OUTLINE OF SOLUTIONS OF SOME OF THE ASSIGNMENTS

1. Week 1

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

Outline of solution. Suppose $\theta \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{2}])$. Because $\sqrt[3]{2}$ is a zero of $x^3 - 2 \in \mathbb{Q}[x]$, one also has that $\theta(\sqrt[3]{2})$ is a zero of $x^3 - 2$, but then $\theta(\sqrt[3]{2}) = \zeta_3^i \sqrt[3]{2}$ for some $i \in \{0, 1, 2\}$. If $i \neq 0$ then one has $\zeta_3^i \sqrt[3]{2} \in \mathbb{Q}[\sqrt[3]{2}]$ and then by dividing you can conclude $\zeta_3^i \in \mathbb{Q}[\sqrt[3]{2}]$. Now one can obtain a contradiction using tower law.

Alternatively you can say that $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$, but for $i \in \{1, 2\}$ the element ζ_3^i is not in $\mathbb{R}$.

2. Suppose p is prime and $\zeta_p := e^{2\pi i/p}$. Prove that

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_p, \sqrt[p]{2}]) \simeq \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Z}_p^{\times}, b \in \mathbb{Z}_p \right\}.$$

Solution. We will define a function $f : \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_p, \sqrt[p]{2}]) \to \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Z}_p^{\times}, b \in \mathbb{Z}_p \right\}$: to this end let $\theta \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_p, \sqrt[p]{2}])$. Notice that θ must send ζ_p to another root of $\Phi_p(x)$, i.e. we must have $\theta(\zeta_p) = \zeta_p^i$ for some $i \in \mathbb{Z}$ coprime to p. Simiarly $\theta(\sqrt[p]{2})$ must be a root of $x^p - 2$, so $\theta(\sqrt[p]{2}) = \zeta_p^j \sqrt[p]{2}$ for some $j \in \mathbb{Z}$. We then define $f(\theta) = \begin{pmatrix} [i]_p & [j]_p \\ 0 & 1 \end{pmatrix}$. To see this is well-defined we notice that $[i]_p \in \mathbb{Z}_p^{\times}$ because $\gcd(i, p) = 1$, and if $\zeta_p^i = \zeta_p^{i'}$ then $i \equiv i' \pmod{p}$; similarly if $\zeta_p^j \sqrt[p]{2} = \zeta_p^{j'} \sqrt[p]{2}$ then $j \equiv j' \pmod{p}$.

We claim f is a homomorphism: for this let $\theta, \theta' \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_p, \sqrt[p]{2}])$, say with $\theta(\zeta_p) = \zeta_p^i$, $\theta(\sqrt[p]{2}) = \zeta_p^j \sqrt[p]{2}$, $\theta'(\zeta_p) = \zeta_p^{i'}$ and $\theta'(\sqrt[p]{2}) = \zeta_p^{j'} \sqrt[p]{2}$. Then we calculate

$$(\theta \circ \theta')(\zeta_p) = \theta(\theta'(\zeta_p)) = \theta(\zeta_p^{i'}) = \theta(\zeta_p)^{i'} = (\zeta_p^i)^{i'} = \zeta_p^{ii'},$$

and

$$(\theta \circ \theta')(\sqrt[p]{2}) = \theta(\theta'(\sqrt[p]{2})) = \theta(\zeta_p^{j'} \sqrt[p]{2}) = \theta(\zeta_p)^{j'} \theta(\sqrt[p]{2}) = (\zeta_p^i)^{j'} (\zeta_p^j \sqrt[p]{2}) = \zeta_p^{ij'+j} \sqrt[p]{2}.$$

Thus we see that

$$f(\theta \circ \theta') = \begin{pmatrix} [ii']_p & [ij' + j]_p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} [i]_p & [j]_p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} [i']_p & [j']_p \\ 0 & 1 \end{pmatrix} = f(\theta) f(\theta').$$

This shows f is a homomorphism. We now notice that f is injective, because if $f(\theta) = I$ then this means that $\theta(\zeta_p) = \zeta_p$ and $\theta(\sqrt[p]{2}) = \sqrt[p]{2}$, but then $\theta = \mathrm{id}$.

Finally we notice that, because $\mathbb{Q}[\zeta_p, \sqrt[p]{2}]$ is the splitting field over $\mathbb{Q}$ of the separable polynomial $x^p - 2 \in \mathbb{Q}[x]$, we have from class that $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_p, \sqrt[p]{2}])| = [\mathbb{Q}[\zeta_p, \sqrt[p]{2}] : \mathbb{Q}] = p(p-1)$, where the latter equality is a calculation we've made in a previous homework. Thus the two groups in question have the same size, so f being injective implies it is surjective as well, and then f is an isomorphism.

3. Suppose F is a field.

(a) Suppose $f(x) \in F[x]$ is irreducible. Prove that f is not separable if and only if $f'(x) = 0$.

Outline of solution. If $f'(x) = 0$ then for $c = \mathrm{ld}(f)$ we have $\gcd(f, f')$ equals f up to a unit in particular it is not equal to 1 so f is separable. On the other hand, if $f'(x) \neq 0$ and $\gcd(f, f') \neq 1$ then using the fact that f is irreducible one can show that $\gcd(f, f')$ equals f up to a unit, and then $f|f'$ which is a contradiction by degree considerations.

(b) Prove that if $\mathrm{char}(F) = 0$ then every non-constant polynomial in $F[x]$ is separable.

Outline of solution. By definition of separable polynomial, one just needs to consider irreducible polynomials. If we have an irreducible polynomial $f(x)$ then necessarily $f'(x) \neq 0$ (i.e. $f'(x)$ is not the zero polynomial), because we are in characteristic 0. Then one applies part (a) to deduce $f(x)$ 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 $f_1 \in F[x]$.

Outline of solution. By part (a) we have $f_0'(x) = 0$. If we write $f_0(x) = \sum_{i=0}^{n} a_i x^i$, then $f_0'(x) = \sum_{i=0}^{n-1} (ia_i)x^{i-1}$. Now for any i such that $a_i \neq 0$, deduce that $i = 0$ in F, and then using $\mathrm{char}(F) = p$ deduce $p|i$ for any such i. Thus for each i with $a_i \neq 0$ we have $x^i = (x^p)^{i/p}$ and then one sees that $f_0(x)$ is a polynomial in x^p. More precisely for any $a_i \neq 0$ (so one has $p|i$) one can let $b_{i/p} := a_i$, and $b_j = 0$ other wise, and then one can take $f_1(x) = \sum_i b_i x^i$. The fact that f_0 is irreducible implies f_1 is irreducible, because a factorization $f_1(x) = g(x)h(x)$ would lead to a factorization $f_0(x) = g(x^p)h(x^p)$.

(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 some irreducible separable polynomial $h \in F[x]$.

Outline of solution. One can proceed by strong induction: if $\deg(f_0) = 1$ then $f_0(x)$ is always separable so the statement is vacuous. If $\deg(f_0) > 1$ then one can use part (c) to write $f_0(x) = f_1(x^p)$ for some irreducible $f_1(x)$. Then one has $\deg(f_0) = p\deg(f_1)$ so $\deg(f_1) < \deg(f_0)$, allowing one to apply the induction hypothesis.

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

Solution. Choose some element $\alpha \in F \setminus F^p$; this is possible because ϕ is not surjective by assumption. Notice that $\alpha^p = \phi(\alpha) \in F^p$, and thus we have $x^p - \alpha^p \in F^p[x]$. Because α is a root of this polynomial we see that $m_{\alpha,F^p}(x)|(x^p - \alpha^p)$. Also notice that $x^p - \alpha^p = (x - \alpha)^p$ in $F[x]$ because we are in characteristic p. Thus by unique factorization we see that $m_{\alpha,F^p}(x) = (x - \alpha)^k$ in $F[x]$ for some $1 \leq k \leq p$. Notice if $k = 1$ then we would have $x - \alpha = m_{\alpha,F^p}(x) \in F^p[x]$, which would imply $\alpha \in F^p$, which contradicts our choice of α. Thus we must have $k \geq 2$, and we see that $m_{\alpha,F^p}(x)$ has at least two copies of $x - \alpha$ in its decomposition into irreducible factors in $F[x]$, which means that $m_{\alpha,F^p}(x)$ is not a separable polynomial. Thus $\alpha \in F$ is an element which is not separable over F^p, so F/F^p is not a separable extension.

5. Suppose E/F is an algebraic field extension.

(a) If $\mathrm{char}(F) = 0$ then E/F is separable.

Outline of solution. By definition one needs to show that if $\alpha \in E$ then $m_{\alpha,F}(x)$ is a separable element of $F[x]$. This follows directly from Problem 3(b).

(b) If $\mathrm{char}(F) = p$ and $\phi : F \to F$, $\phi(a) = a^p$ is surjective, prove E/F is separable.

Solution. Again one needs to show that if $\alpha \in E$ then $m_{\alpha,F}(x) \in F[x]$ is separable. By Problem 3(d) one can write $m_{\alpha,F}(x) = h(x^{p^m})$ for some non-negative integer m and an irreducible separable polynomial $h \in F[x]$ (remark: the case $m = 0$ is coming if $m_{\alpha,F}(x)$ is separable, and when $m_{\alpha,F}(x)$ is non-separable this is when we are applying Problem 3(d)). If one writes $h(x) = \sum_{i=0}^n a_i x^i$, then using that ϕ is surjective one can write $a_i = b_i^{p^m}$ for some $b_i \in F$. But then one sees that

$$m_{\alpha,F}(x) = h(x^{p^m}) = \sum_{i=0}^n b_i^{p^m} x^{p^m} = (\sum_{i=0}^n b_i x^i)^{p^m}.$$

Unless $m = 0$ this contradicts the fact that $m_{\alpha,F}(x)$ is irreducible, so we deduce $m = 0$ and then $m_{\alpha,F}(x) = h(x)$ 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 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 $a \in F^\times$.

   Solution. The field $F[\sqrt[n]{a}]$ is the splitting field of $x^n - a$ over F: the polynomial splits in $F[\sqrt[n]{a}]$ with roots $\sqrt[n]{a}, \zeta\sqrt[n]{a}, \ldots, \zeta^{n-1}\sqrt[n]{a}$ (these are all elements of $F[\sqrt[n]{a}]$ because $\zeta \in F$ by hypothesis), and one can see that $F[\sqrt[n]{a}] = F[\sqrt[n]{a}, \zeta\sqrt[n]{a}, \ldots, \zeta^{n-1}\sqrt[n]{a}]$. These n roots of $x^n - a$ are distinct (because ζ has order n), so in particular $x^n - a$ is separable. Thus $F[\sqrt[n]{a}]$ is the splitting field of a separable polynomial over F.

   (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.

   Solution. First we show it is a homomorphism: we know for some i and some j we have $\sigma(\sqrt[n]{a}) = \zeta^i\sqrt[n]{a}$ and $\tau(\sqrt[n]{a}) = \zeta^j\sqrt[n]{a}$. One then has $(\sigma\circ\tau)(\sqrt[n]{a}) = \zeta^{i+j}\sqrt[n]{a}$, and as a result one has

$$f_a(\sigma\circ\tau) = \frac{(\sigma\circ\tau)(\sqrt[n]{a})}{\sqrt[n]{a}} = \zeta^{i+j} = \zeta^i\zeta^j = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = f_a(\sigma)f_a(\tau).$$

   If one has $f_a(\sigma) = 1$ then one sees that $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}$, but then $\sigma = \mathrm{id}$.

   (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 $\alpha \in F$.

