Algebra Homework

May 22, 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

Ex 2.1. Show that
$$\mathbb{F}_q \subseteq \mathbb{F}_r \iff r = q^n \text{ for some } n \in \mathbb{N}.$$

Ex 2.2. Let $K = \mathbb{F}_q$ be a finite field.

1. Show that there exists an irreducible polynomial of degree n in $K[x]$ for all $n \in \mathbb{N}$.
2. Let L be a splitting field of $x^n - 1$ over K. Show that $[L : K] = k$ is the least positive integer s.t. $n \mid q^k - 1$.

Ex 2.3. Let K be a finite field. Show that any element in K can be written as the sum of two squares.

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 $f_i(x) \in L[x] \quad \forall\, i=1,\dots,n$. 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 $\chi_1, \dots, \chi_n$ of G are said to be linearly independent over L if there is no nontrivial relation

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

  as a function on G.

1. Show that if $\chi_1, \dots, \chi_n$ are distinct characters of G with values in L, then they are linearly independent over L.
2. Show that if $\sigma_1, \dots, \sigma_n$ 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 $\mathrm{Aut}(L)$.
   (c) K is the fixed field of $\mathrm{Aut}(L/K)$.

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 $\operatorname{ord}(a) = m$ 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 $(1+2^2)^{2^{e-3}} \not\equiv 1 \pmod{2^e}$.
2. If each Sylow p-subgroup of G is normal, then G is isomorphic to the product of all sylow p-subgroups.

Ex 5.4.

(a) 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 $\operatorname{Gal}(L/\mathbb{C}(t))$.

(b) Let $\mathbb{F}_p(t)$ be the field of rational functions over $\mathbb{F}_p$ and L be a splitting field of $x^3 - 2t$ over $\mathbb{F}_p(t)$. Find $\operatorname{Gal}(L/\mathbb{F}_p(t))$.

Ex 5.5. Let $\operatorname{char} K \neq 2, 3$ 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 $G_f = \operatorname{Gal}(L/K) \leq S_4$. Set $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$.

(a) Show that $L^{G_f \cap V} = K(\beta_1, \beta_2, \beta_3)$ and $\operatorname{Gal}(K(\beta_1, \beta_2, \beta_3)/K) \cong G_f / G_f \cap V$ where $V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \leq S_4$.

(b) Show that there exists i s.t. $\beta_i \in K \iff G_f \leq D_4$.

(c) Let $h(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3) \in K[x]$ with discriminant $D(h)$, Show that

  (1) If $h(x)$ is irr. and $D(h) \notin K^2$, then $G_f \cong S_4$.

  (2) If $h(x)$ is irr. and $D(h) \in K^2$, then $G_f \cong A_4$.

  (3) If $h(x)$ splits completely in $K[x]$, then $G_f \cong V$.

  (4) 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 $G_f \cong C_4$.

6 Week 6

Ex 6.1. Is $f(x) = 2x^5 - 10x + 5 \in \mathbb{Q}[x]$ solvable by radicals? Justify your answer!

Ex 6.2. Show that if $|G| = p^2q$ where p, q are distinct primes, then G is solvable.

Ex 6.3. Solve $x^4 + ax + b = 0$ in terms of radicals.

Ex 6.4. power sum: $p_k = \sum_{i=1}^{n} x_i^k$. show that newton identities: $s_0 = 1$,

$$ks_k = \sum_{i=1}^{k} (-1)^{i-1} s_{k-i} p_i, \qquad p_k = \sum_{i=1}^{k-1} (-1)^{i+k-1} s_{k-i} p_i + (-1)^{k-1} k s_k$$

(s_k are the elementary symmetric polynomials in $x_1, \ldots, x_n$.)

Ex 6.5. For any prime $p \geq 5$. Let $k, m, n_1, \ldots, n_{k-2} \in \mathbb{Z}$ s.t.

$$\begin{cases} k \text{ is odd and } > 3, \\ m \text{ is even and } > 0, \\ n_1, \ldots, n_{k-2} \text{ are even and } n_1 < n_2 < \cdots < n_{k-2}. \end{cases}$$

Consider $g(x) = (x^2 + m)(x - n_1) \ldots (x - n_{k-2})$ and $f(x) = g(x) - 2 \in \mathbb{Z}[x]$.

1. Show that f is irr. in $\mathbb{Z}[x]$
2. Show that f has exactly two non-real roots for $m \gg 0$. If $k = p$, then $G_f \cong S_p$.

7 Week 7

Ex 7.1.

