DISCUSSION AND PROBLEM SESSION

1. Discussion and Problem sessions 1

For a field extension E of F, we let $\mathrm{Aut}_F(E)$ be the set of all F-isomorphims from E to E.

1.1. Some of the previous topics.

1. Suppose E is an extension field of F and $\alpha \in E$ is algebraic over F. Suppose n is a positive integer, $\gcd([F[\alpha] : F], n!) = 1$, and $f(x) \in F[x]$ is of degree n. Prove that $F[\alpha] = F[f(\alpha)]$.

2. Suppose F is a field, $f(x) \in F[x]$ is irreducible, and E is a splitting field of $f(x)$ over F. Suppose there is $\alpha \in E$ such that
$$f(\alpha) = f(\alpha + 1) = 0.$$
Prove that $\mathrm{Aut}_F(E)$ has an element of order p.

3. Suppose p is a prime which does not divide n. Let $\Phi_n(x)$ be the n-th cyclotomic polynomial and view it as an element of $\mathbb{Z}_p[x]$. Suppose $E_{n,p}$ is a splitting field of Φ_n over $\mathbb{Z}_p$.
   (a) Suppose $\alpha \in E_{n,p}$ is a zero of Φ_n. Prove that $E_{n,p} = \mathbb{Z}_p[\alpha]$.
   (b) Prove that $\mathrm{Aut}_{\mathbb{Z}_p}(E_{n,p})$ is isomorphic to the subgroup of $\mathbb{Z}_n^\times$ which is generated by $[p]_n$.
   (c) Prove that all the irreducible factors of $\Phi_n(x)$ in $\mathbb{Z}_p[x]$ have the same degree and they are equal to the multiplicative order of p modulo n.

2. Discussion and Problem sessions 2

2.1. Field of rational functions.

1. Suppose F is a field. Let
$$F(t) := \left\{ \frac{f(t)}{g(t)} \mid f, g \in F[t] \right\}$$
be the field of fractions of $F[t]$. Suppose $u := \frac{f}{g} \notin F$ with $f, g \in F[t]$ and $\gcd(f, g) = 1$. Let $K := F(u)$ be the smallest subfield of $L := F(t)$ which contains F and u.
   (a) Consider $p(x) := ug(x) - f(x) \in K[x]$. Argue that t is a zero of p. Deduce that L/K is a finite extension.
   (b) Argue that $\deg p = \max\{\deg f, \deg g\}$.
   (c) Argue that p is irreducible in $F(x)[u]$.
   (d) Notice that p is a primitive element of $F(x)[u]$ and deduce that p is irreducible in $F[x][u]$.
   (e) Show that p is irreducible in $K[x]$.
   (f) Prove that $[F(t) : F(u)] = \max\{\deg f, \deg g\}$.

2. Suppose F is a field and $\theta \in \mathrm{Aut}_F(F(t))$. Prove that there is $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(F)$ such that
$$\theta(t) = \frac{at + b}{ct + d}.$$

3. Prove that $\mathrm{Aut}_F(F(t)) \simeq \mathrm{PGL}_2(F)$ where $\mathrm{PGL}_2(F) = \mathrm{GL}_2(F)/F^{\times}I$.

2.2. Automorphisms of a field extension and permutation groups.

1. Suppose $f \in F[x]$ is a non-constant polynomial and E is a splitting field of f over F. Let $R := \{\alpha_1, \ldots, \alpha_n\}$ be the set of zeros of f in E. Prove that $\mathrm{Aut}_F(E)$ can be embedded into the symmetric group S_n.
2. Suppose $f \in \mathbb{Q}[x]$ is an irreducible polynomial of prime degree p which has exactly two complex zeros. Let $E \subseteq \mathbb{C}$ be a splitting field of f over $\mathbb{Q}$. Prove that $\mathrm{Aut}_{\mathbb{Q}}(E)$ can be identified with a subgroup G of the symmetric group S_p such that
$$(1, 2, \ldots, p) \in G \text{ and } (1, a) \in G$$
for some $a \in \{2, \ldots, p\}$.

3. Discussion and Problem sessions 3

3.1. Automorphisms of a field extension and permutation groups.

1. Suppose $f \in F[x]$ is a non-constant polynomial and E is a splitting field of f over F. Let $R := \{\alpha_1, \ldots, \alpha_n\}$ be the set of zeros of f in E. Prove that $\mathrm{Aut}_F(E)$ can be embedded into the symmetric group S_n.
2. Suppose $f \in \mathbb{Q}[x]$ is an irreducible polynomial of prime degree p which has exactly two complex non-real zeros. Let $E \subseteq \mathbb{C}$ be a splitting field of f over $\mathbb{Q}$. Prove that $\mathrm{Aut}_{\mathbb{Q}}(E)$ can be identified with a subgroup G of the symmetric group S_p such that
$$(1, 2, \ldots, p) \in G \text{ and } (1, a) \in G$$
for some $a \in \{2, \ldots, p\}$.

