}(L/Q)$.
2. Determine the splitting field L for x^6-4 over $\mathbb{Q}$, $[L:\mathbb{Q}]$ and $\mathrm{Aut}(L/Q)$.

Ex 1.6. Let $L_1, L_2 \subseteq L$ with $[L_1 : K] < \infty$ and $[L_2 : K] < \infty$. Assume L_1 and L_2 are splitting fields over K. Show that

1. L_1L_2 is a splitting fields over K.
2. $L_1 \cap L_2$ is a splitting fields over K.

2 Week 2

3 Week 3

Ex 3.1. Let L/K be a finite extension with $[L:K]=n$. For any field extension M/K, there are at most n monomorphisms from L to M which fix K.

Ex 3.2.

1. If F is a finite field, then F is not algebraically closed.
2. Let F be a finite field and $F(\alpha,\beta)/F$ be an algebraic extension. Show that $\exists c \in F(\alpha,\beta)$ s.t. $F(\alpha,\beta)=F(c)$. i.e. $F(\alpha,\beta)/F$ is a simple extension.

Ex 3.3.

1. Let F be a finite field and G, H be subgroups of $(F^{\times},\cdot,1)$. If $|G|=|H|=n$, then $G=H$.
2. If F is a field such that $(F^{\times},\cdot,1)$ is cyclic, then F is a finite field.

Ex 3.4.

1. For any prime p and any nonzero $a \in \mathbb{F}_p$, prove that $x^p - x + a$ is irreducible and separable.
2. Show that $f(x)=x^3+px+q \in K[x]$ is separable $\iff 4p^3+27q^2 \neq 0$.

Ex 3.5. Let L/K be a separable extension and $f(x) \in K[x]$ be an irreducible polynomial. Assume that $f(x)=f_1(x)\cdots f_n(x)$ for some $f_i(x) \in L[x] \quad \forall i=1,\ldots,n$. Show that if f_i is separable $\forall i$, then f is separable.

Ex 3.6.

1. If $\operatorname{char} K = p \neq 0$ and $[L:K] < \infty$ with $p \nmid [L:K]$, then L is separable over K.
2. Let $\operatorname{char} K = p \neq 0$. Show that an algebraic element $\alpha \in L$ is separable over $K \iff K(\alpha) = K\left(\alpha^{p^n}\right)$ for all $n \geq 1$.

4 Week 4

Ex 4.1.

1. Determine the Galois group of $f(x) = x^5 - 4x + 2$ over $\mathbb{Q}$.
2. Determine the Galois group of $f(x) = x^3 - 3x + 1$ over $\mathbb{Q}$.

Ex 4.2. Let $\operatorname{char} K = 0$ and F/K be finite, normal. Let $g(x) \in K[x]$ and L be a splitting field of $g(x)$ over F. Show that L/K is a normal extension.

(Note: $g(x) \in K[x]$ but L is over F)

Ex 4.3.

Def 1.

- A character χ of a group G with values in a field L is a homomorphism $\chi : G \to L^\times$.
- The characters $\chi_1, \ldots, \chi_n$ of G are said to be linearly independent over L if there is no nontrivial relation

$$a_1\chi_1 + \cdots + a_n\chi_n = 0, \quad a_1, \ldots, a_n \in L \text{ are not all } 0$$

  as a function on G.

1. Show that if $\chi_1, \ldots, \chi_n$ are distinct characters of G with values in L, then they are linearly independent over L.
2. Show that if $\sigma_1, \ldots, \sigma_n$ are distinct monomorphisms from K to L, then they are linearly independent over L.
3. Show that distinct automorphisms of K are linearly independent over K.

Ex 4.4.

1. If L/K is Galois, then $\exists f$: irr. in $K[x]$ s.t. L is a splitting field of $f(x)$ over K.
2. TFAE
   (a) L/K is a Galois extension.
   (b) K is the fixed field of a subgroup of $\operatorname{Aut}(L)$.
   (c) K is the fixed field of $\operatorname{Aut}(L/K)$.

Ex 4.5. Find the Galois group of $x^4 - 2$ over $\mathbb{Q}$. Find all subgroups of this group and find all corresponding intermediate fields between the splitting field of $x^4 - 2$ over $\mathbb{Q}$ and $\mathbb{Q}$.