   Solution. Part (b) tells us that $\mathrm{Aut}_F(F[\sqrt[n]{a}])$ is isomorphic to a subgroup of a cyclic group, hence is cyclic itself. For σ_0 as in the statement, one can verify that $\sigma_0(\alpha) = \alpha$ if and only if $\sigma(\alpha) = \alpha$ for all $\sigma \in \mathrm{Aut}_F(F[\sqrt[n]{a}])$ (for the forward direction one simply writes σ as a power of σ_0). Then recalling that $F = \mathrm{Fix}(\mathrm{Aut}_F(F[\sqrt[n]{a}]))$ (this is a consequence of part (a)), one has

$$\sigma_0(\alpha) = \alpha \iff \sigma(\alpha) = \alpha \text{ for all } \sigma \in \mathrm{Aut}_F(F[\sqrt[n]{a}]) \iff \alpha \in F.$$

2. Suppose F is a field of characteristic zero and it contains an element ζ such that the multiplicative order of ζ 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

$$\sigma_0^d = \mathrm{id} \iff (a(F^\times)^n)^d = (F^\times)^n \text{ in } F^\times/(F^\times)^n.$$

Solution. Using parts (b) and (c) of Problem 1 (where applicable) one has

$$\begin{aligned}
\sigma_0^d = \mathrm{id} &\iff f_a(\sigma_0^d) = \sigma_0^d \iff f_a(\sigma_0)^d = 1 \\
&\iff \Big(\frac{\sigma_0(\sqrt[n]{a})}{\sqrt[n]{a}}\Big)^d = 1 \iff \sigma_0(\sqrt[n]{a}^d) = \sqrt[n]{a}^d \\
&\iff \sqrt[n]{a}^d \in F \overset{(\star)}{\iff} a^d \in (F^\times)^n \\
&\iff a^d(F^\times)^n = (F^\times)^n \iff (a(F^\times)^n)^d = (F^\times)^n.
\end{aligned}$$

[Remark: the $\iff$ labeled with a $(\star)$ requires a line or two of justification, but it is not difficult to verify using the fact that F contains all nth roots of 1.]

(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 cyclic subgroup of $F^\times/(F^\times)^n$ which is generated by $a(F^\times)^n$.

Solution. Using part (b) one sees that $o(\sigma_0) = o(a(F^\times)^n)$, and then because $\mathrm{Aut}_F(F[\sqrt[n]{a}]) = \langle\sigma_0\rangle$, one sees that the two groups in question are cyclic of equal order, hence isomorphic.

3. Suppose F is a field of characteristic zero and it contains an element ζ such that the multiplicative order of ζ is n. For $a \in F$, $\sqrt[n]{a}$ denotes a zero of $x^n - a$. Prove that for $a_1, a_2 \in F^\times$ we have $F[\sqrt[n]{a_1}] = F[\sqrt[n]{a_2}]$ if and only if $\langle a_1(F^\times)^n\rangle = \langle a_2(F^\times)^n\rangle$.

Solution. First suppose $\langle a_1(F^\times)^n\rangle = \langle a_2(F^\times)^n\rangle$. Then we can write $a_1(F^\times)^n = (a_2(F^\times)^n)^i$ for some i, and as a result one has $a_1 = a_2^i b^n$ for some $b \in F$. As a result one has $\sqrt[n]{a_1} = \sqrt[n]{a_2}^i \zeta^j b$ for some j, and in particular $\sqrt[n]{a_1} \in F[\sqrt[n]{a_2}]$ so $F[\sqrt[n]{a_1}] \subseteq F[\sqrt[n]{a_2}]$. The reverse inclusion is completely symmetric.

Now suppose $F[\sqrt[n]{a_1}] = F[\sqrt[n]{a_2}]$. Consider the function f_{a_1} and f_{a_2} as in Problem 1(b). Because these are injective homomorphisms one has

$$|\operatorname{Im}(f_{a_1})| = |\mathrm{Aut}_F(F[\sqrt[n]{a_1}])| = |\mathrm{Aut}_F(F[\sqrt[n]{a_2}])| = |\operatorname{Im}(f_{a_2})|.$$

Thus these two images are subgroups of $\langle\zeta\rangle$ of equal size, hence are equal. If we let σ_0 denote a generator of the automorphism group, one sees that $f_{a_2}(\sigma_0)$ generates $\operatorname{Im}(f_{a_2})$, so as a result one can write $f_{a_1}(\sigma_0) = (f_{a_2}(\sigma_0))^i$ for some i. Using the definition of f_a and rewriting, one has $\sigma_0(\sqrt[n]{a_1}/\sqrt[n]{a_2}^i) = \sqrt[n]{a_1}/\sqrt[n]{a_2}^i$, and then applying Problem 1(c) one sees that $\sqrt[n]{a_1}/\sqrt[n]{a_2}^i \in F$. Calling this element b one has $\sqrt[n]{a_1} = \sqrt[n]{a_2}^i b$ and then $a_1 = a_2^i b^n$. In terms of cosets then we see that $a_1(F^\times)^n = (a_2(F^\times)^n)^i$, so $\langle a_1(F^\times)^n\rangle \subseteq \langle a_2(F^\times)^n\rangle$. The reverse inclusion is symmetric.

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 n.

Solution. Let P be a p-Sylow subgroup of $\mathrm{Aut}_F(E)$. Then by the fundamental theorem of Galois theory, $\mathrm{Fix}(P)$ is an intermediate subfield of E/F with $[\mathrm{Fix}(P):F] = [\mathrm{Aut}_F(E):P]$, which is coprime to p by definition of Sylow subgroup. But by our original hypothesis, if $p \nmid [\mathrm{Fix}(P):F]$ then $\mathrm{Fix}(P) = F$. As a result of the fundamental theorem one then has $P = \mathrm{Aut}_F(E)$, and in particular $[E:F] = |\mathrm{Aut}_F(E)|$ is a power of p.

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

Solution. Let L be a normal closure of E/F. Because E/F is separable, L/F is Galois. Thus part (a) tells us that $[L:F]$ is a power of p, and then by tower law one has $[E:F]$ divides $[L:F]$, hence $[E:F]$ is a power of p.

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

Solution. Let $\ell := \mathrm{char}(F)$. If there exists a finite non-separable extension of F, then Problem 5(b) of Homework 1 tells us that $\phi : F \to F$, $\phi(a) = a^\ell$ cannot be surjective. If we take some $t \in F \setminus F^\ell$ then we let E be a splitting field of $x^\ell - t$ over F and $\alpha \in E$ a root of $x^\ell - t$. One necessarily has $m_{\alpha,F}(x) | x^\ell - t$, and $x^\ell - t = (x-\alpha)^\ell$ in $E[x]$ so one has $m_{\alpha,F}(x) = (x-\alpha)^k$ for some $2 \le k \le \ell$ (notice one cannot have $k = 1$ because this would imply that $\alpha \in F$, contradicting the fact that $t \notin F^\ell$). By examining the constant term one sees that $\alpha^k \in F$. If we rephrase this as the statement $(\alpha F^\times)^k = F^\times$ in the group $E^\times / F^\times$, we can use group theory: one has $\alpha^\ell = t \in F$, so $(\alpha F^\times)^\ell = F^\times$, and thus the order of $\alpha F^\times$ divides ℓ. But ℓ is prime and $\alpha \notin F^\times$, so this order is exactly ℓ. Now from the statement $(\alpha F^\times)^k = F^\times$ one sees that the order ℓ must divide k. But $k \le \ell$ so we find $k = \ell$, and thus $m_{\alpha,F}(x) = (x-\alpha)^\ell = x^\ell - t$, and in particular $x^\ell - t$ is irreducible in $F[x]$. As a result we see that E/F is a finite extension of degree ℓ, and then by the original hypothesis one has $p|\ell$, so because these are primes we find $p = \ell = \mathrm{char}(F)$.

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.

Solution. The statement is trivial in characteristic 0, so suppose $\mathrm{char}(F) = p > 0$. Then E/F is purely inseparable if and only if for every $\alpha \in E$ there exists some $k \ge 0$ such that $\alpha^{p^k} \in F$.

First suppose E/F is purely inseparable. If $\alpha \in K$, then $\alpha \in E$ so there exists $k \ge 0$ such that $\alpha^{p^k} \in F$, which shows K/F is purely inseparable. In addition if $\alpha \in E$, then taking $k \ge 0$ so that $\alpha^{p^k} \in F$, we also have $\alpha^{p^k} \in K$, so E/K is purely inseparable.

Conversely suppose E/K and K/F are purely inseparable. If $\alpha \in E$ then because E/K is purely inseparable we can find $k \ge 0$ with $\alpha^{p^k} \in K$. Then because K/F is purely inseparable we can find $\ell \ge 0$ such that $(\alpha^{p^k})^{p^\ell} \in F$. Thus $\alpha^{p^{k+\ell}} \in F$ and we see that E/F is purely inseparable.

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

Outline of solution. First consider the case that the extension is simple, say $E = F[\alpha]$. From our equivalent conditions for an extension to be purely inseparable, we know that $m_{\alpha,F}(x) = x^{p^k} - a$ for some $k \ge 0$ and $a \in F$. As a result one has

$$[E : F] = [F[\alpha] : F] = \deg(m_{\alpha,F}) = p^k,$$

which gives the result in this special case.

For the general case, write $E = F[\alpha_1, \dots, \alpha_n]$ and consider the tower

$$F \subseteq F[\alpha_1] \subseteq F[\alpha_1, \alpha_2] \subseteq \cdots \subseteq F[\alpha_1, \dots, \alpha_{n-1}] \subseteq F[\alpha_1, \dots, \alpha_n] = E.$$

At each step of the tower apply the simple case to find $[F[\alpha_1, \dots, \alpha_{i+1}] : F[\alpha_1, \dots, \alpha_i]]$ is a power of p (we use part (a) to see that this extension is still purely inseparable). Applying the tower law to the tower one sees $[E : F]$ is a power of p as well.

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

Solution. If E/F is separable then this is exactly Homework 2 Problem 4(b). If E/F is non-separable we can apply part (c) to find $\mathrm{char}(F) = p$. In this case consider the separable closure E_{sep} of F in E. We know that E/E_{sep} is a purely inseparable extension and E_{sep}/F is a separable extension. From Homework 2 Problem 4(b) we have that $[E_{\mathrm{sep}} : F]$ is a power of p, and from part (b) above we have that $[E : E_{\text{sep}}]$ is a power of p. Using tower law we conclude the result.

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 ratioanl functions. Suppose $\sigma, \tau \in \operatorname{Aut}_F(F(t))$ are such that $\sigma(t) := t + 1$ and $\tau(t) = -t$. Let H be the subgroup generated by σ and τ.
   (a) Prove that $\operatorname{Fix}(\tau) = F(t^2)$ and $\operatorname{Fix}(\sigma) = F(t^p - t)$.

   Solution. Recall we have seen in problem session that if $u = \frac{f(t)}{g(t)}$ with $f, g \in F[t]$ and $\gcd(f, g) = 1$, one has that $F(t)/F(u)$ is a finite extension with $[F(t) : F(u)] = \max\{\deg(f), \deg(g)\}$.