3.2. Fundamental Theorem of Galois Theory.

1. Consider the extension $\mathbb{Q}[\zeta_3, \sqrt[3]{2}]/\mathbb{Q}$.
   (a) Give an isomorphism $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_3, \sqrt[3]{2}]) \simeq S_3$.
   (b) Use your isomorphism and the Galois correspondence to write down every intermediate subfield of $\mathbb{Q}[\zeta_3, \sqrt[3]{2}]/\mathbb{Q}$.
   (c) Determine which intermediate subfields are Galois over $\mathbb{Q}$.
2. Prove any intermediate subfield of $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ is Galois over $\mathbb{Q}$.
3. Suppose E/F is a finite (not necessarily Galois) extension. Define Ψ and Φ as in the fundamental theorem of Galois theory, i.e.
$$\Psi : \mathrm{Int}(E/F) \to \mathrm{Sub}(\mathrm{Aut}_F(E)), \quad \Psi(K) := \mathrm{Aut}_K(E), \qquad \text{and}$$
$$\Phi : \mathrm{Sub}(\mathrm{Aut}_F(E)) \to \mathrm{Int}(E/F), \quad \Phi(G) := \mathrm{Fix}(G).$$
   (a) Prove in this generality one still has $\Psi \circ \Phi = \mathrm{id}$, so Φ is injective and Ψ is surjective.
   (b) Prove $\mathrm{Im}(\Phi) = \{K \in \mathrm{Int}(E/F) \mid E/K \text{ is Galois}\}$.

4. Discussion and Problem sessions 4

4.1. Fundamental Theorem of Galois Theory.

1. Prove any intermediate subfield of $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ is Galois over $\mathbb{Q}$.

2. Suppose E/F is a finite (not necessarily Galois) extension. Define Ψ and Φ as in the fundamental theorem of Galois theory, i.e.

$$\begin{aligned} &\Psi : \mathrm{Int}(E/F) \to \mathrm{Sub}(\mathrm{Aut}_F(E)), \quad \Psi(K) := \mathrm{Aut}_K(E), \qquad \text{and} \\ &\Phi : \mathrm{Sub}(\mathrm{Aut}_F(E)) \to \mathrm{Int}(E/F), \quad \Phi(G) := \mathrm{Fix}(G). \end{aligned}$$

   (a) Prove in this generality one still has $\Psi \circ \Phi = \mathrm{id}$, so Φ is injective and Ψ is surjective.
   (b) Prove $\mathrm{Im}(\Phi) = \{K \in \mathrm{Int}(E/F) \mid E/K \text{ is Galois}\}$.

4.2. **Separable closure and purely inseparable extensions.**

1. Suppose E/F is a field extension and $K \in \mathrm{Int}(E/F)$. Prove that E/F is purely inseparable if and only if E/K and K/F are purely inseparable.

4.3. **Galois group of polynomials.**

1. Suppose $f \in F[x]$ is a separable irreducible polynomial of degree n, K is a splitting field of f over F, and consider the action of $\mathrm{Aut}_F(K)$ on the set of zeros X of f in K. Prove that $\mathrm{Aut}_F(K)$ acts transitively on X; that means for every $x, x' \in X$ there is $\theta \in \mathrm{Aut}_F(K)$ such that $\theta(x) = x'$. Prove that n divides $|\mathrm{Aut}_F(K)|$.
2. Suppose $f \in F[x]$ does not have multiple zeros in a splitting field K over F, and consider the action of $\mathrm{Aut}_F(K)$ on the set of zeros X of f in K. Prove that number of $\mathrm{Aut}_F(K)$-orbits in X is the same as the number of irreducible factors of f in $F[x]$.

5. Discussion and Problem sessions 5

5.1. **compositum.** Let Ω/F be a field extension and E, K be intermediate subfields. We define the *compositum* of E and K in Ω, denoted EK, to be the smallest subfield of Ω containing both E and K, i.e. the intersection of all subfields of Ω containing both E and K.

