HOMEWORK ASSIGNMENTS

1. Week 1

1. Prove that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{2}]) = \{\mathrm{id}\}$.

2. Suppose p is prime and $\zeta_p := e^{2\pi i/p}$. Prove that
$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_p, \sqrt[p]{2}]) \simeq \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Z}_p^{\times}, b \in \mathbb{Z}_p \right\}.$$

3. Suppose F is a field.
   (a) Suppose $f \in F[x]$ is irreducible. Prove that f is not separable if and only if $f'(x) = 0$ (Look at Section 24.1 in the lecture note).
   (b) Prove that if $\mathrm{char}(F) = 0$, then every non-constant polynomial in $F[x]$ is separable.
   (c) Suppose $\mathrm{char}(F) = p$ is prime. Suppose $f_0 \in F[x]$ is irreducible and non-separable. Prove that $f_0(x) = f_1(x^p)$ for some irreducible polynomial $f_1 \in F[x]$.
   (d) Suppose $\mathrm{char}(F) = p$ is prime. Suppose $f_0 \in F[x]$ is irreducible and non-separable. Prove that $f_0(x) = h(x^{p^m})$ for some positive integer m and an irreducible separable polynomial $h \in F[x]$.

4. Suppose F is a field $\mathrm{char}(F) = p$ is prime and $\phi : F \to F, \phi(a) = a^p$ is not surjective. Image of ϕ is denoted by F^p. Prove that F/F^p is not separable.

5. Suppose E/F is an algebraic field extension.
   (a) If $\mathrm{char}(F) = 0$, then prove that E/F is separable.
   (b) If $\mathrm{char}(F) = p$ is prime and $\phi : F \to F, \phi(a) = a^p$ is surjective, then prove that E/F is separable.

2. Week 2

1. Suppose F is a field of characteristic zero and it contains an element ζ such that the multiplicative order of ζ_n is n. For $a \in F$, $\sqrt[n]{a}$ denotes a zero of $x^n - a$. Let $(F^{\times})^n := \{a^n \mid a \in F^{\times}\}$. Notice that $(F^{\times})^n$ is a subgroup of $F^{\times}$.
   (a) Prove that $F[\sqrt[n]{a}]/F$ is a Galois extension for every $a \in F^{\times}$.
   (b) Prove that $f_a : \mathrm{Aut}_F(F[\sqrt[n]{a}]) \to \langle \zeta_n \rangle, f_a(\sigma) := \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$ is an injective group homomorphism.
   (c) Use the previous part to deduce that $\mathrm{Aut}_F(F[\sqrt[n]{a}])$ is cyclic. Suppose σ_0 generates $\mathrm{Aut}_F(F[\sqrt[n]{a}])$, and prove that for $\alpha \in F[\sqrt[n]{a}]$, we have $\sigma_0(\alpha) = \alpha$ if and only if $\alpha \in F$.

2. Suppose F is a field of characteristic zero and it contains an element ζ such that the multiplicative order of ζ_n is n. For $a \in F$, $\sqrt[n]{a}$ denotes a zero of $x^n - a$.
   (a) Suppose $\mathrm{Aut}_F(F[\sqrt[n]{a}]) = \langle \sigma_0 \rangle$. Prove that for every positive integer d we have
$$\sigma_0^d = \mathrm{id} \iff (a(F^{\times})^n)^d = (F^{\times})^n \text{ in } F^{\times}/(F^{\times})^n.$$

(b) Prove that $\mathrm{Aut}_F(F[\sqrt[n]{a}]) \simeq \langle a(F^\times)^n \rangle$, where $\langle a(F^\times)^n \rangle$ is the subgroup of $F^\times/(F^\times)^n$ which is generated by $a(F^\times)^n$.

3. Suppose F is a field of characteristic zero and it contains an element ζ such that the multiplicative order of ζ_n is n. For $a \in F$, $\sqrt[n]{a}$ denotes a zero of $x^n - a$. Prove that for $a_1, a_2 \in F$ we have $F[\sqrt[n]{a_1}] = F[\sqrt[n]{a_2}]$ if and only if $\langle a_1(F^\times)^n \rangle = \langle a_2(F^\times)^n \rangle$.
(Hint: Let f_{a_1} and f_{a_2} be the group embeddings given in the earlier problems. Argue that the image of f_{a_1} is equal to the image of f_{a_2}.)

4. Suppose F is a field and p is a prime with the following property: if E/F is a finite field extension and $E \neq F$, then p divides $[E : F]$.
(a) Prove that if E/F is a finite Galois extension, then $[E : F] = p^n$ for some integer n.
(Hint: let P be a Sylow p-subgroup of $\mathrm{Aut}_F(E)$ and consider $\mathrm{Fix}(P)$.)