Ex 4.6. Find all proper subfields of $\mathbb{Q}\left(\sqrt[3]{5}, \frac{-1+i\sqrt{3}}{2}\right)$ and $\mathbb{Q}\left(i, \sqrt{7}\right)$ respectively.

5 Week 5

Ex 5.1.

1. Let p be an odd prime with $p \nmid m$. Suppose $a \in \mathbb{Z}$ s.t. $\Phi_m(a) \equiv 0 \pmod{p}$. then $\mathrm{ord}(a) = m$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. (hint: $x^m - 1 = \prod_{d|m} \Phi_d(x)$)
2. Let $a \in \mathbb{Z}$. Show that if p is an odd prime dividing $\Phi_m(a)$, then either $p \mid m$ or $p \equiv 1 \pmod{m}$.

Ex 5.2.

1. Show that $\left[\mathbb{Q}\left(\zeta_n + \frac{1}{\zeta_n}\right) : \mathbb{Q}\right] = \frac{\varphi(n)}{2}$.
2. Find Φ_8, Φ_9.
3. Show that $x^16 + 1$ is irreducible in $\mathbb{Q}[x]$ and is reducible in $\mathbb{F}_7[x]$ as a product of 4 quartic polynomials.

Ex 5.3. show that p: odd prime, $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is cyclic of order $p^{e-1}(p-1)$ and $(\mathbb{Z}/2^e\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z}, e \geq 2$.

Hints:

1. Check $(1+p)^{p^{e-1}} \equiv 1 \pmod{p^e}$ but $(1+p)^{p^{e-2}} \not\equiv 1 \pmod{p^e}$. And for $e \geq 3$, $(1+2^2)^{2^{e-2}} \equiv 1 \pmod{2^e}$ but $(1+2^2)^{2^{e-3}} \equiv 1 \pmod{2^e}$.
2. If each Sylow p-subgroup of g is normal, then G is isomorphic to the product of all sylow p-subgroups. $(1+p)^{p^{e-2}} \not\equiv 1 \pmod{p^e}$.

Ex 5.4.

1. Let $\mathbb{C}(t)$ be the field of rational functions over $\mathbb{C}$ and L be a splitting field of $x^n - t$ over $\mathbb{C}(t)$. Find $\mathrm{Gal}(L/\mathbb{C}(t))$.
2. Let $\mathbb{F}_p(t)$ be the field of rational functions over $\mathbb{F}_p$ and L be a splitting field of $x^n - t$ over $\mathbb{F}_p(t)$. Find $\mathrm{Gal}(L/\mathbb{F}_p(t))$.

Ex 5.5. Let $\mathrm{char}\, K \neq 2, 3$ and $f(x) = x^4 + px^2 + qx + r$ be irr. and separable with roots $\alpha_1, \ldots, \alpha_4$. Let $L = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and $G_f = \mathrm{Gal}(L/K) \leq S_4$. Set $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$.

1. Show that $L^{G_f \cap V} = K(\beta_1, \beta_2, \beta_3)$ and $\mathrm{Gal}\left(K(\beta_1, \beta_2, \beta_3)/K\right) \cong G_f/G_f \cap V$ where $V = \{\, 1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \,\} \leq S_4$.
2. Show that there exists i s.t. $\beta_i \in K \iff G_f \subseteq D_4$.
3. Let $h(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3) \in K[x]$ with discriminant $D(h)$, Show that
   (a) If $h(x)$ is irr. and $D(h) \notin K^2$, then $G_f \cong S_4$.
   (b) If $h(x)$ is irr. and $D(h) \in K^2$, then $G_f \cong A_4$.
   (c) If $h(x)$ splits completely in $K[x]$, then $G_f \cong V$.
   (d) Let $h(x)$ has one root in K. Then
      i. If $f(x)$ is irr. over $K(\beta_1, \beta_2, \beta_3)$, then $G_f \cong D_4$.
      ii. If $f(x)$ is reducible over $K(\beta_1, \beta_2, \beta_3)$, then $G_f \cong C_4$.