1. Let $\alpha_1, \dots, \alpha_n$ be roots of $f(x)$ and then

$$\delta = \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{vmatrix}$$

   Show that

$$D = \begin{vmatrix} n & p_1 & \dots & p_{n-1} \\ p_1 & p_2 & \dots & p_n \\ \vdots & \vdots & \ddots & \vdots \\ p_{n-1} & p_n & \dots & p_{2n-2} \end{vmatrix}, \quad p_i = \sum_{k=1}^{n} \alpha_k^i$$

2. If $f(x) = x^n + px + q$, then $D = y_{n+1} n^n q^{n-1} + y_n (n-1)^{n-1} p^n$, where

$$y_n = \begin{cases} 1, & n \equiv 1, 2 \pmod 4 \\ -1, & n \equiv 0, 3 \pmod 4 \end{cases}$$

Ex 7.2. A transitive subgroup G of S_n containing a transposition and an $(n-1)$-cycle is S_n.

Ex 7.3.

1. If $f(x) = x^5 - x - 1$, then $G_f \cong S_5$.
2. If $f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$, then $G_f \cong \mathbb{Z}/5\mathbb{Z}$.

8 Week 8

Ex 8.1. Use Zorn's lemma to show the existence of a transcendence base S of any extension L/K. (S may equal to $\emptyset$)

Ex 8.2. Given $L/M, M/K$, show that $\operatorname{tr}\deg_K L = \operatorname{tr}\deg_M L + \operatorname{tr}\deg_K M$.

Ex 8.3. Show that for any extension L/K, $\mathrm{Tr} : L \to K$ is surjective.

Ex 8.4. If L/K with $|L| < \infty$, show that $\mathrm{N}_{L/K} : L^\times \to K^\times$ is also surjective.

9 Week 9

Ex 9.1.

1. ED $\implies$ PID.
2. ED $\implies$ GCD domain.

Ex 9.2. A_{-19} is a PID but not a ED.

10 Week 10

Ex 10.1.

1. If $\sqrt{I}$ is a maximal ideal, then I is primary.
2. A power of a maximal ideal is m-primary.

Ex 10.2.

Def 2. The Jacobson radical of R is the intersection of all maximal ideals of R and is denoted by $\operatorname{Jac} R$.

Show that $x \in \operatorname{Jac} R \iff 1 - rx$ is a unit $\forall\, r \in R$.

Ex 10.3.

1. Show that if M is a finitely generated R-module and $IM = M$ with $I \subseteq \operatorname{Jac} R$, then $M = 0$.
2. Show that if M is a finitely generated R-module, N is a submodule of M and $I \subseteq \operatorname{Jac} R$, then
$$M = IM + N \implies M = N.$$

Ex 10.4.

1. $V_1 \subseteq V_2 \iff \mathcal{I}(V_1) \supseteq \mathcal{I}(V_2)$.
2. $\mathcal{I}(V_1 \cup V_2) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$.
3. $V_1 \cup V_2 = \mathcal{V}(\mathcal{I}(V_1)\mathcal{I}(V_2))$.
4. $\bigcap\limits_{\lambda\in\Lambda} V_\lambda = \mathcal{V}\left(\sum\limits_{\lambda\in\Lambda} \mathcal{I}(V_\lambda)\right)$.
5. V is irr. $\iff \mathcal{I}(V) \in \operatorname{Spec} k[x_1, \ldots, x_n]$.

Ex 10.5.

1. $f(\alpha) \in W \quad \forall\, \alpha \in V$.
2. $\varphi = f^*$.
3. For different representations of R, $R \cong k[x_1, \ldots, x_n]/I_1 \underset{\Psi^{-1}}{\overset{\Psi}{\cong}} k[z_1, \ldots, z_l]/I_2$ and $\begin{cases} V_1 = \mathcal{V}(I_1) \\ V_2 = \mathcal{V}(I_2) \end{cases}$.

   Show that Ψ (and Ψ^{-1}) will give an isom. of V_1 and V_2.

Ex 10.6.

1. Show that if $V = \mathcal{V}(y - x^2) \subseteq \mathbb{A}^2_{\mathbb{C}}$, then
$$\begin{aligned} f : \mathbb{A}^1_{\mathbb{C}} &\to V \\ t &\mapsto (t, t^2) \end{aligned} \quad \text{is an isom.}$$

2. Show that if $V = \mathcal{V}(y^2 - x^3) \subseteq \mathbb{A}^2_{\mathbb{C}}$, then
$$\begin{aligned} f : \mathbb{A}^1_{\mathbb{C}} &\to V \\ t &\mapsto (t^2, t^3) \end{aligned} \quad \text{is bijective but not an isom.}$$

11 Week 11

Ex 11.1.

(a) Show that $\{ y - x^2, z - x^3 \}$ is not a Gröbner basis for $x > y > z$.

(b) Find a Gröbner basis for $\langle y - x^2, z - x^3 \rangle$.

Ex 11.2.

(a) Find a Gröbner basis of $I = \langle -x^3 + y, x^2y - y^2 \rangle$.

(b) Check $x^6 - x^5y \overset{?}{\in} I$.

Def 3.