(b) Prove that if E/F is a finite separable extension, then $[E : F] = p^n$ for some integer n.
(Hint: consider a normal closure L/F of E/F.)

(c) Suppose there is a finite non-separable extension E/F. Prove that $\mathrm{char}(F) = p$.

3. Week 3

1. (a) 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.

(b) Suppose E/F is a finite purely inseparable extension. Prove that $[E : F] = p^m$ for some integer m where $p = \mathrm{char}(F)$.

(c) Suppose F is a field and p is a prime with the following property: if E/F is a finite field extension and $E \neq F$, then p divides $[E : F]$. Prove that $[E : F] = p^n$ for some integer n.

2. Suppose F is a field of characteristic $p > 2$. Let $F(t) := \left\{ \frac{f(t)}{g(t)} \mid f, g \in F[t] \right\}$ be the field of rational functions. Suppose $\sigma, \tau \in \mathrm{Aut}_F(F(t))$ are such that $\sigma(t) := t + 1$ and $\tau(t) = -t$. Let H be the subgroup generated by σ and τ.
(a) Prove that $\mathrm{Fix}(\tau) = F(t^2)$ and $\mathrm{Fix}(\sigma) = F(t^p - t)$.

(b) Prove that $\mathrm{Fix}(H) = F((t^p - t)^2)$.

(c) Prove that $F(t^2)/F((t^p - t)^2)$ is not a normal extension.

3. Suppose E/F is a finite Galois extension and $f \in F[x] \setminus F$. Suppose L is a splitting field of a separable polynomial f over E. Prove that L/F is a Galois extension.

4. Suppose p is prime, $\sigma = (0, 1, \ldots, p-1)$ in the symmetric group S_p of the set $\{0, 1, \ldots, p-1\}$ and $\tau = (0, a) \in S_p$ for some integer $a \in [1, p-1]$. Let H_a be the group generated by σ and τ.
(a) Prove that $H_1 = S_p$. (Hint: Notice that $\gamma := (0,1)(0,1,\ldots,p-1) = (1,\ldots,p-1) \in H_1$. Recall or convince yourself that for every $\alpha \in S_p$ we have $\alpha(0,1)\alpha^{-1} = (\alpha(0), \alpha(1))$. Consider $\gamma^i(0,1)\gamma^{-i}$ and deduce that $(i, i+1)$ is in H_1 for every i. Notice that $(1,2)(0,1)(1,2) = (0,2)$ and continue like that to obtain that $(0, i) \in H_1$. Use this to conclude that all the transpositions (i, j)'s are in H_1. Deduce that $H_1 = S_p$.)

(b) Prove that $H_a = S_p$. (Hint: Notice that $\sigma^i(0,a)\sigma^{-i} = (i, a+i)$ where $+$ is in $\mathbb{Z}_p := \{0, \dots, p-1\}$. Hence $(ka, (k+1)a) \in H_a$ for every k. Next notice that $(a, 2a)(0, a)(a, 2a) = (0, 2a)$ and continue like that to conclude that $(0, ak) \in H_a$ for every k. Deduce that $(0, 1) \in H_a$.)

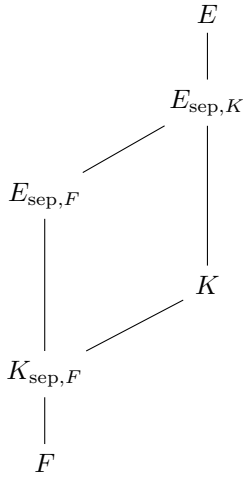
5. Suppose $p > 4$ is prime, and $f \in \mathbb{Q}[x]$ is an irreducible polynomial of degree p which has two non-real complex zeros and $p-2$ real zeros. Let $E \subseteq \mathbb{C}$ be a splitting field of f over $\mathbb{Q}$.
   (a) Prove that $\mathrm{Aut}_{\mathbb{Q}}(E) \simeq S_p$.
   (b) Prove that f is not solvable by radicals over $\mathbb{Q}$,

4. Week 4

1. Suppose L/F is an algebraic extension. Let
$$F_{\mathrm{ab}} := \{\alpha \in L \mid F[\alpha]/F \text{ is Galois, and } \mathrm{Aut}_F(F[\alpha]) \text{ is abelian}\}.$$
Prove that F_{ab}/F is a Galois extension. Moreover prove that $\mathrm{Aut}_F(F_{\mathrm{ab}})$ is abelian if L/F is a finite extension.