1. Suppose K/F is finite, say $K = F[\beta_1, \dots, \beta_m]$. Write $F_i = F[\beta_1, \dots, \beta_i]$ and $F_0 = F$, and similarly write $E_i = E[\beta_1, \dots, \beta_i]$ with $E_0 = E$. Prove that $[E_{i+1} : E_i] \le [F_{i+1} : F_i]$ for each $i \in [0, m-1]$, and conclude that EK/E is finite with $[EK : E] \le [K : F]$.
2. Conclude if E/F and K/F are both finite then EK/F is finite with $[EK : F] \le [E : F][K : F]$.
3. Prove if E/F and K/F are both finite and $\gcd([E : F], [K : F]) = 1$, then $[EK : F] = [E : F][K : F]$.
4. Prove if E/F and K/F are both finite normal (resp. finite separable) then EK/F is also normal (resp. separable).
5. Prove if K/F is finite Galois then EK/E and $K/E \cap K$ are both finite Galois, and that we have an isomorphism $\mathrm{Aut}_E(EK) \to \mathrm{Aut}_{E\cap K}(K)$ via restriction.
6. Suppose E/F and K/F are both finite Galois, as then is EK/F. Show we have an injective homomorphism $\mathrm{Aut}_F(EK) \to \mathrm{Aut}_F(E) \times \mathrm{Aut}_F(K)$ sending $\sigma \mapsto (\sigma|_E, \sigma|_K)$. Prove if $E \cap K = F$ then this map is an isomorphism.

5.2. **Solvability by radicals.**

1. Prove that $f(x) = 2x^5 - 10x + 5$ is not solvable by radicals over $\mathbb{Q}$.
2. Prove that every polynomial of degree at most 4 over a characteristic zero field is solvable by radicals.

5.3. **Discriminant.** Suppose F is a field of characteristic 0. For $f \in F[x]$, suppose E is a splitting field of f and $\alpha_i \in E$ are such that

$$f(x) = \mathrm{ld}(f)(x - \alpha_1) \cdots (x - \alpha_n).$$

Let $\Delta_f := \prod_{i<j}(\alpha_i - \alpha_j)$. The discriminant D_f of f is $D_f := \Delta^2$.

1. Prove that $D_f \in F$.
2. Prove that $\Delta_f \in F$ if and only if $\mathcal{G}_{f,F}$ is a subgroup of the alternating group.

6. Discussion and Problem sessions 6

6.1. Solvability by radicals.

1. Prove that $f(x) = 2x^5 - 10x + 5$ is not solvable by radicals over $\mathbb{Q}$.
2. Prove that every polynomial of degree at most 4 over a characteristic zero field is solvable by radicals.

6.2. Discriminant.

Suppose F is a field of characteristic 0. For $f \in F[x]$, suppose E is a splitting field of f and $\alpha_i \in E$ are such that

$$f(x) = \mathrm{ld}(f)(x - \alpha_1) \cdots (x - \alpha_n).$$

Let $\Delta_f := \prod_{i<j}(\alpha_i - \alpha_j)$. The discriminant D_f of f is $D_f := \Delta_f^2$.

1. Prove that $D_f \in F$.
2. Prove that $\Delta_f \in F$ if and only if $\mathcal{G}_{f,F}$ is a subgroup of the alternating group.
3. Find D_f where $f(x) = x^3 - px + q$.

6.3. Some Galois groups.

1. Find the Galois group $\mathcal{G}_{f,\mathbb{Q}}$ where $f(x) = x^3 - 4x + 2$. (Hint: use discriminant.)
2. Prove that $\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}$ is a Galois extension and $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.
3. Prove that there is a Galois extension $F/\mathbb{Q}$ such that $\mathrm{Aut}_{\mathbb{Q}}(F) \simeq \mathbb{Z}/p\mathbb{Z}$ where p is a prime.

7. Discussion and Problem sessions 6

Recall:

7.1. Discriminant.

Suppose F is a field of characteristic 0. For $f \in F[x]$, suppose E is a splitting field of f and $\alpha_i \in E$ are such that

$$f(x) = \mathrm{ld}(f)(x - \alpha_1) \cdots (x - \alpha_n).$$

Let $\Delta_f := \prod_{i<j}(\alpha_i - \alpha_j)$. The discriminant D_f of f is $D_f := \Delta_f^2$.

1. Prove that $D_f \in F$.
2. Prove that $\Delta_f \in F$ if and only if $\mathcal{G}_{f,F}$ is a subgroup of the alternating group.
3. Find D_f where $f(x) = x^3 - px + q$. (Answer is $4p^3 - 27q^2$.)

7.2. Some Galois groups.

1. Find the Galois group $\mathcal{G}_{f,\mathbb{Q}}$ where $f(x) = x^3 - 4x + 2$. (Hint: use discriminant.)
2. Prove that $\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}$ is a Galois extension and $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.
3. Prove that there is a Galois extension $F/\mathbb{Q}$ such that $\mathrm{Aut}_{\mathbb{Q}}(F) \simeq \mathbb{Z}/p\mathbb{Z}$ where p is a prime.
4. Prove that $x^p - 4x + 2$ is not solvable by radicals over $\mathbb{Q}$ if p is a prime more than 3.