   Clearly one has $\operatorname{Fix}(\tau) \subseteq F(t^2)$. Writing $\operatorname{Fix}(\tau) = \operatorname{Fix}(\langle\tau\rangle)$ and using Theorem 26.1.3 one has

   $$[F(t) : \operatorname{Fix}(\tau)] = [F(t) : \operatorname{Fix}(\langle\tau\rangle)] = |\operatorname{Aut}_{\operatorname{Fix}(\langle\tau\rangle)}(F(t))| = |\langle\tau\rangle| = 2.$$

   Using the fact stated above (or via more elementary methods), one also has $[F(t) : F(t^2)] = 2$. Now we can consider the tower applied to $\operatorname{Fix}(\tau) \subseteq F(t^2) \subseteq F(t)$, and get

   $$2 = [F(t) : \operatorname{Fix}(\tau)] = [F(t) : F(t^2)][F(t^2) : \operatorname{Fix}(\tau)] = 2[F(t^2) : \operatorname{Fix}(\tau)],$$

   and cancelling we find $[F(t^2) : \operatorname{Fix}(\tau)] = 1$, so $F(t^2) = \operatorname{Fix}(\tau)$.

   For the other equality we apply similar techniques: one can easily verify $F(t^p - t) \subseteq \operatorname{Fix}(\sigma)$, then use a similar chain of equalities to find $[F(t) : \operatorname{Fix}(\sigma)] = o(\sigma) = p$. Then apply our fact above to find $[F(t) : F(t^p - t)] = p$, and conclude $F(t^p - t) = \operatorname{Fix}(\sigma)$ using tower law.

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

   Outline of solution. One has inclusions $F((t^p - t)^2) \subseteq \operatorname{Fix}(H) \subseteq \operatorname{Fix}(\tau) \cap \operatorname{Fix}(\sigma) = F(t^2) \cap F(t^p - t)$. We can use the same fact as before to see that $[F(t) : F((t^p - t)^2)] = 2p$, so by the same methods used in (a) it suffices to see that $[F(t) : F(t^2) \cap F(t^p - t)] = 2p$. In fact, the inclusions above (along with tower law) gives us $[F(t) : F(t^2) \cap F(t^p - t)] \leq 2p$, so we just need to see the reverse inequality. But considering the diagram of extensions

   $$\begin{tikzcd}
   & F(t) \arrow[dl, dash, "2"'] \arrow[dr, dash, "p"] & \\
   F(t^2) \arrow[dr, dash] & & F(t^p - t) \arrow[dl, dash] \\
   & F(t^2) \cap F(t^p - t) &
   \end{tikzcd}$$

   one sees with tower law that 2 and p both divide $[F(t) : F((t^p - t)^2]$, and because p is odd then we see that $2p$ divides this quantity as well, giving the desired inequality.

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

   Solution. Because $F((t^p - t)^2) = \operatorname{Fix}(H)$ we can apply Theorem 26.1.3 to find $F(t)/F((t^p - t)^2)$ is Galois with $\operatorname{Aut}_{F((t^p - t)^2)}(F(t)) = H$. Because $F(t^2) = \operatorname{Fix}(\tau) = \operatorname{Fix}(\langle\tau\rangle)$, we have by the fundamental theorem of Galois theory that $F(t^2)/F((t^p - t)^2)$ is normal if and only if $\langle\tau\rangle$ is a normal subgroup of H. But one can directly verify that $\sigma\tau\sigma^{-1} \notin \langle\tau\rangle$, so we conclude this extension is not normal.

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

Solution. Theorem 29.1.4 says that L/F is a normal extension, so it suffices to prove separability. Notice f is also a separable polynomial of $E[x]$, because any irreducible factor as an element of $E[x]$

divides an irreducible factor from $F[x]$, and we know each of these has distinct roots in a splitting field. Thus L/E is separable as it is the splitting field of a separable polynomial over E. We have by hypothesis that E/F is separable, and then L/E and E/F both separable implies L/F separable as well.

Alternatively, if E is a splitting field of a separable polynomial $g \in F[x] \setminus F$ over F, then one can directly prove that L is the splitting field of $f(x)g(x)$ over F, and $f(x)g(x)$ is a separable polynomial because both $f(x)$ and $g(x)$ are.

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 $H_1 = S_p$.

   Solution. Recall every element of S_p can be written as a product of transpositions, so it suffices to show that any transposition (i, j) is in H_1. Let $\gamma := \tau\sigma = (0, 1)(0, 1, \ldots, p-1) = (1, \ldots, p-1)$, which is in H_1 because τ and σ are. Then for each $i \in [1, p-2]$ one has $(i, i+1) = \gamma^i \circ \tau \circ \gamma^{-i} \in H_1$. From this we see that $(1, 2)(0, 1)(1, 2)^{-1} = (0, 2)$ is in H_1. Then $(2, 3)(0, 2)(2, 3)^{-1} = (0, 3)$ is also in H_1, and inductively we find that $(i-1, i)(0, i-1)(i-1, i) = (0, i)$ is in H_1 for each $i \in [1, p-1]$ Finally for any i, j we deduce that $(i, j) = (0, i)(0, j)$ is inside H_1 as well. Thus we have shown all transpositions are in H_1 and we are done.

   (b) Prove that $H_a = S_p$.

   Solution. Notice for any integer i that $\sigma^i(0, a)\sigma^{-i} = (a, a+i)$ is an element of H_a, where we consider addition modulo p. Applying this fact for $i = ka$, this says that $(ka, (k+1)a)$ is inside H_a for any integer k. Notice then $(0, 2a) = (a, 2a)(0, a)(a, 2a)^{-1}$ is inside H_a, and continuing inductively we find that $(0, ka) = ((k-1)a, ka)(0, (k-1)a)((k-1)a, ka)^{-1}$ is inside H_a for any k. In particular because $a \in [1, p-1]$ we can choose some k for which $ka = 1$ in $\mathbb{Z}_p$, and then this says that $(0, 1) \in H_a$. But then using part (a) we have inclusions

$$S_p = H_1 = \langle \sigma, (0, 1) \rangle \subseteq H_a \subseteq S_p,$$

   and then we deduce all the above groups are equal, so in particular $H_a = S_p$.

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 $\mathrm{Aut}_{\mathbb{Q}}(E) \simeq S_p$.

   See Theorem 30.3.3 in the notes.

   (b) Prove that f is not solvable by radicals over $\mathbb{Q}$.

   See Theorem 30.3.3 in the notes.

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.

Outline of solution. Suppose $\alpha, \beta \in F_{\mathrm{ab}}$. Because $F[\alpha]/F$ is Galois there is some separable polynomial $f \in F[x] \setminus F$ such that $F[\alpha]$ is a splitting field of f over F, and similarly there is some separable $g \in F[x] \setminus F$ such that $F[\beta]$ is a splitting field of g over F. One can verify then that $F[\alpha, \beta]$ is a splitting field of the (separable) polynomial $f(x)g(x)$ over F, so $F[\alpha, \beta]/F$ is Galois. Next, we see that we have a homomorphism

$$\mathrm{Aut}_F(F[\alpha,\beta]) \to \mathrm{Aut}_F(F[\alpha]) \times \mathrm{Aut}_F(F[\beta]), \quad \sigma \mapsto (\sigma|_{F[\alpha]}, \sigma|_{F[\beta]}),$$

where we note these restrictions are well-defined because $F[\alpha]$ and $F[\beta$ are both normal over F. It is easy to see this homomorphism is also injective, and thus the fact that $\mathrm{Aut}_F(F[\alpha])$ and $\mathrm{Aut}_F(F[\beta])$ are both abelian implies $\mathrm{Aut}_F(F[\alpha,\beta])$ is abelian as well. In particular, by the fundamental theorem of Galois theory this implies that $F[\alpha-\beta]$ is Galois over F, because the corresponding subgroup of $\mathrm{Aut}_F(F[\alpha,\beta])$ is automatically normal. Furthermore, one has a surjective map (see Theorem 23.1.1)

$$\mathrm{Aut}_F(F[\alpha,\beta]) \to \mathrm{Aut}_F(F[\alpha-\beta]), \quad \sigma \mapsto \sigma|_{F[\alpha-\beta]}$$

and thus the fact that $\mathrm{Aut}_F(F[\alpha,\beta])$ is abelian implies the same for $\mathrm{Aut}_F(F[\alpha-\beta])$ and then we see that $\alpha-\beta \in F_{\mathrm{ab}}$. Similarly one has $\alpha\beta$ and (when $\beta \neq 0$) α/β are both in F_{ab}/F as well, so F_{ab} is a field.

If $\alpha \in F_{\mathrm{ab}}$ then $F[\alpha]/F$ being Galois in particular means α is separable over F, so F_{ab} is separable. Furthermore, one has that $m_{\alpha,F}$ splits into linear factors in $F[\alpha]$, and hence the same is true inside F_{ab}, so F_{ab}/F is normal as well. This completes the proof that F_{ab}/F is a Galois extension.

For the final part of the proof, if L/F is finite then F_{ab}/F is finite as well, and because it is separable (what we have just shown above) the Primitive Element Theorem (Theorem 27.2.2) implies that $F_{\mathrm{ab}} = F[\alpha]$ for some $\alpha \in F_{\mathrm{ab}}$; but then by definition of F_{ab} we have that $\mathrm{Aut}_F(F_{\mathrm{ab}}) = \mathrm{Aut}_F(F[\alpha])$ is abelian.

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.

Solution. We have seen in class that E_{sep} is a field and E_{sep}/F is a separable extension by definition, so we need to show normality. Suppose $\alpha \in E_{\mathrm{sep}}$. We want to see that $m_{\alpha,F}$ splits into linear factors in E_{sep}. Because E/F is normal we have can split $m_{\alpha,F}$ into linear factors in E, say $m_{\alpha,F}(x) = \prod_i (x-\beta_i)$. Then notice that for each i one has $m_{\beta_i,F} = m_{\alpha,F}$, so β_i is separable over F because α is. But this means $\beta_i \in E_{\mathrm{sep}}$ so this gives the conclusion we wanted.

(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.

Solution. The statement is trivial in characteristic 0 so suppose $\mathrm{char}(F) = p > 0$. Surjectivity of r follows from the fact that E/F is normal, see for instance Proposition 23.1.1. For injectivity, suppose $r(\theta) = \mathrm{id}$, so $\theta(\beta) = \beta$ for all $\beta \in E_{\mathrm{sep}}$. Then if $\alpha \in E_{\mathrm{sep}}$ one has $\alpha^{p^k} \in E_{\mathrm{sep}}$ for some $k \geq 0$ because E/E_{sep} is purely inseparable. But then one has $\theta(\alpha^{p^k}) = \alpha^{p^k}$, and from this one subtracts and finds that $(\theta(\alpha)-\alpha)^{p^k} = 0$, which implies $\theta(\alpha) = \alpha$. Thus $\theta = \mathrm{id}$ and this shows r is injective.

(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.

Solution. Theorem 26.1.3 immediately implies E/K is Galois with $\mathrm{Aut}_K(E) = \mathrm{Aut}_F(E)$. Thus we can calculate

$$[E : K] = |\mathrm{Aut}_K(E)| = |\mathrm{Aut}_F(E)| = |\mathrm{Aut}_F(E_{\mathrm{sep}})| = [E_{\mathrm{sep}} : F].$$

To see K/F is purely inseparable we again suppose we are in characteristic p (the characteristic 0 case being trivial) and suppose $\alpha \in K$. Because $\alpha \in E$ we can find $k \geq 0$ such that $\alpha^{p^k} \in E_{\mathrm{sep}}$. We will show $\alpha^{p^k} \in F$ by showing it is fixed by every $\theta \in \mathrm{Aut}_F(E_{\mathrm{sep}})$; for any such θ we know by part (b) that $\theta = \widetilde{\theta}|_{E_{\text{sep}}}$ for some $\widetilde{\theta} \in \text{Aut}_F(E)$. Then because $\alpha \in K = \text{Fix}(\text{Aut}_F(E))$ we have

$$\theta(\alpha^{p^k}) = \widetilde{\theta}(\alpha^{p^k}) = \widetilde{\theta}(\alpha)^{p^k} = \alpha^{p^k}.$$

We conclude $\alpha^{p^k} \in F$ and because $\alpha \in K$ was arbitrary we conclude the result.