2. Suppose E/F is a finite normal extension, and
$$E_{\mathrm{sep}} := \{\alpha \in E \mid m_{\alpha,F} \text{ is separable}\}.$$
   (a) Prove that E_{sep}/F is a Galois extension.
   (b) Prove that $r : \mathrm{Aut}_F(E) \to \mathrm{Aut}_F(E_{\mathrm{sep}}),\ r(\theta) := \theta|_{E_{\mathrm{sep}}}$ is a group isomorphism.
   (c) Let $K := \mathrm{Fix}(\mathrm{Aut}_F(E))$. Prove that $[E : K] = [E_{\mathrm{sep}} : F]$, E/K is Galois, and K/F is purely inseparable.

3. For a finite extension E/F, we let $[E : F]_s := [E_{\mathrm{sep}} : F]$. Suppose $K \in \mathrm{Int}(E/F)$.



Let $E_{\mathrm{sep},K}$ be the separable closure of K in E/K, let $E_{\mathrm{sep},F}$ be the separable closure of F in E/F, and let $K_{\mathrm{sep},F}$ be the separable closure of F in K/F.
   (a) In the above setting prove that $K_{\mathrm{sep},F} \subseteq E_{\mathrm{sep},F} \subseteq E_{\mathrm{sep},K}$.
   (b) Argue that there is $\alpha \in E_{\mathrm{sep},F}$ such that $E_{\mathrm{sep},F} = K_{\mathrm{sep},F}[\alpha]$.
   (c) Prove that $E_{\mathrm{sep},K}/K[\alpha]$ is both separable and purely inseparable. Deduce that $E_{\mathrm{sep},K} = K[\alpha]$.
   (d) Prove that $m_{\alpha,K} | m_{\alpha,K_{\mathrm{sep},F}}$ and $m_{\alpha,K_{\mathrm{sep},F}} | m^q_{\alpha,K}$ where q is either 1 if $\mathrm{char}(F) = 0$ or a power of p if $\mathrm{char}(F) = p > 0$. Deduce that $m_{\alpha,K} = m_{\alpha,K_{\mathrm{sep},F}}$.
   (e) Prove that $[E : F]_s = [E : K]_s[K : F]_s$.

4. Suppose F is a field, $L := F(x_1, \dots, x_n)$ is the field of fractions of $F[x_1, \dots, x_n]$. For $\sigma \in S_n$ and $f \in L$, let $T_\sigma(f) = f(x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)})$.
   (a) Prove that $T : S_n \to \mathrm{Aut}_F(L),\ (T(\sigma))(f) := T_\sigma(f)$ is an injective group homomorphism.
   (b) Let $K := \mathrm{Fix}(T(S_n))$. Elements of K are called *symmetric functions*. Let
$$(t - x_1) \cdots (t - x_n) = t^n - s_1 t^{n-1} + s_2 t^{n-2} - \cdots + (-1)^n s_n.$$
Let $E := F(s_1, \dots, s_n)$. Prove that L is a splitting field of $t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n$ over E. Deduce that $[L : E] \leq n!$.

(c) Prove that $K = E$.

(d) For $f \in L$, let $G(f) := \{\sigma \in S_n \mid T_\sigma(f) = f\}$. Prove that $\mathrm{Fix}(T(G(f))) = K[f]$.

(e) Prove that $G(f) \subseteq G(g)$ for $f, g \in L$ if and only if there is $\theta \in K[t]$ such that $g = \theta(f)$. (This result is known as *Lagrange's Rational Function Theorem*, and Lagrange proved this result before Galois theory was developed. Along the way, he proved some results about permutation groups, which later got generalized to what we call Lagrange's theorem in group theory!)

5. Week 5

1. Suppose L/F is a field extension and L is algebraically closed. Suppose E is the algebraic closure of F in L. Prove that E is algebraically closed.

2. Suppose E/F is an algebraic extension and every $f \in F[x] \setminus F$ can be decomposed into linear factors in $E[x]$. Prove that E is algebraically closed.

3. Suppose F is a perfect field, and $\overline{F}$ is an algebraic closure of F; that means $\overline{F}/F$ is an algebraic extension and $\overline{F}$ is algebraically closed. Let
$$\mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F) := \{E \in \mathrm{Int}(\overline{F}/F) \mid E/F \text{ is a finite normal extension}\},$$
and
$$\mathcal{O}_{\mathrm{n}}(\mathrm{Aut}_F(\overline{F})) := \{\mathrm{Aut}_E(\overline{F}) \mid E \in \mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F)\}.$$
(a) For $E \in \mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F)$, let $r_E : \mathrm{Aut}_F(\overline{F}) \to \mathrm{Aut}_F(E)$ be the restriction map $r_E(\phi) := \phi|_E$. Argue why r_E is a well-defined surjective group homomorphism.