8. Discussion and Problem sessions 8

1. Suppose E/F be a finite extension and $\overline{F}$ is an algebraic closure of F. Prove that $[E:F]_s$ equals the number of distinct F-embeddings of E into $\overline{F}$.
2. Suppose E/F be a finite separable extension and $\overline{F}$ is an algebraic closure of F. For $\alpha \in E$ define
$$N_{E/F}(\alpha) := \prod_{\sigma \in \mathrm{Embed}_F(E,\overline{F})} \sigma(\alpha).$$
   (a) Prove when E/F is Galois this agrees with the definition of $N_{E/F}$ given in class.
   (b) Prove one still has $N_{E/F}(\alpha) \in F$ for all $\alpha \in E$.
   (c) Prove that $N_{E/F} : E^\times \to F^\times$ is a group homomorphism.
   (d) Prove if $K \in \mathrm{Int}(E/F)$ one has $N_{K/F} \circ N_{E/K} = N_{E/F}$.
3. Let A be a commutative unital ring. Suppose $S \subseteq A$ is multiplicatively close; that means $1 \in S$ and $s_1 s_2 \in S$ for every $s_1, s_2 \in S$. Suppose $I_0 \trianglelefteq A$ and $I_0 \cap S = \varnothing$.
   (a) Let
$$\Sigma_{I_0,S} := \{I \trianglelefteq A \mid I_0 \subseteq I, I_0 \cap S = \varnothing\}.$$
   Prove that Σ has a maximal element with respect to inclusion.
   (b) Suppose P is a maximal element of $\Sigma_{I_0,S}$. Prove that P is a prime ideal.
4. Let A be a commutative unital ring. Prove that the set of nilpotent elements of A is precisely the intersection of all prime ideals of A. [Hint: if $a \in A$ is not nilpotent,consider $S_a := \{1, a, a^2, \ldots\}$ and the previous problem.]

9. Discussion and Problem sessions 9

9.1. Separable extensions and embeddings.

1. Suppose E/F be a finite extension and $\overline{F}$ is an algebraic closure of F. Prove that $[E:F]_s$ equals the number of distinct F-embeddings of E into $\overline{F}$. (This part we discussed in length in the previous session.)
2. Suppose E/F be a finite separable extension and $\overline{F}$ is an algebraic closure of F. For $\alpha \in E$ define
$$N_{E/F}(\alpha) := \prod_{\sigma \in \mathrm{Embed}_F(E,\overline{F})} \sigma(\alpha).$$
   (a) Prove when E/F is Galois this agrees with the definition of $N_{E/F}$ given in class.
   (b) Prove one still has $N_{E/F}(\alpha) \in F$ for all $\alpha \in E$.
   (c) Prove that $N_{E/F} : E^\times \to F^\times$ is a group homomorphism.
   (d) Prove if $K \in \mathrm{Int}(E/F)$ one has $N_{K/F} \circ N_{E/K} = N_{E/F}$.
3. Let A be a commutative unital ring. Suppose $S \subseteq A$ is multiplicatively close; that means $1 \in S$ and $s_1 s_2 \in S$ for every $s_1, s_2 \in S$. Suppose $I_0 \trianglelefteq A$ and $I_0 \cap S = \varnothing$.
   (a) Let
$$\Sigma_{I_0,S} := \{I \trianglelefteq A \mid I_0 \subseteq I, I \cap S = \varnothing\}.$$
   Prove that Σ has a maximal element with respect to inclusion.
   (b) Suppose P is a maximal element of $\Sigma_{I_0,S}$. Prove that P is a prime ideal.
4. Let A be a commutative unital ring. Prove that the set of nilpotent elements of A is precisely the intersection of all prime ideals of A. [Hint: if $a \in A$ is not nilpotent,consider $S_a := \{1, a, a^2, \ldots\}$ and the previous problem.]

10. Discussion and Problem sessions 10

10.1. **Separable extensions and embeddings.**

1. Suppose $\overline{F}$ is an algebraic closure of F and $E \in \mathrm{Int}(\overline{\mathrm{F}}/F)$ is a separable extension of F. Prove if $K \in \mathrm{Int}(E/F)$ one has $N_{K/F} \circ N_{E/K} = N_{E/F}$.