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

Let $E_{\text{sep},K}$ be the separable closure of K in E/K, let $E_{\text{sep},F}$ be the separable closure of F in E/F, and let $K_{\text{sep},F}$ be the separable closure of F in K/F.

(a) In the above setting prove that $K_{\text{sep},F} \subseteq E_{\text{sep},F} \subseteq E_{\text{sep},K}$.

Solution. If $\alpha \in K_{\text{sep},F}$ then $\alpha \in K$ and $m_{\alpha,F}$ is separable in $F[x]$. Because $K \subseteq E$ it is immediate that $\alpha \in E_{\text{sep},F}$ as well. Now if $\alpha \in E_{\text{sep},F}$ then $\alpha \in E$ with $m_{\alpha,F}$ separable. One has $m_{\alpha,K}|m_{\alpha,F}$ in $K[x]$ so $m_{\alpha,K}$ is separable as well, and thus $\alpha \in E_{\text{sep},K}$. This shows the desired inclusions.

(b) Argue that there is $\alpha \in E_{\text{sep},F}$ such that $E_{\text{sep},F} = K_{\text{sep},F}[\alpha]$.

Solution. We have that $E_{\text{sep},F}/F$ is separable by construction. Because $F \subseteq K_{\text{sep},F} \subseteq E_{\text{sep},F}$, and the fact that separability satisfies a block-tower phenomena (Theorem 28.2.1) one finds that $E_{\text{sep},F}/K_{\text{sep},F}$ is separable, and it is finite because E/F is finite by hypothesis. Thus it follows from the Primitive Element Theorem (Theorem 27.2.2) that $E_{\text{sep},F} = K_{\text{sep},F}[\alpha]$ for some $\alpha \in E_{\text{sep},F}$.

(c) Prove that $E_{\text{sep},K}/K[\alpha]$ is both separable and purely inseparable. Deduce that $E_{\text{sep},K} = K[\alpha]$.

Solution. By construction $E_{\text{sep},K}/K$ is separable, and then $E_{\text{sep},K}/K[\alpha]$ is also separable. On the other hand, recall that $E/E_{\text{sep},F}$ is purely inseparable. But we have inclusions

$$E_{\text{sep},F} = K_{\text{sep},F}[\alpha] \subseteq K[\alpha] \subseteq E_{\text{sep},K} \subseteq E,$$

and because we have proved in the previous homework that purely inseparable extensions satisfy a block-tower phenomena we deduce that $E_{\text{sep},K}/K[\alpha]$ is purely inseparable. The only extensions which are both separable and purely inseparable are trivial extensions, so $E_{\text{sep},K} = K[\alpha]$.

(d) Prove that $m_{\alpha,K}|m_{\alpha,K_{\text{sep},F}}$ and $m_{\alpha,K_{\text{sep},F}}|m^q_{\alpha,K}$ where q is either 1 if $\text{char}(F) = 0$ or a power of p if $\text{char}(F) = p > 0$. Deduce that $m_{\alpha,K} = m_{\alpha,K_{\text{sep},F}}$.

Solution. The statement is trivial if $\text{char}(F) = 0$ so suppose $\text{char}(F) = p > 0$. The fact that $m_{\alpha,K}|m_{\alpha,K_{\text{sep},F}}$ is immediate from $K_{\text{sep},F} \subseteq K$. On the other hand let's write $m_{\alpha,F}(x) = c_0 + \cdots + c_{n-1}x^{n-1} + x^n$ with $c_i \in K$. Because $K/K_{\text{sep},F}$ is purely inseparable for each i we can find some $m \geq 0$ such that $c_i^{p^{m_i}} \in K_{\text{sep},F}$. If we take $m = \text{lcm}(m_i)$ and $q = p^m$ then $c_i^q \in K_{\text{sep},F}$ for each i. As a result we have $m^q_{\alpha,K} \in K_{\text{sep},F}[x]$, and this polynomial has α as a root so we deduce that $m_{\alpha,K_{\text{sep},F}}|m^q_{\alpha,K}$.

For the second claim notice that $m_{\alpha,K_{\text{sep},F}}$ and $m_{\alpha,K}$ are both separable, and by the facts proved above the two polynomials have exactly the same roots (take in some splitting field). Thus one concludes that $m_{\alpha,K} = m_{\alpha,K_{\text{sep},F}}$.

(e) Prove that $[E : F]_s = [E : K]_s[K : F]_s$.

Solution. Using part (b) we calculate

$$[E : F]_s = [E_{\text{sep},F} : F] = [K_{\text{sep},F}[\alpha] : F] = [K_{\text{sep},F}[\alpha] : K_{\text{sep},F}][K_{\text{sep},F} : F].$$

Now we use parts (c) and (d) to calculate

$$[K_{\text{sep},F}[\alpha] : K_{\text{sep},F}] = \deg(m_{\alpha,K_{\text{sep},F}}) = \deg(m_{\alpha,K}) = [K[\alpha] : K] = [E_{\text{sep},K} : K] = [E : K]_s.$$

Because $[K_{\mathrm{sep},F} : F] = [K : F]_s$, returning to the first line we get the result.

4. Suppose F is a field, $L := F(x_1, \ldots, x_n)$ is the field of fractions of $F[x_1, \ldots, x_n]$. For $\sigma \in S_n$ and $f \in L$, let $T_\sigma(f) = f(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$.
   (a) Prove that $T : S_n \to \mathrm{Aut}_F(L)$, $(T(\sigma))(f) := T_\sigma(f)$ is an injective group homomorphism.

   Solution. One needs to show that $T_{\sigma\circ\tau} = T_\sigma \circ T_\tau$ for $\sigma, \tau \in S_n$. We calculate for $f \in L$

$$\begin{aligned} T_\sigma(T_\tau(f)) &= T_\tau(f)(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}) = f(x_{\tau^{-1}(\sigma^{-1}(1))}, \ldots, x_{\tau^{-1}(\sigma^{-1}(n))}) \\ &= f(x_{(\sigma\circ\tau)^{-1}(1)}, \ldots, x_{(\sigma\circ\tau)^{-1}(n)}) = T_{\sigma\circ\tau}(f). \end{aligned}$$

   This shows T is a homomorphism. To see it is injective, suppose $T(\sigma) = \mathrm{id}$, i.e. $T_\sigma(f) = f$ for all f. Taking $f = x_i$ this says that $x_{\sigma^{-1}(i)} = x_i$, so $\sigma^{-1}(i) = i$ for each i which implies $\sigma = \mathrm{id}$.

   (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 $E := F(s_1, \ldots, s_n)$. Prove that L is a splitting field of $t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n$ over E. Deduce that $[L : E] \le n!$.

   Solution. Notice that the x_i are algebraic over E by construction, and by construction the polynomial in question splits in L. The former, in particular, implies that $E(x_1, \ldots, x_n) = E[x_1, \ldots, x_n]$, and we find that

$$L = F(x_1, \ldots, x_n) \subseteq E(x_1, \ldots, x_n) \subseteq E[x_1, \ldots, x_n] \subseteq L.$$

   Thus one has equality all across the above inclusions, so in particular $L = E[x_1, \ldots, x_n]$ and so L is the splitting field of $t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n$ over E. The second claim follows the fact L is the splitting field of a degree n polynomial over E.

   (c) Prove that $K = E$.

   Solution. The inclusion $E \subseteq K$ is clear. But because $K = \mathrm{Fix}(T(S_n))$ we know that L/K is Galois with $\mathrm{Aut}_K(L) = T(S_n)$, and in particular $[L : K] = |T(S_n)| = |S_n| = n!$. Using tower law we see that $[L : E] = [L : K][K : E] = n![K : E]$, and then the fact that $[L : E] \le n!$ by part (b) implies $[K : E] = 1$, so $K = E$.

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

   Solution. We calculate

$$\begin{aligned} T(G(f)) &= \{T_\sigma \mid \sigma \in G(f)\} = \{T_\sigma \mid T_\sigma(f) = f\} \\ &= \{\theta \in T(S_n) \mid \theta(f) = f\} = \{\theta \in \mathrm{Aut}_K(L) \mid \theta(f) = f\} \\ &= \mathrm{Aut}_{K[f]}(L). \end{aligned}$$

   Now the result follows from the fundamental theorem of Galois theory.

   (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 $g = \theta(f)$.

   Solution. By fundamental theorem of Galois theory and part (d) one has

$$\begin{aligned} G(f) \subseteq G(g) &\iff \mathrm{Fix}(T(G(g))) \subseteq \mathrm{Fix}(T(G(f))) \\ &\iff K[g] \subseteq K[f] \\ &\iff g \in K[f] \iff \text{there exists } \theta \in K[t] \text{ such that } g = \theta(f). \end{aligned}$$

5. Week 5

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

Solution. Suppose $f \in E[x] \setminus E$. Then $f \in L[x] \setminus L$ so because L is algebraically closed there is some zero $\alpha \in L$ of f. We claim that $\alpha \in E$: we have that α is algebraic over E, so $E[\alpha]/E$ is algebraic, and also E/F is algebraic, so $E[\alpha]/F$ is also algebraic and thus the element α is algebraic over F, but then by definition of E this means that $\alpha \in E$.

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.

   Solution. Suppose L/E is an algebraic extension; we will show that $L = E$. Because L/E and E/F are both algebraic, L/F is also algebraic. Thus if $\alpha \in L$ then it is algebraic over F so $m_{\alpha,F} \in F[x]$ exists and by assumption decomposes into linear factors in $E[x]$. Because α is a zero of $m_{\alpha,F}$ this implies $\alpha \in E$, proving $L = E$.

3. Suppose F is a perfect field, and $\overline{F}$ is an algebraic closure of F. Let
$$\mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F) = \{E \in \mathrm{Int}(\overline{F}/F) \mid E/F \text{ is a finite normal extension}\}.$$

   (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.

   Solution. The map r_E is well-defined because E/F is normal, so $\phi(E) = E$ for any $\phi \in \mathrm{Aut}_F(\overline{F})$. Surjectivity is Lemma 33.4.1.

   (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 $r_{E',E}(\phi) := \phi|_E$. Argue that $r_{E',E}$ is a well-defined surjective group homomorphism and $r_E = r_{E',E} \circ r_{E'}$.

   Solution. Again well-definedness is because E/F is normal, so the restriction in fact is an automorphism of E (which is still F-linear). Surjectivity comes from E'/F being normal, for instance Proposition 23.1.1.

   (c) Let $G(\overline{F}/F) := \{(\phi_E) \in \prod_{E \in \mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F)} \mathrm{Aut}_F(E) \mid \forall E \subseteq E', r_{E',E}(\phi_{E'}) = \phi_E\}$. 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.

   Solution. To check well-definedness, we just need to see that $r(\phi) \in G(\overline{F}/F)$, i.e. one needs to check that for $E \subseteq E'$ one has $r_{E',E}(r_{E'}(\phi)) = r_E(\phi)$. This is really just the equality $(\phi|_{E'})|_E = \phi|_E$, which is clear.

   To show injectivity, suppose $r(\phi) = \mathrm{id}_{G(\overline{F}/F)} = (\mathrm{id}_E)_{E \in \mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F)}$. This says that $r_E(\phi) = \mathrm{id}_E$ for all $E \in \mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F)$. Then for any $\alpha \in E$ one can choose any $E \in \mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F)$ containing α (for instance take the normal closure of $F[\alpha]/F$ in $\overline{F}$), and then one has $\phi(\alpha) = \phi|_E(\alpha) = r_E(\alpha) = \mathrm{id}_E(\alpha) = \alpha$. Because α was arbitrary this shows ϕ is the identity on $\overline{F}$.