(b) Suppose $E, E' \in \mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F)$ and $E \subseteq E'$. Let $r_{E',E} : \mathrm{Aut}_F(E') \to \mathrm{Aut}_F(E)$ be the restriction map $r_{E',E}(\theta) := \theta|_E$. Argue that $r_{E',E}$ is a well-defined surjective group homomorphism and $r_E = r_{E',E} \circ r_{E'}$.

(c) Let $G(\overline{F}/F) := \{(\phi_E) \in \prod_{E \in \mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F)} \mathrm{Aut}_F(E) \mid \forall E \subseteq E', r_{E',E}(\phi'_E) = \phi_E\}$. (So $G(\overline{F}/F)$ consists of families of *compatible* automorphisms of finite normal extensions of F. This is called the *inverse limit* of $\mathrm{Aut}_F(E)$'s). Consider
$$r : \mathrm{Aut}_F(\overline{F}) \to G(\overline{F}/F), \quad r(\phi) := (r_E(\phi))_{E \in \mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F)}.$$
Prove that r is a well-defined isomorphism.

4. Suppose $\overline{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$.
(a) Prove that for every positive integer n there is a unique $F_n \in \mathrm{Int}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ that is isomorphic to $\mathbb{F}_{p^n}$.

(b) Prove that $\mathrm{Int}_{\mathrm{f,n}}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \{F_n \mid n \in \mathbb{Z}^+\}$ and $\overline{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} F_n$.

(c) Let $\widehat{\mathbb{Z}} := \{(a_n) \in \prod_{n=2}^{\infty} \mathbb{Z}_n \mid \forall n | n', a_{n'} \equiv a_n \pmod{n}\}$. Prove that $\mathrm{Aut}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p) \simeq \widehat{\mathbb{Z}}$.

(d) Prove that $\widehat{\mathbb{Z}}$ does not have a torsion element.

(e) Prove that if $\overline{\mathbb{F}}_p/E$ is a finite extension, then $E = \overline{\mathbb{F}}_p$.

6. Week 6

1. Prove that $\mathbb{Q}[\cos(\frac{2\pi}{n})]/\mathbb{Q}$ is a Galois extension and $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\cos(\frac{2\pi}{n})]) \simeq \mathbb{Z}_n^\times/\{\pm 1\}$.

2. Suppose E/F is a field extension, and $f \in F[x]$ is a polynomial of degree n with distinct zeros $\alpha_1, \ldots, \alpha_n$ in E. Suppose $[F[\alpha_1, \alpha_2] : F] = n(n-1)$.
   (a) Find the degrees of irreducible factors of f in $F[x]$ and $(F[\alpha_1])[x]$.
   (b) Prove that $\mathcal{G}_{f,F}$ acts two transitively on $\{\alpha_1, \ldots, \alpha_n\}$; that means for every $i \neq j$, there is $\theta \in \mathcal{G}_{f,F}$ such that $\theta(\alpha_1) = \alpha_i$ and $\theta(\alpha_2) = \alpha_j$.
   (c) Let $g(x) := m_{\alpha_1+\alpha_2,F}(x)$. Prove that $g(\alpha_i + \alpha_j) = 0$ for every $i \neq j$.

3. Suppose $K_0 := \mathbb{Q} \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{C}$ is a tower of fields such that K_{i+1}/K_i is a Galois extension and $[K_{i+1} : K_i] = p_i$ where p_i is an odd prime for all i.
   (a) Prove that $K_i \subseteq \mathbb{R}$ for all i.
   (b) Prove that $\mathbb{Q}[\sqrt[3]{2}]$ is not contained in K_n.

4. Suppose F is a field and $\overline{F}$ is an algebraic closure of F. Suppose $K, E \in \mathrm{Int}(\overline{\mathrm{F}}\,/F)$ such that K/E is a Galois extension and $[K : E] = p$ where p is prime. Suppose E/F is a Galois extension and $|\operatorname{Aut}_F(E)| = p^m$ for some integer m.
   (a) Argue why there is $\alpha \in K$ such that $K = E[\alpha]$. Let $L \in \mathrm{Int}(\overline{\mathrm{F}}\,/E)$. Prove that $L[\alpha]/L$ is a Galois extension and $[L[\alpha] : L] = 1$ or p.
   (b) Argue that for every $\theta_i \in \operatorname{Aut}_F(E)$, there is $\widehat{\theta}_i \in \operatorname{Aut}_F(\overline{\mathrm{F}})$ such that $\widehat{\theta}_i|_E = \theta_i$. Let $\alpha_i := \widehat{\theta}_i(\alpha)$. Prove that $E[\alpha_i]/E$ is a Galois extension and $[E[\alpha_i] : E] = p$ for all i.
   (c) In the above setting, prove that $E[\alpha_1, \ldots, \alpha_{p^m}]/F$ is a Galois extension, and if $\widehat{L} \in \mathrm{Int}(\overline{\mathrm{F}}\,/K)$ and $\widehat{L}/F$ is Galois, then $E[\alpha_1, \ldots, \alpha_{p^m}] \subseteq \widehat{L}$. (We say $E[\alpha_1, \ldots, \alpha_{p^m}]$ is a Galois closure of K/F.)
   (d) Prove that $[E[\alpha_1, \ldots, \alpha_{p^m}] : F]$ is a power of p.