11. Discussion and Problem sessions 11

11.1. **Gauss sum, cyclotomic extensions, and quadratic reciprocity.** Suppose p is an odd prime and $\zeta_p := e^{\frac{2\pi i}{p}}$.

(a) Prove that there is a surjective group homomorphism $\chi_0 : \mathbb{Z}_p^\times \to \{\pm 1\}$. Show that $\chi_0(a) = 1$ is $a = b^2$ for some $b \in \mathbb{Z}_p^\times$ and $\chi_0(a) = -1$ if there is no $b \in \mathbb{Z}_p^\times$ such that $a = b^2$. We often use Legendre symbol and write $\chi(a) = (\frac{a}{p})$.
(b) Let $g_p := \sum_{a \in \mathbb{Z}_p^\times} \chi(a)\zeta_p^a$. For $a \in \mathbb{Z}_p^\times$, let $\theta_a \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_p])$ be such that $\theta_a(\zeta_p) = \zeta_p^a$. Prove that for every $a \in \mathbb{Z}_p^\times$, $\theta_a(g_p) = (\frac{a}{p})g_p$.
(c) Let $K := \mathrm{Fix}(\{\theta_a \mid a \in \ker \chi\})$. Prove that K is the unique quadratic extension of $\mathbb{Q}$ in $\mathrm{Int}(\mathbb{Q}[\zeta_p]/\mathbb{Q})$ and $K = \mathbb{Q}[g_p]$.
(d) Prove that $g_p = \sum_{i \in \mathbb{Z}_p} \zeta_p^{i^2}$.
(e) Use $\sum_{a \in \mathbb{Z}_p^\times} \theta_a(g_p)\theta_{-a}(g_p)$ to prove that $g_p^2 = (\frac{-1}{p})p$. (Notice that $\sum_{a \in \mathbb{Z}_p} \zeta_p^{ia} = [i = 0]p$ where $[i = 0]$ is 1 if $i = 0$ and 0 if $i \neq 0$.)
(f) Suppose q is an odd prime. Use the fact that $\mathbb{Z}_q^\times$ is cyclic to prove that for every $a \in \mathbb{Z}$ with $\gcd(a, q) = 1$, we have that $a^{\frac{q-1}{2}} = (\frac{a}{q})$ modulo q.
(g) Prove that g_p^{q-1} is equal to $(\frac{-1}{p})^{\frac{q-1}{2}} p^{\frac{q-1}{2}}$ in the quotient ring $\mathbb{Z}[\zeta_p]/\langle q \rangle$; and so $g_p^{q-1} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} (\frac{p}{q})$ modulo q. In particular, g_p in $\mathbb{Z}[\zeta_p]/\langle q \rangle$ is a unit and $g_p^q = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} (\frac{p}{q}) g_p$ modulo q.
(h) Use the fact that $\mathbb{Z}[\zeta_p]/\langle q \rangle$ has characteristic q to show $g_p^q = \theta_q(g_p)$ modulo q.
(i) (Quadratic reciprocity) Prove that $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.
(j) (Very special case of Kronecker-Weber theorem) Suppose $F \subseteq \mathbb{C}$ is a quadratic extension of $\mathbb{Q}$. Prove that there is a positive integer n such that $F \subseteq \mathbb{Q}[\zeta_n]$.

12. Discussion and Problem sessions 12

12.1. **Gauss sum, cyclotomic extensions, and quadratic reciprocity.** Suppose p is an odd prime and $\zeta_p := e^{\frac{2\pi i}{p}}$. (we have already discussed the first 4 parts and part (f).)

(a) Prove that there is a surjective group homomorphism $\chi_0 : \mathbb{Z}_p^\times \to \{\pm 1\}$. Show that $\chi_0(a) = 1$ is $a = b^2$ for some $b \in \mathbb{Z}_p^\times$ and $\chi_0(a) = -1$ if there is no $b \in \mathbb{Z}_p^\times$ such that $a = b^2$. We often use Legendre symbol and write $\chi(a) = (\frac{a}{p})$.
(b) Let $g_p := \sum_{a \in \mathbb{Z}_p^\times} \chi(a)\zeta_p^a$. For $a \in \mathbb{Z}_p^\times$, let $\theta_a \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_p])$ be such that $\theta_a(\zeta_p) = \zeta_p^a$. Prove that for every $a \in \mathbb{Z}_p^\times$, $\theta_a(g_p) = (\frac{a}{p})g_p$.
(c) Let $K := \mathrm{Fix}(\{\theta_a \mid a \in \ker \chi\})$. Prove that K is the unique quadratic extension of $\mathbb{Q}$ in $\mathrm{Int}(\mathbb{Q}[\zeta_p]/\mathbb{Q})$ and $K = \mathbb{Q}[g_p]$.
(d) Prove that $g_p = \sum_{i \in \mathbb{Z}_p} \zeta_p^{i^2}$.
(e) Use $\sum_{a \in \mathbb{Z}_p^\times} \theta_a(g_p)\theta_{-a}(g_p)$ to prove that $g_p^2 = (\frac{-1}{p})p$. (Notice that $\sum_{a \in \mathbb{Z}_p} \zeta_p^{ia} = [i = 0]p$ where $[i = 0]$ is 1 if $i = 0$ and 0 if $i \neq 0$.)
(f) Suppose q is an odd prime. Use the fact that $\mathbb{Z}_q^\times$ is cyclic to prove that for every $a \in \mathbb{Z}$ with $\gcd(a, q) = 1$, we have that $a^{\frac{q-1}{2}} = (\frac{a}{q})$ modulo q.