   For surjectivity, suppose $(\phi_E)_{E \in \mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F)} \in G(\overline{F}/F)$. Then define $\phi : \overline{F} \to \overline{F}$ as follows: if $\alpha \in E$, choose any $E \in \mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F)$ containing α and define $\phi(\alpha) := \phi_E(\alpha)$. One needs to check this does not depend on our choice of E: if both $E, E' \in \mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F)$ contain α, then consider the compositum E'' of E and E' in $\overline{F}$. We have seen that E''/F is finite normal because the same is true for both E and E', and one has $E \subseteq E''$ and $E' \subseteq E''$. Using the compatibility of the ϕ_E we find $\phi_E(\alpha) = (r_{E'',E}(\phi_{E''}))(\alpha) = \phi_{E''}|_E(\alpha) = \phi_{E''}(\alpha)$. Similarly one has $\phi_{E'}(\alpha) = \phi_{E''}(\alpha)$, and thus $\phi_E(\alpha) = \phi_{E'}(\alpha)$. We see that $\phi(\alpha)$ does not depend on the choice of E, so ϕ is well-defined, and one can readily verify that ϕ is an F-automorphism of $\overline{F}$ satisfying $r(\phi) = (\phi_E)_{E \in \mathrm{Int}_{\mathrm{f,n}}(\overline{F}/F)}$.

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 $F_n \in \mathrm{Int}_{\mathrm{f,n}}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ that is isomorphic to $\mathbb{F}_{p^n}$.

   Solution. Recall $\mathbb{F}_{p^n}$ is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Thus if one lets $\alpha_1, \dots, \alpha_{p^n}$ denote the zeros of $x^{p^n} - x$ in $\overline{\mathbb{F}}_p$ then $\mathbb{F}_p[\alpha_1, \dots, \alpha_{p^n}]$ is the unique subfield of $\overline{\mathbb{F}}_p$ which is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$, and thus the unique subfield of $\overline{\mathbb{F}}_p$ which 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 $\overline{\mathbb{F}}_p = \bigcup_{n=1}^\infty F_n$.

   Solution. If $E \in \mathrm{Int}_{\mathrm{f,n}}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ then $E/\mathbb{F}_p$ is finite, so in particular E is a finite field of characteristic p and thus $E \simeq \mathbb{F}_{p^n}$ for some n, but then from part (a) we see that $E = F_n$. This shows the first equality. For the second equality one inclusion is clear, and conversely if $\alpha \in \overline{\mathbb{F}}_p$ then $\mathbb{F}_p[\alpha]$ is a finite field contained in $\overline{\mathbb{F}}_p$, so by the same reasoning above $\mathbb{F}_p[\alpha] = F_n$ for some $n \in \mathbb{Z}^+$, in particular $\alpha \in F_n$.

   (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 $\mathrm{Aut}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p) = \widehat{\mathbb{Z}}$.

   Outline of solution. One can invoke Problem 3(c) here: we know by 4(a) that $\mathrm{Int}_{\mathrm{f,n}}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \{F_n \mid n \in \mathbb{Z}^+\}$, one has $\mathrm{Aut}_F(F_n) \simeq \mathbb{Z}_n$ and also $F_n \subseteq F_{n'} \iff n|n'$. Thus one just needs to know that the compatibility condition $r_{F_{n'},F_n}(\phi_{F_{n'}}) = \phi_{F_n}$ corresponds to $a_n' \equiv a_n \pmod{n}$ whenever ϕ_{F_k} corresponds to a_k under $\mathrm{Aut}_{\mathbb{F}_p}(F_k) \simeq \mathbb{Z}_k$ for $k = n, n'$. This can be summarized as the commutativity of the following square (which is straightward to check):

$$\begin{tikzcd}
\mathrm{Aut}_{\mathbb{F}_p}(F_{n'}) \arrow[r, "r_{F_{n'},F_n}"] \arrow[d, "\simeq"] & \mathrm{Aut}_{\mathbb{F}_p}(F_n) \arrow[d, "\simeq"] \\
\mathbb{Z}_{n'} \arrow[r] & \mathbb{Z}_n
\end{tikzcd}$$

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

   Solution. Suppose $(a_n)_{n\geq 2}$ is a torsion element of $\widehat{\mathbb{Z}}$. This means there is some $k \in \mathbb{Z}^+$ such that $k\cdot(a_n)_{n\geq 2} = 0$, i.e. n divides ka_n for each n. For a given n, one in particular has $kn|ka_{nk}$, but one can verify this implies $n|a_{nk}$. Because $a_{nk} \equiv a_n \pmod{n}$ by the definition of $\widehat{\mathbb{Z}}$ we conclude $n|a_n$, i.e. $a_n = 0$ in $\mathbb{Z}_n$. This proves $(a_n)_{n\geq 2} = 0$.

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

   Solution. Because $\overline{\mathbb{F}}_p/\mathbb{F}_p$ is Galois (recall we have seen $\mathbb{F}_p$ is perfect) we have that $\overline{\mathbb{F}}_p/E$ is Galois, so in particular $[\overline{\mathbb{F}}_p : E] = |\mathrm{Aut}_E(\overline{\mathbb{F}}_p)|$. Now $\mathrm{Aut}_E(\overline{\mathbb{F}}_p)$ is a finite subgroup of $\mathrm{Aut}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p) \simeq \widehat{\mathbb{Z}}$, and so any non-identity element of $\mathrm{Aut}_E(\overline{\mathbb{F}}_p)$ is torsion, but we have seen that $\widehat{\mathbb{Z}}$ has no (non-identity) torsion elements, so we must deduce $\mathrm{Aut}_E(\overline{\mathbb{F}}_p) = \{\mathrm{id}\}$, and hence $[\overline{\mathbb{F}}_p : E] = 1$, i.e. $E = \overline{\mathbb{F}}_p$.

6. Week 6

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

Solution. Recall $\zeta_n = e^{2\pi i/n} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$; thus $\cos(\frac{2\pi}{n}) = \frac{1}{2}(\zeta_n + \zeta_n^{-1})$. In particular we have $\mathbb{Q}[\cos(\frac{2\pi}{n})] \subseteq \mathbb{Q}[\zeta_n]$. Because $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ is an Galois extension with abelian automorphism group, we deduce that $\mathbb{Q}[\cos(\frac{2\pi}{n})]/\mathbb{Q}$ is Galois as well.

Recall that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n]) \simeq \mathbb{Z}_n^\times$ via $\sigma \mapsto [i]_n$ where $\sigma(\zeta_n) = \zeta_n^i$. If we denote this isomorphism by φ then one has $\{\pm 1\} = \varphi(\{1, \tau\})$ where τ is the restriction of complex conjugation to $\mathbb{Q}[\zeta_n]$. If we can show that $\mathrm{Aut}_{\mathbb{Q}[\cos(\frac{2\pi}{n})]}(\mathbb{Q}[\zeta_n]) = \{1, \tau\}$ then this means φ induces an isomorphism

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\cos(\frac{2\pi}{n})]) \simeq \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n]) / \mathrm{Aut}_{\mathbb{Q}[\cos(\frac{2\pi}{n})]}(\mathbb{Q}[\zeta_n]) \simeq \mathbb{Z}_n^\times / \{\pm 1\},$$

which is the result we want. To show the equality, notice the inclusion $\{1, \tau\} \subseteq \mathrm{Aut}_{\mathbb{Q}[\cos(\frac{2\pi}{n})]}(\mathbb{Q}[\zeta_n])$ is clear. On the other hand, notice that ζ_n is a root of $x^2 - 2\cos(\frac{2\pi}{n})x + 1 \in \mathbb{Q}[\cos(\frac{2\pi}{n})][x]$, which shows that $[\mathbb{Q}[\zeta_n] : \mathbb{Q}[\cos(\frac{2\pi}{n})]] \le 2$ from which we deduce equality holds.

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 $(F[\alpha_1])[x]$.

   Solution. Notice because $m_{\alpha_1,F} | f$ one has $[F[\alpha_1] : F] \le \deg(f) = n$. In $(F[\alpha_1])[x]$ one has a factorization $f(x) = (x - \alpha_1)g(x)$, and then because $\alpha_1 \ne \alpha_2$ one has $m_{\alpha_2,F[\alpha_1]} | g$ in $(F[\alpha_1])[x]$. As a result $[F[\alpha_1, \alpha_2] : F[\alpha_1]] \le \deg(g) = n - 1$. But we know that $[F[\alpha_1, \alpha_2] : F] = n(n-1)$. So if, for instance, $[F[\alpha_1] : F] < n$ we would deduce that

   $$n(n-1) = [F[\alpha_1, \alpha_2] : F] = [F[\alpha_1, \alpha_2] : F[\alpha_1]][F[\alpha_1] : F] < n(n-1),$$

   giving a contradiction. We deduce $[F[\alpha_1] : F] = n$ and similarly $[F[\alpha_1, \alpha_2] : F[\alpha_1]] = n - 1$. As a result one sees that $\deg(m_{\alpha_1,F}) = n$ so $m_{\alpha_1,F} = f$, and similarly $m_{\alpha_2,F[\alpha_1]} = g$. We deduce that f is irreducible in $F[x]$ and has two irreducible factors (given by $x - \alpha_1$ and $g(x)$) in $(F[\alpha_1])[x]$.

   (b) Prove that $\mathcal{G}_{f,F}$ acts two-transitively on $\{\alpha_1, \ldots, \alpha_n\}$.

   Outline of solution. Fix some $i \ne j$. Because f is irreducible in $F[x]$, one can find, using Lemma 16.2.2, an F-isomorphism $\theta : F[\alpha_1] \to F[\alpha_i]$ sending $\alpha_1 \mapsto \alpha_i$. Now we know from (a) we have $f(x) = (x - \alpha_1)g(x)$ in $(F[\alpha_1])[x]$ with $g(x)$ irreducible; one sees that α_2 is a root of g while α_j is a root of $\theta(g)$, so using Lemma 16.2.2 again one can extend this isomorphism to an isomorphism $F[\alpha_1][\alpha_2] \to F[\alpha_i][\alpha_j]$ sending $\alpha_2 \mapsto \alpha_j$. From here one just needs to extend this isomorphism to the splitting field to get the desired element of $\mathcal{G}_{f,F}$.

   (c) Let $g(x) := m_{\alpha_1+\alpha_2,F}(x)$. Prove that $g(\alpha_i + \alpha_j) = 0$ for every $i \ne j$.

   Solution. For any $i \ne j$, by (b) we can find $\theta \in \mathcal{G}_{f,F}$ such that $\theta(\alpha_1) = \alpha_i$ and $\theta(\alpha_2) = \alpha_j$. Thus one has

   $$0 = \theta(0) = \theta(g(\alpha_1 + \alpha_2)) = \theta(g)(\theta(\alpha_1 + \alpha_2)) = g(\alpha_i + \alpha_j),$$

   which gives the result.

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.

   Solution. Suppose some K_i is not contained in $\mathbb{R}$; let i be the largest i such that $K_i \subseteq \mathbb{R}$, so $K_{i+1} \not\subseteq \mathbb{R}$. Let $\tau \in \mathrm{Aut}(\mathbb{C})$ denote complex conjugation. Because K_{i+1}/K_i is Galois and τ fixes all elements of K_i, one has that $\tau|_{K_{i+1}}$ is an element of $\mathrm{Aut}_{K_i}(K_{i+1})$. But because $K_{i+1} \not\subseteq \mathbb{R}$ this element is nontrivial, hence has order 2. This is impossible because $|\mathrm{Aut}_{K_i}(K_{i+1})| = [K_{i+1} : K_i]$ is odd and we have a contradiction.