7. Week 7

1. Suppose $p_1, \ldots, p_n$ are distinct primes. Let $F := \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}]$.
   (a) Prove that $F/\mathbb{Q}$ is a Galois extension and $\operatorname{Aut}_{\mathbb{Q}}(F) \simeq \underbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n \text{ times}}$.
   (b) Prove that every $K \in \mathrm{Int}(F/\mathbb{Q})$ which is a quadratic extension of $\mathbb{Q}$ is of the form $\mathbb{Q}[\sqrt{\prod_{i \in I} p_i}]$ where I is a non-empty subset of $\{1, 2, \ldots, n\}$.
   (c) Prove that $F = \mathbb{Q}[\sqrt{p_1} + \cdots + \sqrt{p_n}]$.

2. Suppose p is an odd prime number and $\zeta_n := e^{\frac{2\pi i}{n}}$ for every positive integer n.
   (a) Prove that $\mathbb{Q}[\zeta_{4p}] = \mathbb{Q}[\zeta_p, i]$.
   (b) Prove that $\mathbb{Q}[\sin(\frac{2\pi}{p})]/\mathbb{Q}$ is a Galois extension and $\operatorname{Aut}_{\mathbb{Q}[\sin(\frac{2\pi}{p})]}(\mathbb{Q}(\zeta_{4p})) = \{\mathrm{id}, \tau\}$ where τ is the restriction of the complex conjugation.
   (c) Prove that $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sin(\frac{2\pi}{p})]) \simeq \frac{\mathbb{Z}_{4p}^{\times}}{\{\pm 1\}}$; in particular $[\mathbb{Q}[\sin(\frac{2\pi}{p})] : \mathbb{Q}] = p - 1$.

3. Suppose p is prime, F is a field of characteristic zero, and $a \in F$. Let E be a splitting field of $x^p - a$ over F.

(a) Suppose $\alpha \in E$ is a zero of $x^p - a$. Argue that there is an element ζ of order p in E such that $x^p - a = (x-\alpha)(x-\zeta\alpha)\cdots(x-\zeta^{p-1}\alpha)$. Suppose $f(x) \in F[x]$ divides $x^p - a$ and $\deg f < p$. Prove that $\zeta^i \alpha^{\deg f}$ is in F for some integer i.

(b) Prove that if $x^p - a$ is reducible in $F[x]$, then $x^p - a$ has a zero in F.

4. Suppose $n, n_1, \ldots, n_k$ are positive integers.
   (a) Use a special case of Dirichlet's theorem which says that there are infinitely many primes in the arithmetic progression $\{mk+1\}_{k=1}^{\infty}$ for every positive integer m, to show that $\mathbb{Z}_n$ is isomorphic to a quotient of $\mathbb{Z}_p^\times$ for some prime p.

   (b) Prove that $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ is isomorphic to a quotient of $\mathbb{Z}_q^\times$ for some $q = p_1 \cdots p_k$ and primes p_i's.

   (c) Prove that there is a Galois extension $F/\mathbb{Q}$ such that $\mathrm{Aut}_{\mathbb{Q}}(F) \simeq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

8. Week 8

1. Suppose R is a unital commutative ring and n is a positive integer. For every permutation $\sigma \in S_n$, let

$$d_\sigma : R^n \times \cdots \times R^n \to R, \quad d_\sigma(\mathbf{v}_1, \ldots, \mathbf{v}_n) := \prod_{j=1}^{n} v_{\sigma(j)j}$$

where $\mathbf{v}_j = \begin{pmatrix} v_{1j} \\ \vdots \\ v_{nj} \end{pmatrix}$. Let

$$d : R^n \times \cdots \times R^n \to R, \quad d(\mathbf{v}_1, \ldots, \mathbf{v}_n) := \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) d_\sigma(\mathbf{v}_1, \ldots, \mathbf{v}_n).$$