(g) Prove that g_p^{q-1} is equal to $(\frac{-1}{p})^{\frac{q-1}{2}} p^{\frac{q-1}{2}}$ in the quotient ring $\mathbb{Z}[\zeta_p]/\langle q\rangle$; and so $g_p^{q-1} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}(\frac{p}{q})$ modulo q. In particular, g_p in $\mathbb{Z}[\zeta_p]/\langle q\rangle$ is a unit and $g_p^q = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}(\frac{p}{q})g_p$ modulo q.

(h) Use the fact that $\mathbb{Z}[\zeta_p]/\langle q\rangle$ has characteristic q to show $g_p^q = \theta_q(g_p)$ modulo q.

(i) (Quadratic reciprocity) Prove that $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

(j) (Very special case of Kronecker-Weber theorem) Suppose $F \subseteq \mathbb{C}$ is a quadratic extension of $\mathbb{Q}$. Prove that there is a positive integer n such that $F \subseteq \mathbb{Q}[\zeta_n]$.

13. Discussion and Problem sessions 13

13.1. Gauss sum, cyclotomic extensions, and quadratic reciprocity.

1. (Very special case of Kronecker-Weber theorem) Suppose $F \subseteq \mathbb{C}$ is a quadratic extension of $\mathbb{Q}$. Prove that there is a positive integer n such that $F \subseteq \mathbb{Q}[\zeta_n]$.

13.2. Determinant. For this part, we go over some of the HW assignments for week 8 and use them for the following problems.

1. Suppose R is a unital commutative ring. Prove that $X \in \mathrm{GL}_n(R)$ (that means $X \in \mathrm{M}_n(R)$ is a unit) if and only if $\det(X) \in R^\times$.
2. Suppose R is a ring with only one maximal ideal M. Suppose $f : R^n \to R^n$ is a surjective R-module homomorphism and $f(\mathbf{e}_j) = \sum_{i=1}^n f_{ij}\mathbf{e}_i$. Prove that $[f_{ij}] \in \mathrm{GL}_n(R)$. Deduce that f is an isomorphism. (Recall that $R^\times = R \setminus M$.)
3. Suppose R is a unital commutative ring, $A \in \mathrm{M}_n(R)$, and $A = [a_{ij}]$.
   (a) Consider the following scalar product $R[x] \times R^n \to R^n$,
   $$(\sum_{s=0}^m c_s x^s) \cdot v := \sum_{s=0}^m c_s (A)^s v,$$
   where A is the transpose of A. Convince yourself that $V := R^n$ is an $R[x]$-module with respect to the above scalar multiplication. Notice that
   $$x \cdot \mathbf{e}_j = \sum_{i=1}^n a_{ij}\mathbf{e}_i.$$
   Try to understand the following equation:
   $$\begin{pmatrix} x - a_{11} & -a_{21} & \cdots & -a_{n1} \\ -a_{12} & x - a_{22} & \cdots & -a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{1n} & -a_{2n} & \cdots & x - a_{nn} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \\ \vdots \\ \mathbf{e}_n \end{pmatrix} = 0. \tag{1}$$
   (b) Use the previous part and deduce that
   $$\mathrm{adj}(xI - A^T) \cdot ((xI - A^T) \cdot \begin{pmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \\ \vdots \\ \mathbf{e}_n \end{pmatrix}) = 0,$$
   where A^T is the transpose A.
   (c) Prove that $\det(xI - A^T) \cdot \mathbf{e}_i = 0$ for every i.
   (d) Prove that $f(A^T) = 0$ where $f(x) := \det(xI - A)$, and deduce that $f(A) = 0$ as well.