   (b) Prove that $\mathbb{Q}[\sqrt[3]{2}]$ is not contained in K_n.

   Suppose for a contradiction $\sqrt[3]{2} \in K_n$; let i be maximal such that $\sqrt[3]{2} \notin K_i$, so $\sqrt[3]{2} \in K_{i+1}$. Notice that $m_{\sqrt[3]{2},K_i}(x) | x^3 - 2$; from the tower $K_i \subseteq K_i[\sqrt[3]{2}] \subseteq K_{i+1}$ and the fact that $[K_{i+1} : K_i]$

is an odd prime, we deduce that $\deg(m_{\sqrt[3]{2},K_i}) = [K_i[\sqrt[3]{2}] : K_i] = 3$. But because K_{i+1}/K_i is Galois, $m_{\sqrt[3]{2}}(x) = x^3 - 2$ should then split in K_{i+1}, and this is impossible because two roots of $x^3 - 2$ are not real and by (a) we should have $K_{i+1} \subseteq \mathbb{R}$. We have a contradiction and so $\sqrt[3]{2} \notin K_n$.

4. Suppose F is a field and $\overline{F}$ is an algebraic closure of F. Suppose $K, E \in \mathrm{Int}(\overline{F}/F)$ such that K/E is a Galois extension and $[K : E] = p$ where p is prime. Suppose E/F is a Galois extension and $|\mathrm{Aut}_F(E)| = p^m$ for some integer m.
   (a) Argue why there is $\alpha \in K$ such that $K = E[\alpha]$. Let $L \in \mathrm{Int}(\overline{F}/E)$. Prove that $L[\alpha]/L$ is a Galois extension and $[L[\alpha] : L] = 1$ or p.

   Solution. The first claim is from primitive element theorem, which applies because K/E is finite Galois (one can also argue more directly by taking any $\alpha \in K \setminus E$ and using the fact that $[K : E]$ is prime). For the second claim, one can verify that K is the splitting field of $m_{\alpha,E}$ over E, and then one can also verify that $L[\alpha]$ is a splitting field of $m_{\alpha,E}$ over L. Because $m_{\alpha,E}$ is separable in $E[x]$ (because K/E is Galois), one has that it is separable in $L[x]$ as well, so $L[\alpha]/L$ is Galois.

   For the final claim suppose $[L[\alpha] : L] \neq 1$. Then $\alpha \notin L$ and one can conclude from this, by considering the tower $E \subseteq L \cap K \subseteq K$, that $L \cap K = E$. Then notice one has a natural restriction homomorphism $\mathrm{Aut}_L(L[\alpha]) \to \mathrm{Aut}_{L\cap K}(K) = \mathrm{Aut}_E(K)$, which is well-defined because K/E is Galois. One can easily check this is a bijection (surjectivity is because $L[\alpha]/L$ is Galois), and then looking at the size of each group one deduces $[L[\alpha] : L] = [E : K] = p$. This proves $[L[\alpha] : L] = 1$ or p.

   (b) Argue why for every $\theta_i \in \mathrm{Aut}_F(E)$, there is $\widehat{\theta}_i \in \mathrm{Aut}_F(\overline{F})$ 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.

   Solution. We know because $E[\alpha]/E$ is Galois that $E[\alpha]$ is a splitting field of $m_{\alpha,E}$ over E. From this one can verify that $E[\alpha_i]/E$ is a splitting field of $\widehat{\theta}_i(m_{\alpha,E})$ over E: for instance if one writes $m_{\alpha,E}(x) = (x - \beta_1)\cdots(x - \beta_m)$, then $\beta_j \in E[\alpha]$ for each i, and then $\theta_i(m_{\alpha,E}) = (x - \widehat{\theta}_i(\beta_1))\cdots(x - \widehat{\theta}_i(\beta_m))$, and one can directly verify that $\beta_j \in E[\alpha]$ implies that $\widehat{\theta}_i(\beta_j) \in E[\alpha_i]$. The degree formula follows because $\theta_i(m_{\alpha,E})$ is irreducible, which implies $\theta_i(m_{\alpha,E}) = m_{\alpha_i,E}$; the irreducibility is because if it were reducible, then one could apply θ_i^{-1} to get a factorization of $m_{\alpha,E}$ in $E[x]$, which is impossible.

   (c) In the above setting, prove that $E[\alpha_1, \ldots, \alpha_{p^m}]/F$ is a Galois extension, and if $\widehat{L} \in \mathrm{Int}(\overline{F}/K)$ and $\widehat{L}/F$ is Galois, then $E[\alpha_1, \ldots, \alpha_{p^m}] \subseteq \widehat{L}$.

   Outline of solution. We claim $E[\alpha_1, \ldots, \alpha_{p^m}]$ is a splitting field of $f(x) := \prod_{i=1}^{p^m} \theta_i(m_{\alpha,E})$ over F; notice this polynomial is actually in $F[x]$ because $\sigma(f) = f$ for all $\sigma \in \mathrm{Aut}_F(E)$ and E/F is Galois. Also notice that each α_i is a root of $f(x)$, because α_i is a root of $\theta_i(m_{\alpha,E})$. So to see it is a splitting field we just need to see that each root of f is in this field; but each $\theta_i(m_{\alpha,E})$ splits in $E[\alpha_i]$ by (b), so it splits in $E[\alpha_1, \ldots, \alpha_{p^m}]$, and then f splits in this field as well. Thus we have the claim, and we notice that f is separable, as it is a product of separable polynomials in $E[x]$, so $E[\alpha_1, \ldots, \alpha_{p^m}]/E$ is Galois.

   For the second claim, if $\widehat{L} \in \mathrm{Int}(\overline{F}/K)$ such that $\widehat{L}/F$ is Galois, then because $\widehat{\theta}_i \in \mathrm{Aut}_F(\overline{F})$ one has that $\widehat{\theta}_i(\widehat{L}) = \widehat{L}$. In particular because $\alpha \in K \subseteq L$ one has that $\alpha_i = \widehat{\theta}_i(\alpha) \in \widehat{L}$ for each i, and then the claim $E[\alpha_1, \ldots, \alpha_{p^m}] \subseteq \widehat{L}$ follows.

   (d) Prove that $[E[\alpha_1, \ldots, \alpha_{p^m}] : F]$ is a power of p.

Outline of solution. Because $[E : F]$ is a power of p by hypothesis, it suffices to show that $[E[\alpha_1, \dots, \alpha_{p^m}] : E]$ is a power of p. If we fix some i and take $K = E[\alpha_i]$ then $[K : E] = p$ by (b). Thus we are in the situation of (a), and for $L = E[\alpha_1, \dots, \alpha_{i-1}]$ we deduce that $[E[\alpha_1, \dots, \alpha_i] : E[\alpha_1, \dots, \alpha_{i-1}]] = 1$ or p. Thus the claim follows by induction on i.

7. Week 7

1. Suppose $p_1, \dots, p_n$ are distinct primes. Let $F := \mathbb{Q}[\sqrt{p_1}, \dots, \sqrt{p_n}]$.
   (a) Prove that $F/\mathbb{Q}$ is a Galois extension and $\mathrm{Aut}_{\mathbb{Q}}(F) \simeq \underbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n \text{ times}}$.

   Solution. The extension is Galois because F is a splitting field of $(x^2 - p_1) \cdots (x^2 - p_n)$ over $\mathbb{Q}$. For the second claim one uses Kummer theory: notice that, if Λ is as in our notation from Kummer theory, base field $\mathbb{Q}$ and $n = 2$, then one exactly has $F = \Lambda(\langle p_1(\mathbb{Q}^\times)^2, \dots, p_n(\mathbb{Q}^\times)^2\rangle)$. As a result of Kummer theory then one has $\mathrm{Aut}_{\mathbb{Q}}(F) \simeq \widehat{\langle p_1(\mathbb{Q}^\times)^2, \dots, p_n(\mathbb{Q}^\times)^2\rangle}$. First one claims that $\langle p_1(\mathbb{Q}^\times)^2, \dots, p_n(\mathbb{Q}^\times)^2\rangle \simeq \underbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n \text{ times}}$. To prove this claim, consider

   $$\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 \to \langle p_1(\mathbb{Q}^\times)^2, \dots, p_n(\mathbb{Q}^\times)^2\rangle, \quad (\varepsilon_1, \dots, \varepsilon_n) \mapsto \prod_{i=1}^n p_i^{\varepsilon_i}(\mathbb{Q}^\times)^2.$$

   One can prove this is an isomorphism: each generator of the right hand side is clearly in the image, and injectivity follows from the fact that the primes are distinct, so $\prod_{i=1}^n p_i^{\varepsilon_i}$ can never be a square in $\mathbb{Q}$ unless each $\varepsilon_i = 0$. With this isomorphism proved one has $\mathrm{Aut}_{\mathbb{Q}}(F) \simeq \widehat{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}$. To simplify the right hand side, one can either show that in general $\widehat{G \times H} \simeq \widehat{G} \times \widehat{H}$ for finite groups G, H, and then prove $\widehat{\mathbb{Z}_2} \simeq \mathbb{Z}_2$, or one can directly show that

   $$\widehat{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2} \to \{\pm 1\} \times \cdots \times \{\pm 1\}, \quad \chi \mapsto (\chi(e_1), \dots, \chi(e_n))$$

   where $e_i := (0, \dots, 0, 1, 0, \dots, 0)$ (with a 1 in the ith position) is an isomorphism. The right-hand side is clearly isomorphic to $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ so this gives the result.

   (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 $\{1, 2, \dots, n\}$.

   Outline of solution. Notice that every $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(F)$ must send $\sqrt{p_i} \mapsto \pm\sqrt{p_i}$ for each i, and these choices for $i = 1, \dots, n$ determine σ. Thus there are at most 2^n automorphisms; but from (a) there are exactly 2^n automorphisms, and thus every possibility occurs with regards to where $\sqrt{p_i}$ is mapped to. That is, for any choice of subset $I \subseteq \{1, \dots, n\}$, there exists an automorphism σ satisfying $\sigma(\sqrt{p_i}) = \sqrt{p_i}$ for $i \in I$ and $\sigma(\sqrt{p_j}) = -\sqrt{p_j}$ for $j \notin I$.

   Now to the claim at hand: we claim that the subfields $\mathbb{Q}[\sqrt{\prod_{i \in I} p_i}]$ are distinct as I varies over different (non-empty) subsets of $\{1, \dots, n\}$. To see this, suppose $I \neq J$ and take (without loss of generality) some $i \in I \setminus J$. Take some σ sending $\sqrt{p_i} \mapsto -\sqrt{p_i}$ and $\sqrt{p_j} \mapsto \sqrt{p_j}$ for $j \neq i$; then σ fixes all elements of $\mathbb{Q}[\sqrt{\prod_{j \in J} p_j}]$ but not $\mathbb{Q}[\sqrt{\prod_{i \in I} p_i}]$, and thus these two fields are distinct. This gives us $2^n - 1$ distinct possible $K \in \mathrm{Int}(F/\mathbb{Q})$ which are quadratic over $\mathbb{Q}$, and if we can show there are at most $2^n - 1$ possible K then this shows that every such K has the form $\mathbb{Q}[\sqrt{\prod_{i \in I} p_i}]$.