   (a) Prove that for every $\sigma \in S_n$ and integer $i \in [1, n]$, d_σ is an R-module homomorphism from R^n to R with respect to $\mathbf{v}_i$. This means

$$d_\sigma(\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_i + c\mathbf{v}_i', \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n) = d_\sigma(\mathbf{v}_1, \ldots, \mathbf{v}_n) + c d_\sigma(\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_i', \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n)$$

   for every $\mathbf{v}_j$'s and $\mathbf{v}_i'$ in R^n, and $c \in R$. (We say d_σ is n-linear).
   (b) Prove that d is n-linear.
   (c) Suppose $\mathbf{v}_i = \mathbf{v}_j$ and τ is the transposition $(i, j) \in S_n$. Prove that for every $\sigma \in S_n$, we have

$$d_{\sigma\tau}(\mathbf{v}_1, \ldots, \mathbf{v}_n) = d_\sigma(\mathbf{v}_1, \ldots, \mathbf{v}_n).$$

   (d) Suppose $\mathbf{v}_i = \mathbf{v}_j$ for some $i \neq j$. Prove that $d(\mathbf{v}_1, \ldots, \mathbf{v}_n) = 0$. (We say d is alternating.)
   (e) For every index i, we identify $\{1, \ldots, n\} \setminus \{i\}$ with $\{1, \ldots, n-1\}$ by shifting all the numbers more than i by 1; this means we let

$$\ell_i : \{1, \ldots, n\} \setminus \{i\} \to \{1, \ldots, n-1\}, \quad \ell_i(j) := \begin{cases} j & \text{if } j < i \\ j-1 & \text{if } j > i. \end{cases}$$

   For every $\sigma \in S_n$ and integer i in $[1, n]$, we let σ_i be the induced permutation on $\{1, \ldots, n\}$ after dropping i; this means σ_i is the composite of the following bijections

$$\{1, \ldots, n-1\} \xrightarrow{\ell_i^{-1}} \{1, \ldots, n\} \setminus \{i\} \xrightarrow{\sigma} \{1, \ldots, n\} \setminus \{\sigma(i)\} \xrightarrow{\ell_{\sigma(i)}} \{1, \ldots, n-1\}.$$

   Let $\widehat{\sigma}_i \in S_n$ be such that $\widehat{\sigma}_i(j) = \sigma_i(j)$ if $j < n$ and $\widehat{\sigma}_i(n) = n$. Prove that

$$\widehat{\sigma}_i = (\sigma(i), \ldots, n)^{-1} \, \sigma \, (i, \ldots, n)$$

where the first and the last factors are cycle permutations in S_n. Deduce that

$$\operatorname{sgn}(\sigma_i) = (-1)^{i+\sigma(i)} \operatorname{sgn}(\sigma).$$

(f) For indexes i, k, let $\mathbf{v}_i^{(k)}$ be the $(n-1)$-by-1 column that we obtain after dropping the k-th row of $\mathbf{v}_i$. We want to start with n column vectors in R^n, drop the j-th vector and the k-th components of the rest to get $n-1$ vectors in R^{n-1}. Starting with $\mathbf{v}_1, \ldots, \mathbf{v}_n$, we get $\mathbf{w}_r := \mathbf{v}^{(k)}_{\ell_j^{-1}(r)}$. Justify yourself that the $\sigma_j(r)$ component of $\mathbf{w}_r$ is the $\sigma(\ell_j^{-1}(r))$-th component of $\mathbf{v}_{\ell_j^{-1}(r)}$ if $\sigma(j) = k$. Prove that

$$d_\sigma(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{e}_k, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_n) = \begin{cases} d_{\sigma_j}(\mathbf{w}_1, \ldots, \mathbf{w}_{n-1}) & \text{if } \sigma(j) = k \\ 0 & \text{otherwise,} \end{cases}$$

where $\mathbf{e}_i$ is the column matrix with 1 in its i-th row and 0 in the rest of entries.

(g) Prove that

$$d(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1}, \mathbf{e}_k, \mathbf{v}_{j+1}, \ldots, \mathbf{v}_n) = (-1)^{j+k} d(\mathbf{v}^{(k)}_{\ell_j^{-1}(1)}, \ldots, \mathbf{v}^{(k)}_{\ell_j^{-1}(n-1)}),$$

and deduce that

$$d(\mathbf{v}_1, \ldots, \mathbf{v}_n) = \sum_{k=1}^{n} (-1)^{j+k} v_{kj}\ d(\mathbf{v}^{(k)}_{\ell_j^{-1}(1)}, \ldots, \mathbf{v}^{(k)}_{\ell_j^{-1}(n-1)}). \tag{1}$$