14. Discussion and Problem sessions 14

14.1. **Determinant.** A few remarks on the Caley-Hamilton theorem based on the questions and discussions with some of the students during the previous session:

Suppose R is a unital commutative ring and $A \in \mathrm{M}_n(R)$. Let $f_A(x) := \det(xI - A) \in R[x]$ be the characteristic polynomial of A. In the lecture using a rational canonical form of A and in the previous Discussion and Problem session using an $R[x]$-module structure of R^n which comes out of multiplication by A we proved the Cayley-Hamilton theorem which states that $f_A(A) = 0$.

Here is one way of understanding this equation: let S be the subring of $\mathrm{M}_n(R)$ which is generated by R and the matrix A. This means S is the image of the evaluation map $\phi_A : R[x] \to \mathrm{M}_n(R)$. This ring is denoted by $R[A]$. Notice that $S := R[A]$ is a unital commutative ring which has R as a subring. Suppose $A = [a_{ij}] \in \mathrm{M}_n(R)$ and consider the following matrix in $\mathrm{M}_n(S)$:

$$B := \begin{pmatrix} A - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & A - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & A - a_{nn} \end{pmatrix}$$

The Cayley-Hamilton theorem states that $\det B = 0$. Notice that determinant of the above matrix and its transpose are the same, it is the same as what we have in (1) evaluated at $x = A$.

We can view B as an n^2-by-n^2 matrix with entries in R. In this case, we are having diagonal blocks of A subtracting by a block matrix where the (i,j)-block is a scalar matrix given by a_{ij}. Starting with two square matrices $X := [x_{ij}] \in \mathrm{M}_n(R)$ and $Y := [y_{ij}] \in \mathrm{M}_m(R)$, we can create a new one in $\mathrm{M}_{nm}(R)$ using X as a block and multiplying it by entries of Y:

$$X \otimes Y := \begin{pmatrix} y_{11}X & \cdots & y_{1n}X \\ \vdots & \ddots & \vdots \\ y_{n1}X & \cdots & y_{nn}X \end{pmatrix}.$$

With this notation, $B = A \otimes I - I \otimes A$. This does not quite help us get an easier proof of the Caley-Hamilton theorem, but it might give us more insight on the involved subtleties.

14.2. **Module theory.**

1. Suppose R is a unital commutative ring and M is an R-module. Let
$$\mathrm{Ann}_R(M) := \{r \in R \mid \forall m \in M, r \cdot m = 0\}.$$
   (a) Prove that $\mathrm{Ann}_R(M)$ is an ideal of R.
   (b) Let $(a + \mathrm{Ann}(M)) \cdot m := a \cdot m$ for $a \in R$ and $m \in M$. Prove that this is a well-defined operator and M is an $(R/\mathrm{Ann}(M))$-module with respect to this scalar multiplication.
   (c) We say M is a *faithful* R-module if $\mathrm{Ann}_R(M) = 0$. Prove that M is a faithful $R/\mathrm{Ann}_R(M)$-module.
2. Suppose R is a unital commutative ring and M is an R-module which is generated by $m_1, \ldots, m_n$.
   (a) Suppose J is an ideal of R and $JM = M$ where
$$JM := \{\sum_{i=1}^{m} r_i x_i \mid \forall r_i \in J, x_i \in M, m \in \mathbb{Z}^+\}.$$
   Prove that there is $A := [a_{ij}] \in \mathrm{M}_n(J)$ such that
$$m_i = \sum_{j=1}^{n} a_{ij} \cdot m_j,$$

and try to understand the following equation:

$$\begin{pmatrix} 1-a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & 1-a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & 1-a_{nn} \end{pmatrix} \cdot \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

(b) Prove that $\det(I-A) \in \mathrm{Ann}_R(M)$ and $\det(I-A) = 1+a$ for some $a \in J$.
(c) (Nakayama's lemma) Suppose M is a faithful finitely generated R-module, J is an ideal of R, and $JM = M$. Prove that $J = R$.
(d) Suppose M is a finitely generated R-module and for every maximal ideal $\mathfrak{m}$ of R, $\mathfrak{m}M = M$. Prove that $M = 0$.

3. Suppose R has only one maximal ideal $\mathfrak{m}$, and M is a finitely generated R-module.
   (a) Prove that $M/\mathfrak{m}M$ is a finite dimensional vector space over $R/\mathfrak{m}$ with respect to the following scalar multiplication $(r+\mathfrak{m}) \cdot (m+\mathfrak{m}M) := r \cdot m + \mathfrak{m}M$.
   (b) Prove that the minimum number of elements needed to generate M is equal to $\dim_{R/\mathfrak{m}}(M/\mathfrak{m}M)$.