   To prove this, we notice that $K \in \mathrm{Int}(F/\mathbb{Q})$ correspond bijectively to index 2 subgroups of $\mathrm{Aut}_{\mathbb{Q}}(F) \simeq \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$, so we instead show that $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ has $2^n - 1$ subgroups of index 2. For this, one notices that an index 2 subgroup $H \leq \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ is equivalent giving a surjective homomorphism $\mathbb{Z}_2 \times \cdots \mathbb{Z}_2 \to \mathbb{Z}_2$. To count the number of such homomorphisms, it is convenient to use the language of vector spaces: both $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ and $\mathbb{Z}_2$ are $\mathbb{Z}_2$-vector spaces, and group homomorphisms $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 \to \mathbb{Z}_2$ are the same as $\mathbb{Z}_2$-linear maps. To count these, we can consider the basis $\{e_1, \ldots, e_n\}$ where $e_i := (0, \ldots, 0, 1, 0, \ldots, 0)$ with a 1 in the i-th position. Then giving a $\mathbb{Z}_2$-linear map $\mathbb{Z}_2 \times \cdots \mathbb{Z}_2 \to \mathbb{Z}_2$ is the same as choosing where the basis elements go, i.e. is the same as a function $\{e_1, \ldots, e_n\} \to \mathbb{Z}_2$. There are 2^n such functions, hence 2^n such linear maps, and only one of these (the zero map) is not surjective. Thus there are $2^n - 1$ surjective linear maps, and then $2^n - 1$ index 2 subgroups of $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$, as desired.

(c) Prove that $F = \mathbb{Q}[\sqrt{p_1} + \cdots + \sqrt{p_n}]$.

Solution. First we claim that part (a) implies $\sqrt{p_1}, \ldots, \sqrt{p_n}$ are linearly independent over $\mathbb{Q}$: if not then, after relabeling if necessary, we can write $\sqrt{p_n}$ as a $\mathbb{Q}$-linear combination of $\sqrt{p_i}$ for $1 \le i < n$, and then $\sqrt{p_n} \in \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}]$, so $\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}] = \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}]$. But applying part (a) to both sides would imply that

$$\underbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n-1 \text{ times}} \simeq \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}]) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}]) \simeq \underbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n \text{ times}},$$

yielding a contradiction. Now to show the result we show that $\mathrm{Aut}_{\mathbb{Q}[\sqrt{p_1}+\cdots+\sqrt{p_n}]}(F) = \{\mathrm{id}\}$. To show this, suppose we have such an automorphism σ: then $\sigma(\sqrt{p_1}+\cdots+\sqrt{p_n}) = \sqrt{p_1}+\cdots+\sqrt{p_n}$. Writing $\sigma(\sqrt{p_i}) = \varepsilon_i\sqrt{p_i}$ for $\varepsilon_i \in \{\pm 1\}$ we have $\sqrt{p_1} + \cdots + \sqrt{p_n} = \varepsilon_1\sqrt{p_1} + \cdots + \varepsilon_n\sqrt{p_n}$, and rearranging one has the equation

$$(1-\varepsilon_1)\sqrt{p_1} + \cdots + (1-\varepsilon_n)\sqrt{p_n} = 0.$$

Now by our first remark about linear independence, we conclude $1 - \varepsilon_i = 0$ for each i, i.e. $\sigma(\sqrt{p_i}) = \sqrt{p_i}$ for each i, and this shows $\sigma = \mathrm{id}$.

2. Suppose p is an odd prime and $\zeta_n := e^{\frac{2\pi i}{n}}$ for every positive integer n.

(a) Prove that $\mathbb{Q}[\zeta_{4p}] = \mathbb{Q}[\zeta_p, i]$.

Notice that $\zeta_p = \zeta_{4p}^4$ and $i = \zeta_{4p}^p$, so $\mathbb{Q}[\zeta_p, i] \subseteq \mathbb{Q}[\zeta_{4p}]$. On the other hand, notice that $(i\zeta_p)^{4p} = 1$, so $o(i\zeta_p) | 4p$, and one can directly verify that $(i\zeta_p)^k \neq 1$ for $k \in \{2, 4, p, 2p\}$, and thus we see $o(i\zeta) = 4p$. This means that $i\zeta_p$ must generate all $4p$-th roots of unity, and in particular $\zeta_{4p} \in \langle i\zeta_p \rangle \subseteq \mathbb{Q}[\zeta_p, i]$.

(b) Prove that $\mathbb{Q}[\sin(\frac{2\pi}{p})]/\mathbb{Q}$ is a Galois extension and $\mathrm{Aut}_{\mathbb{Q}[\sin(\frac{2\pi}{p})]}(\mathbb{Q}[\zeta_{4p}]) = \{\mathrm{id}, \tau\}$ where τ is the restriction of complex conjugation.

Notice that $\sin(\frac{2\pi}{p}) = \frac{\zeta_p - \zeta_p^{-1}}{2i}$ and in particular $\mathbb{Q}[\sin(\frac{2\pi}{p})] \subseteq \mathbb{Q}[\zeta_{4p}]$. Because $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_{4p}])$ is abelian it follows that $\mathbb{Q}[\sin(\frac{2\pi}{p})]/\mathbb{Q}$ is Galois. For the second claim, the inclusion $\{\mathrm{id}, \tau\} \subseteq \mathrm{Aut}_{\mathbb{Q}[\sin(\frac{2\pi}{p})]}(\mathbb{Q}[\zeta_{4p}])$ is clear because $\mathbb{Q}[\sin(\frac{2\pi}{p})] \subseteq \mathbb{R}$. For the other inclusion, we recall we proved in (a) that $i\zeta_p$ is a primitive $4p$-th root of unity and thus $\mathbb{Q}[\zeta_{4p}] = \mathbb{Q}[i\zeta_p]$. Now taking the equation $\zeta_p = \cos(\frac{2\pi}{p}) + i\sin(\frac{2\pi}{p})$, multiplying by i and rearranging, one can see that $i\zeta_p$ is a root of the polynomial $x^2 + 2\sin(\frac{2\pi}{p})x + 1$, so in particular $[\mathbb{Q}[\zeta_{4p}] : \mathbb{Q}[\sin(\frac{2\pi}{p})]] = [\mathbb{Q}[i\zeta_p] : \mathbb{Q}[\sin(\frac{2\pi}{p})]] \le 2$ and this lets us conclude equality $\mathrm{Aut}_{\mathbb{Q}[\sin(\frac{2\pi}{p})]}(\mathbb{Q}[\zeta_{4p}]) = \{\mathrm{id}, \tau\}$.

(c) Prove that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sin(\frac{2\pi}{p})]) \simeq \frac{\mathbb{Z}_{4p}^\times}{\{\pm 1\}}$; in particular $[\mathbb{Q}[\sin(\frac{2\pi}{p})] : \mathbb{Q}] = p - 1$.

If $\varphi : \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_{4p}]) \to \mathbb{Z}_{4p}^\times$ is the isomorphism we are familiar with, then notice $\varphi(\{1, \tau\}) = \{\pm 1\}$, and thus one has

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sin(\frac{2\pi}{p})]) \simeq \frac{\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_{4p}])}{\mathrm{Aut}_{\mathbb{Q}[\sin(\frac{2\pi}{p})]}(\mathbb{Q}[\zeta_{4p}])} = \frac{\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_{4p}])}{\{1, \tau\}} \simeq \frac{\mathbb{Z}_{4p}^\times}{\{\pm 1\}}.$$

The second claim follows immediately from tower law.

3. Suppose p is prime, F is a field of characteristic zero, and $a \in F^\times$. 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 $f \in F[x]$ divides $x^p - a$ and $\deg f < p$. Prove that $\zeta^i \deg f$ is in F for some integer i.

   Solution. Notice that the formal derivative of $x^p - a$ is px^{p-1}, and p is invertible in F because we are in characteristic zero, so one sees that $\gcd(x^p - a, px^{p-1}) = 1$ which implies $x^p - a$ does not have multiple roots. Thus we can take a root $\alpha' \neq \alpha$ of $x^p - a$ in E, and one sees that $\alpha/\alpha' \neq 1$ but $(\alpha/\alpha')^p = a/a = 1$, and thus one can take $\zeta := \alpha/\alpha'$. Because this ζ has order p we see that $\alpha, \zeta\alpha, \ldots, \zeta^{p-1}\alpha$ are distinct roots of $x^p - a$ in E and so we get the desired decomposition of $x^p - a$.

   For the next claim suppose f is as given. If we write $f(x)g(x) = x^p - a = \prod_{i=0}^{p-1}(x - \zeta^i\alpha)$ then unique factorization in $E[x]$ tells us that $f(x) = \prod_{i\in S}(x - \zeta^i\alpha)$ for some non-empty proper subset $S \subseteq \{0, 1, \ldots, p-1\}$. Looking at the constant term of this and recalling that $f \in F[x]$, we see that $\zeta^i\alpha^{\deg f} \in F$ where $i = \sum_{j\in S} j$.

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

   Solution. If $x^p - a$ is reducible then we have some f as in part (a), with the additional hypothesis that f is non-constant. Thus if $d := \deg(f)$ then $0 < d < p$ and $\zeta^i\alpha^d \in F$. Notice this implies that $a^d = (\zeta^i\alpha^d)^p$, so for $b := \zeta^i\alpha^d \in F$ one has $a = b^d$. We claim now that a is itself a p-th power in F. For this, we notice that $\gcd(d, p) = 1$ and write $1 = dx + py$ for $x, y \in \mathbb{Z}$, then calculate
   $$a = a^{dx+py} = a^{dx}a^{py} = (b^x)^p(a^y)^p = (b^xa^y)^p.$$
   Since $b^xa^y \in F$ we see that that $x^p - a$ 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 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.

   Solution. Dirichlet's theorem says we can find a prime of the form $p = nk+1$ (in fact there are infinitely many choices). Thus n divides $p - 1 = \mathbb{Z}_p^\times$ and so $\mathbb{Z}_n$ can be written as a quotient of $\mathbb{Z}_p^\times$: more precisely, we know because $\mathbb{Z}_p^\times$ is cyclic and $n|p-1$ that there is a (necessarily unique) subgroup $H \leq \mathbb{Z}_p^\times$ of order $(p-1)/n$. Then $\mathbb{Z}_p^\times/H$ is a cyclic group of order n so $\mathbb{Z}_p^\times/H \simeq \mathbb{Z}_n$.

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

   Solution. Using Dirichlet's theorem choose a prime p_1 of the form $p_1 = n_1k + 1$ for some k. Using Dirichlet's theorem, choose a prime $p_2 \neq p_1$ of the form $p_2 = n_2k + 1$ for some k; notice that Dirichlet's theorem gives us infinitely primes to choose from, so we can avoid p_1 if necessary. Next choose $p_3 \notin \{p_1, p_2\}$ of the form $p_3 = n_3k+1$ for some k (again we can avoid p_1, p_2 because Dirichlet's theorem gives us infinitely many choices), and continue in this fashion until one has a sequence of distinct primes $p_1, \ldots, p_k$ with $p_i \equiv 1 \mod n_i$. Let $q = p_1 \cdots p_k$. Using Chinese remainder theorem, and the fact about rings $(A \times B)^\times \simeq A^\times \times B^\times$, we calculate
   $$\mathbb{Z}_q^\times = (\mathbb{Z}_{p_1\cdots p_k})^\times \simeq (\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k})^\times \simeq \mathbb{Z}_{p_1}^\times \times \cdots \times \mathbb{Z}_{p_k}^\times.$$
   (Note: the first isomorphism, which used Chinese remainder theorem, is the reason we insist the primes p_i be distinct.) Now for each i, as in part (a) we can write $\mathbb{Z}_{n_i}$ as a quotient of $\mathbb{Z}_{p_i}^\times$, say $\mathbb{Z}_{n_i} \simeq \mathbb{Z}_{p_i}^\times/H_i$. One then has
   $$\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \simeq \mathbb{Z}_{p_1}^\times/H_1 \times \cdots \times \mathbb{Z}_{p_k}^\times/H_k \simeq (\mathbb{Z}_{p_1}^\times \times \cdots \times \mathbb{Z}_{p_k}^\times)/(H_1 \times \cdots \times H_k).$$

Thus combining our two isomorphisms we see that $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ is a quotient of $\mathbb{Z}_q$.