2. Suppose R is a unital commutative ring and $f : R^n \times R^n \to R$ is bilinear; that means it is an R-module homomorphism with respect to each component separately. Suppose $f(\mathbf{v}, \mathbf{v}) = 0$ for every $\mathbf{v} \in R^n$. Prove that $f(\mathbf{v}, \mathbf{w}) = -f(\mathbf{w}, \mathbf{v})$ for every $\mathbf{v}, \mathbf{w} \in R^n$. (Hint. Consider $f(\mathbf{v} + \mathbf{w}, \mathbf{v} + \mathbf{w})$.)
3. Suppose R is a unital commutative ring and n is a positive integer n. Suppose $f : R^n \times \cdots \times R^n \to R$ is n-linear and alternating.
   (a) Write $\mathbf{v}_j = \sum_{i=1}^n v_{ij} \mathbf{e}_i$ where $\mathbf{e}_i$ is the column matrix with 1 in its i-th row and 0 in the rest of entries. Argue why

$$f(\mathbf{v}_1, \ldots, \mathbf{v}_n) = \sum_{\sigma \in S_n} f(\mathbf{e}_{\sigma(1)}, \ldots, \mathbf{e}_{\sigma(n)}) \prod_{j=1}^{n} v_{\sigma(j)j}.$$

   (b) Argue why $f(\mathbf{e}_{\sigma(1)}, \ldots, \mathbf{e}_{\sigma(n)}) = \operatorname{sgn}(\sigma) f(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ for every $\sigma \in S_n$.
   (c) Prove that $f = f(\mathbf{e}_1, \ldots, \mathbf{e}_n) d$ where d is the function given in the first problem.
4. Suppose R is a unital commutative ring, n is a positive integer, and $A \in \mathrm{M}_n(R)$. Let

$$f_A : R^n \times \cdots \times R^n \to R, f_A(\mathbf{v}_1, \ldots, \mathbf{v}_n) := d(A\mathbf{v}_1, \ldots, A\mathbf{v}_n),$$

where d is the function given in problem 1. Let

$$\det : \mathrm{M}_n(R) \to \det(X) := d(\mathbf{x}_1, \ldots, \mathbf{x}_n),$$

where $\mathbf{x}_j$ is the j-th column of X.
   (a) Prove that f_A is n-linear and alternating.
   (b) Prove that $f_A(\mathbf{x}_1, \ldots, \mathbf{x}_n) = \det(AX)$ where $\mathbf{x}_j$ is the j-th column of X.
   (c) Prove that $\det(XY) = \det(X) \det(Y)$ for every $X, Y \in \mathrm{M}_n(R)$.
   (d) For $X \in \mathrm{M}_n(R)$ and indexes i, j, let X_{ij} be the $(n-1)$-by-$(n-1)$ matrix that we obtain after dropping the i-th row and the j-th column of X. Use (1) and prove that

$$\det(X) = \sum_{k=1}^{n} (-1)^{j+k} x_{kj} \det(X_{kj}).$$

   (e) For $X \in \mathrm{M}_n(R)$, we define the *adjoint* $\operatorname{adj}(X)$ of X as an n-by-n matrix with the (j,k)-entry equals to $(-1)^{j+k} \det(X_{kj})$, where X_{kj} is as in the previous part. Use the previous part to show

$$\operatorname{adj}(X) X = \det(X) I.$$

(for the off diagonal entries, again use the previous problem and notice that on the left hand side you end up getting determinant of a matrix with repeated columns!)

(f) Justify why $\det(X) = \det(X^t)$ where X^t is the transpose of X, and deduce that we could work with rows of X instead of its columns, and we obtain

$$\det(X) = \sum_{j=1}^{n} (-1)^{j+k} x_{kj} \det(X_{kj}),$$

and so

$$X \operatorname{adj}(X) = \det(X) I.$$

9. Week 9

1. For a finite abelian group A, let $\widehat{A}$ be its dual group.
   (a) Suppose A_1 and A_2 are two finite abelian groups. Prove that $\widehat{A_1 \times A_2} \simeq \widehat{A}_1 \times \widehat{A}_2$.

   (b) Suppose A is a finite cyclic group. Prove that $\widehat{A}$ is a cyclic group and deduce that $A \simeq \widehat{A}$.

   (c) Suppose A is a finite abelian group. Prove that $A \simeq \widehat{A}$.

2. Suppose A_i's are square matrices with entries in a unital commutative ring R. Prove that

$$\det \begin{pmatrix} A_1 & * & \cdots & * \\ 0 & A_2 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_n \end{pmatrix} = \prod_{i=1}^{n} \det A_i.$$

3. Recall that an element a of a ring is called nilpotent if $a^k = 0$ for some positive integer k.
   (a) Suppose F is a field and $A \in \mathrm{M}_n(F)$ is nilpotent. Prove that the characteristic polynomial of A is x^n, and deduce that $A^n = 0$.

   (b) Suppose R is a unital commutative ring. Suppose $A \in \mathrm{M}_n(R)$ is nilpotent and P is a prime ideal of R. Prove that all the entries of A^n are in P.