- A Gröbner basis $G = \{ g_1, \dots, g_m \}$ of I is said to be minimal if $\mathrm{LT}(g_i)$ is monic for all i and $\forall\, j, \quad \mathrm{LT}(g_i) \notin \langle \mathrm{LT}(G \setminus \{ g_j \}) \rangle$.
- A minimal Gröbner basis $G = \{ g_1, \dots, g_m \}$ is said to be reduced if for all j, no term in g_j is divisible by any of $\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_{j-1}), \mathrm{LT}(g_{j+1}), \dots, \mathrm{LT}(g_m)$.

Ex 11.3.

1. Show that for a given monomial ordering, every non-zero ideal I in $k[x_1, \dots, x_n]$ has a unique reduced Gröbner basis.
2. Show that $I = \langle x^2y + xy^2 - 2y, x^2 + xy - x + y^2 - 2y, xy^2 - x - y + y^3 \rangle$ and $J = \langle x - y^2, xy - y, x^2 - y \rangle$ are equal.

Ex 11.4. Let $I = \langle x^2 + xy^5 + y^4, xy^6 - xy^3 + y^5 - y^2, xy^5 - xy^2 \rangle, x > y$. Find the reduced Gröbner basis of I.

Ex 11.5.

1. $\left(I : \left(\sum_{i=1}^{r} J_i \right) \right) = \bigcap_{i=1}^{r} (I : J_i)$. Here, $(I : J) \triangleq \{ x \in R \mid xJ \subseteq I \}$.
2. $\left(\bigcap_{i=1}^{r} I_i : J \right) = \bigcap_{i=1}^{r} (I_i : J)$.
3. $\big((I_1 : I_2) : I_3 \big) = (I_1 : I_2 I_3)$.

12 Week 12

Ex 12.1. The following sets are correspondent:

(1) V (an affine algebraic set)

(2) $\operatorname{Max} k[V]$

(3) $\operatorname{Hom}_k(k[V], k)$

Def 4. Let S/R be an extension of rings and $I \subseteq R$ be an ideal. $a \in S$ is said to be integral over I if $\exists\, f(x) = x^n + r_1 x^{n-1} + \cdots + r_n$ with $n > 0$ and $r_i \in I$ s.t. $f(a) = 0$.

Ex 12.2. Let $a \in S$. Show that TFAE

(1) a is integral over I.

(2) $R[a]$ is a finitely generated R-module and $a \in \sqrt{IR[a]}$. Here $IR[a]$ is an ideal in $R[a]$ generated by I.

(3) There exists a subring S' of S (with $R[a] \subset S'$) s.t. S' is a finitely generated R-module and $a \in \sqrt{IS'}$.

Ex 12.3. Show that $\sqrt{I\bar{R}} = \{\, a \in S \mid a \text{ is integral over } I \,\}$ where $\bar{R}$ is the integral closure of R in S.

Ex 12.4. If $\phi : R_1 \to R_2$ is a ring homomorphism and $p \in \operatorname{Spec} R_1$, then

$$p = \phi^{-1}(q) \text{ for some } q \in \operatorname{Spec} R_2 \iff p = \phi^{-1}(R_2\phi(p))$$

Ex 12.5. In a UFD R, $\forall\, p \in \operatorname{Spec} R$ with $h(p) = 1$, $p = \langle \alpha \rangle$ for some prime element $\alpha \in R$.

13 Week 13

Ex 13.1. Let $0 \to N \to M \to L \to 0$ be exact in $\mathbf{Mod}_R$. Show that N, L are Artinian (Noetherian) $\iff$ M is Artinian (Noetherian).

Ex 13.2. Let R be an Artinian local ring with maximal ideal $\mathfrak{m}$, then TFAE:

1. R is a PID
2. $\mathfrak{m}$ is principal
3. $\dim_{R/\mathfrak{m}} \left(\mathfrak{m}/\mathfrak{m}^2\right) \leq 1$

Ex 13.3. (Krull's Intersection Theorem) Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$, show that

$$\bigcap_{n=0}^{\infty} \mathfrak{m}^n = \langle 0 \rangle.$$

Ex 13.4. Let R be a Dedekind domain, $I, J \subseteq R$ and $\begin{cases} I = P_1^{e_1} P_2^{e_2} \cdots P_n^{e_n} \\ J = P_1^{f_1} P_2^{f_2} \cdots P_n^{f_n} \end{cases}$, $e_i, f_j \geq 0$. Show that

1. $I \subseteq J \iff J \mid I \iff f_i \leq e_i$.
2. $I + J = \langle I, J \rangle = P_1^{d_1} P_2^{d_2} \cdots P_n^{d_n}$ where $d_i = \min\{f_i, e_i\}$.

Ex 13.5. Let R be a Dedekind domain, $I \subseteq R$ and $I = P_1^{e_1} P_2^{e_2} \cdots P_n^{e_n}$. Show that

1. $\exists\, J \subseteq R$ with $I + J = R$ s.t. $IJ = \langle a \rangle$ for some $a \in R$.
2. $I \subseteq R \implies R/I$ is a principal ring.
3. $I \subseteq R$, let $a \in I$ with $a \neq 0$. $\implies I = \langle a, b \rangle$ for some $b \in I$.