15. Discussion and Problem sessions 15

15.1. Module theory.

1. Suppose R is a unital commutative ring and M is an R-module which is generated by $m_1, \ldots, m_n$.
   (a) Suppose J is an ideal of R and $JM = M$ where

$$JM := \{\sum_{i=1}^{m} r_i x_i \mid \forall r_i \in J, x_i \in M, m \in \mathbb{Z}^+\}.$$

   Prove that there is $A := [a_{ij}] \in \mathrm{M}_n(J)$ such that

$$m_i = \sum_{j=1}^{n} a_{ij} \cdot m_j,$$

   and try to understand the following equation:

$$\begin{pmatrix} 1-a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & 1-a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & 1-a_{nn} \end{pmatrix} \cdot \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

   (b) Prove that $\det(I-A) \in \mathrm{Ann}_R(M)$ and $\det(I-A) = 1+a$ for some $a \in J$.
   (c) (Nakayama's lemma) Suppose M is a faithful finitely generated R-module, J is an ideal of R, and $JM = M$. Prove that $J = R$.
   (d) Suppose M is a finitely generated R-module and for every maximal ideal $\mathfrak{m}$ of R, $\mathfrak{m}M = M$. Prove that $M = 0$.
2. Suppose R has only one maximal ideal $\mathfrak{m}$, and M is a finitely generated R-module.
   (a) Prove that $M/\mathfrak{m}M$ is a finite dimensional vector space over $R/\mathfrak{m}$ with respect to the following scalar multiplication $(r+\mathfrak{m}) \cdot (m+\mathfrak{m}M) := r \cdot m + \mathfrak{m}M$.
   (b) Prove that the minimum number of elements needed to generate M is equal to $\dim_{R/\mathfrak{m}}(M/\mathfrak{m}M)$.

15.2. misc.

1. (Game of Chomps) Suppose there are cookies on the lattice points in the first quarter of the plane; that means $\{(m,n) \in \mathbb{Z}^2 \mid m,n \geq 0\}$. Two players are playing the following game: at players' turn they choose a square (m,n) and eat all the cookies that are located at (m',n') where either $m' \geq m$

or $n' \geq n$. The cookie at $(0,0)$ is poisoned, and the player who eats it immediately loses. Prove that any game of Chomp ends after finitely many moves.

2. Suppose A is a unital commutative ring and I is an ideal of A. Let
$$\sqrt{I} := \{a \in A \mid a^n \in I \text{ for some posistive integer } n\}.$$
   (a) Prove that $\sqrt{I}$ is an ideal of A.
   (b) Prove that $\sqrt{I}$ is the intersection of all the prime ideals of A which contain I.
3. Suppose R is a unital commutative ring and $a_{ij} \in \mathrm{M}_n(R)$. Let S be the subring of $\mathrm{M}_n(R)$ which is generated by R and a_{ij}'s. Suppose S is commutative. Let $A := [a_{ij}]$ and view it both as an element of $\mathrm{M}_k(S)$ and $\mathrm{M}_{nk}(R)$. Show that $\det_R(A) = \det_R(\det_S(A))$.

16. Discussion and Problem sessions 16

16.1. misc.

1. (Game of Chomps) Suppose there are cookies on the lattice points in the first quarter of the plane; that means $\{(m,n) \in \mathbb{Z}^2 \mid m,n \geq 0\}$. Two players are playing the following game: at players' turn they choose a square (m,n) and eat all the cookies that are located at (m',n') where $m' \geq m$ and $n' \geq n$. The cookie at $(0,0)$ is poisoned, and the player who eats it immediately loses. Prove that any game of Chomp ends after finitely many moves.
2. Suppose A is a unital commutative ring and I is an ideal of A. Let
$$\sqrt{I} := \{a \in A \mid a^n \in I \text{ for some posistive integer } n\}.$$
   (a) Prove that $\sqrt{I}$ is an ideal of A.
   (b) Prove that $\sqrt{I}$ is the intersection of all the prime ideals of A which contain I.
3. Suppose R is a unital commutative ring and $a_{ij} \in \mathrm{M}_n(R)$. Let S be the subring of $\mathrm{M}_n(R)$ which is generated by R and a_{ij}'s. Suppose S is commutative. Let $A := [a_{ij}]$ and view it both as an element of $\mathrm{M}_k(S)$ and $\mathrm{M}_{nk}(R)$. Show that $\det_R(A) = \det_R(\det_S(A))$.
4. Suppose D is an integral domain and $f, g \in D[x] \setminus D$. Then the resultant $r(f,g) = 0$ if and only if they have a common divisor of positive degree.

16.2. Hilbert's Nullstellensatz. State various forms of Hilbert's Nullstellensatz.