   (c) Suppose R is a unital commutative ring which has no non-zero nilpotent elements. Suppose $A \in \mathrm{M}_n(R)$ is nilpotent. Prove that $A^n = 0$. (Hint: you are allowed to use the following result that we have proved in one of the discussion and problem sessions: the set of all nilpotent elements of R is equal to the intersection of all the prime ideals of R.)

4. Suppose E/F is a finite Galois extension and $\mathrm{Aut}_F(E) = \langle \sigma \rangle$ is a cyclic group of order n. For $a \in E$, let $\tau_a : E \to E, \tau_a(e) := a\sigma(e)$. Notice that τ_a is an F-linear map.
   (a) Prove that the minimal polynomial of τ_a is $p(x) := x^n - N_{E/F}(a)$.

   (b) Prove that the companion $C(p)$ of the polynomial $p(x) = x^n - N_{E/F}(a)$ is a rational canonical form of τ_a.

   (c) (Hilbert's theorem 90) Suppose $N_{E/F}(a) = 1$ and argue why $C(p)(\mathbf{e}_1 + \cdots + \mathbf{e}_n) = \mathbf{e}_1 + \cdots + \mathbf{e}_n$. Deduce that $a = \frac{e}{\sigma(e)}$ for some $e \in E$.

   (d) Use part (b) for $\tau_1 = \sigma$ and prove that there is $e_0 \in E$ such that $\mathfrak{B}_0 := (e_0, \sigma(e_0), \ldots, \sigma^{n-1}(e_0))$ is an F-basis of E.

5. Suppose E/F is a finite Galois extension and $\mathrm{Aut}_F(E) = \langle\sigma\rangle$ is a cyclic group of order n. For $a \in E$, let $T_{E/F}(a) := a + \sigma(a) + \cdots + \sigma^{n-1}(a)$.
   (a) Suppose $\mathfrak{B}_0$ is the F-basis of E which is given in 4(d). Notice that $[\sigma]_{\mathfrak{B}_0}$ is the companion matrix of $x^n - 1$. Prove that $T_{E/F}(a) = 0$ if and only if $c_1 + \cdots + c_n = 0$ where $[a]_{\mathfrak{B}_0} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$.
   (b) Suppose for $c_1, \ldots, c_n \in F$, we have $\sum_{i=1}^n c_i = 0$. Prove that
$$\begin{pmatrix} -1 & 0 & 0 & \cdots & 0 & 1 \\ 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & 0 \\ 0 & 0 & 0 & \cdots & 1 & -1 \end{pmatrix} \mathbf{x} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$
   has a solution in F^n.
   (c) (Additive Hilbert's theorem 90) Suppose $a \in E$ such that $T_{E/F}(a) = 0$. Prove that there is $e \in E$ such that $\sigma(e) - e = a$.

10. Week 10

1. Suppose A is a unital commutative ring, n is a positive integer, and $f : A^n \to A^n$ is a surjective A-module homomorphism.
   (a) Suppose A is a Noetherian ring.
      (i) Argue why A^n is a Noetherian A-module.
      (ii) Show that there is an integer n_0 such that for every integer $i \geq n_0$, $\ker f^{(n_0)} = \ker f^{(i)}$.
      (iii) Suppose $\mathbf{x} \in \ker f^{(n_0)}$. Argue that $\mathbf{x} = f^{(n_0)}(\mathbf{y})$ for some $\mathbf{y}$. Deduce that $\mathbf{y} \in \ker f^{(2n_0)}$. Use this to show that $\mathbf{x} = 0$.
      (iv) Prove that f is an isomorphism.
   (b) Suppose A is an arbitrary unital commutative ring.
      (a) Show that there are $M_f := [a_{ij}] \in \mathrm{M}_n(A)$ and $M' = [a'_{ij}] \in Ma_n(A)$ such that
$$f(x_1, \ldots, x_n) = (\sum_{j=1}^n a_{1j}x_j, \ldots, \sum_{j=n}^n a_{1j}x_j)$$
      and $M_f M' = I_n$. Argue that f is an isomorphism if and only if $M_f \in \mathrm{GL}_n(A)$.
      (b) Let A' be the subring of A which is generated by a_{ij}'s and a'_{ij}'s. Argue that
$$M_f\times : \mathrm{M}_{n,1}(A') \to \mathrm{M}_{n,1}(A'), \;\; \mathbf{x} \mapsto M_f\mathbf{x}$$
      is a surjective A'-module homomorphism.
      (c) Prove that $M_f \in \mathrm{GL}_n(A')$ and deduce that f is an isomorphism.

2. What is your favorite theorem, result, method, or technique among the topics that you have learned in math100b and math100c?