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

Solution. We know from (b) we can find q such that $\mathbb{Z}_{n_1} \times \cdots \mathbb{Z}_{n_k} \simeq \mathbb{Z}_q^\times/H$ for some $H \leq \mathbb{Z}_q^\times$. The latter is isomorphic to $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_q])$, so if we write $\varphi : \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_q]) \to \mathbb{Z}_q^\times$ for our isomorphism, and let $G := \varphi^{-1}(H)$, then for $F := \mathrm{Fix}(G)$ one finds that $F/\mathbb{Q}$ is Galois (because the automorphism group is abelian) and

$$\mathrm{Aut}_{\mathbb{Q}}(F) \simeq \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_q])/\mathrm{Aut}_F(\mathbb{Q}[\zeta_q]) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\zeta_q])/G \simeq \mathbb{Z}_q^\times/H \simeq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}.$$

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.)

Solution. Let $\tau = (i, j)$; then one has a decomposition $S_n = A_n \cup A_n\tau$, and thus using (c) we have

$$\begin{aligned} d(\mathbf{v}_1, \ldots, \mathbf{v}_n) &= \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) d_\sigma(\mathbf{v}_1, \ldots, \mathbf{v}_n) \\ &= \Big(\sum_{\sigma \in A_n} \mathrm{sgn}(\sigma) d_\sigma(\mathbf{v}_1, \ldots, \mathbf{v}_n)\Big) + \Big(\sum_{\sigma \in A_n} \mathrm{sgn}(\sigma\tau) d_{\sigma\tau}(\mathbf{v}_1, \ldots, \mathbf{v}_n)\Big) \\ &= \Big(\sum_{\sigma \in A_n} d_\sigma(\mathbf{v}_1, \ldots, \mathbf{v}_n)\Big) - \Big(\sum_{\sigma \in A_n} d_\sigma(\mathbf{v}_1, \ldots, \mathbf{v}_n)\Big) \\ &= 0. \end{aligned}$$

(e) For every index i, we identify $\{1,\dots,n\}\setminus\{i\}$ with $\{1,\dots,n-1\}$ by shifting all the numbers more than i by 1; this means we let

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

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

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

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

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

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

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

Outline of solution. For the first claim one verifies that the two permutations have the same value at each $j \in [1,\dots,n]$; this can easily be verified easily by separating into the following cases:

- $j<i$ and $\sigma(j) \geq \sigma(i)$,
- $j<i$ and $\sigma(j) < \sigma(i)$,
- $i \leq j < n$ and $\sigma(j+1) \geq \sigma(i)$,
- $i \leq j < n$ and $\sigma(j+1) < \sigma(i)$,
- $j=n$.

It is clear from the definition of $\widehat{\sigma}_i$ that $\operatorname{sgn}(\widehat{\sigma}_i) = \operatorname{sgn}(\sigma_i)$, and then we calculate

$$\begin{aligned}
\operatorname{sgn}(\sigma_i) = \operatorname{sgn}(\widehat{\sigma}_i) &= \operatorname{sgn}((\sigma(i),\dots,n)^{-1}\ \sigma\ (i,\dots,n)) \\
&= \operatorname{sgn}((\sigma(i),\dots,n)) \operatorname{sgn}(\sigma) \operatorname{sgn}((i,\dots,n)) \\
&= (-1)^{n-\sigma(i)+1} \operatorname{sgn}(\sigma)\, (-1)^{n-i+1} \\
&= (-1)^{i+\sigma(i)} \operatorname{sgn}(\sigma).
\end{aligned}$$

(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 $\mathbf{v}_1,\dots,\mathbf{v}_n$, 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

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

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

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

and deduce that

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

Using the definition of d and using parts (e) and (f) we have

$$\begin{aligned}
d(\mathbf{v}_1,\ldots,\mathbf{v}_{j-1},\mathbf{e}_k,\mathbf{v}_{j+1},\ldots,\mathbf{v}_n) &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) d_\sigma(\mathbf{v}_1,\ldots,\mathbf{v}_{j-1},\mathbf{e}_k,\mathbf{v}_{j+1},\ldots,\mathbf{v}_n)\\
&= \sum_{\substack{\sigma\in S_n\\ \sigma(j)=k}} (-1)^{j+\sigma(j)} d_{\sigma_j}(\mathbf{v}^{(k)}_{\ell_j^{-1}(1)},\ldots,\mathbf{v}^{(k)}_{\ell_j^{-1}(n-1)})\\
&= (-1)^{j+k} \sum_{\sigma\in S_{n-1}} d_\sigma(\mathbf{v}^{(k)}_{\ell_j^{-1}(1)},\ldots,\mathbf{v}^{(k)}_{\ell_j^{-1}(n-1)})\\
&= (-1)^{j+1} d(\mathbf{v}^{(k)}_{\ell_j^{-1}(1)},\ldots,\mathbf{v}^{(k)}_{\ell_j^{-1}(n-1)}).
\end{aligned}$$

For the second claim we write $\mathbf{v}_j = \sum_{i=1}^n v_{kj}\mathbf{e}_k$ and expand using linearity in the j-th component:

$$\begin{aligned}
d(\mathbf{v}_1,\ldots,\mathbf{v}_n) &= d(\mathbf{v}_1,\ldots,\mathbf{v}_{j-1},\sum_{k=1}^n \mathbf{v}_{kj}\mathbf{e}_k,\mathbf{v}_{j+1},\ldots,\mathbf{v}_n)\\
&= \sum_{k=1}^n v_{kj} d(\mathbf{v}_1,\ldots,\mathbf{v}_{j-1},\mathbf{e}_k,\mathbf{v}_{j+1},\ldots,\mathbf{v}_n)\\
&= \sum_{k=1}^n (-1)^{j+k} v_{kj}\ d(\mathbf{v}^{(k)}_{\ell_j^{-1}(1)},\ldots,\mathbf{v}^{(k)}_{\ell_j^{-1}(n-1)}).
\end{aligned}$$

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 $f(\mathbf{v}+\mathbf{w},\mathbf{v}+\mathbf{w})$.)

   Solution. Using biliearity one computes

$$\begin{aligned}
f(\mathbf{v}+\mathbf{w},\mathbf{v}+\mathbf{w}) &= f(\mathbf{v},\mathbf{v}+\mathbf{w}) + f(\mathbf{w},\mathbf{v}+\mathbf{w})\\
&= f(\mathbf{v},\mathbf{v}) + f(\mathbf{v},\mathbf{w}) + f(\mathbf{w},\mathbf{v}) + f(\mathbf{w},\mathbf{w})\\
&= f(\mathbf{v},\mathbf{w}) + f(\mathbf{w},\mathbf{v}).
\end{aligned}$$

   From this one subtracts to deduce the result.

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.

For any choice of i and vectors $\mathbf{v}_i, \mathbf{v}'_i$ and $c \in R$ we have

$$\begin{aligned} f_A(\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_i + c\mathbf{v}'_i, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n) &= d(A\mathbf{v}_1, \ldots, A\mathbf{v}_{i-1}, A(\mathbf{v}_i + c\mathbf{v}'_i), A\mathbf{v}_{i+1}, \ldots, A\mathbf{v}_n) \\ &= d(A\mathbf{v}_1, \ldots, A\mathbf{v}_{i-1}, A\mathbf{v}_i + cA\mathbf{v}'_i, A\mathbf{v}_{i+1}, \ldots, A\mathbf{v}_n) \\ &= d(A\mathbf{v}_1 \ldots, A\mathbf{v}_{i-1}, A\mathbf{v}_i, A\mathbf{v}_{i+1}, \ldots, A\mathbf{v}_n) + cd(A\mathbf{v}_1, \ldots, A\mathbf{v}_{i-1}, A\mathbf{v}'_i, A\mathbf{v}_{i+1}, \ldots, A\mathbf{v}_n) \\ &= f_A(\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_i, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n) + cf_A(\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}'_i, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n), \end{aligned}$$

where we've used the fact that d is n-linear. The fact that f_A is alternating follows similarly from the fact that d is 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 $X, Y \in \mathrm{M}_n(R)$.

From part (a), we know f_X is n-linear and alternating, which lets us apply problem 3 to se that $f_X = f_X(\mathbf{e}_1, \ldots, \mathbf{e}_n)d$; notice that by definition $f_X(\mathbf{e}_1, \ldots, \mathbf{e}_n) = d(X\mathbf{e}_1, \ldots, X\mathbf{e}_n) = d(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ where $\mathbf{x}_1, \ldots, \mathbf{x}_n$ are the columns of X. Now using part (b), if we let $\mathbf{y}_1, \ldots, \mathbf{y}_n$ denote the columns of Y we have

$$\det(XY) = f_X(\mathbf{y}_1, \ldots, \mathbf{y}_n) = f_X(\mathbf{e}_1, \ldots, \mathbf{e}_n)d(\mathbf{y}_1, \ldots, \mathbf{y}_n) = d(\mathbf{x}_1, \ldots, \mathbf{x}_n)d(\mathbf{y}_1, \ldots, \mathbf{y}_n) = \det(X)\det(Y).$$

(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* $\mathrm{adj}(X)$ 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

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

Let $a_{ij} = (-1)^{i+j}\det(X_{ji})$ denote the (i,j)-th entry of $\mathrm{adj}(X)$. The (i,j)-th entry of $\mathrm{adj}(X)X$ is by definition given by

$$\sum_{k=1}^{n} a_{ik}x_{kj} = \sum_{k=1}^{n} (-1)^{i+k} x_{kj} \det(X_{ki}).$$

One can immediately see from part (d) that if $i = j$ then this is equal to $\det(X)$, so we just need to show this quantity is zero when $i \neq j$. For this, let $X' = (x'_{pq})$ denote the matrix obtained by replacing the i-th column of X by the j-th column, i.e.

$$x'_{pq} := \begin{cases} x_{pq} & \text{if } q \neq i \\ x_{pj}, & \text{if } q = i. \end{cases}$$

Then taking the expansion on the i-th column (i.e. applying (d)) we have

$$\det(X') = \sum_{k=1}^{n} (-1)^{i+k} x'_{ki} \det(X'_{ki}) = \sum_{k=1}^{n} (-1)^{i+k} x_{kj} \det(X_{ki}),$$

and this is exactly equal to the (i,j)-th entry of $\mathrm{adj}(X)X$ as above, but we see that this quantity is zero because X' has a repeated column, so $\det(X') = 0$. This gives the result.

(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 $\widehat{A_1 \times A_2} \simeq \widehat{A_1} \times \widehat{A_2}$.

Solution. Given a homomorphism $\chi : A_1 \times A_2 \to S^1$, one can consider the associated homomorphism $\chi_1 : A_1 \to S^1$ defined by $\chi_1(a_1) = \chi(a_1, 1)$, and similarly one has $\chi_2 : A_2 \to S^1$ given by $\chi_2(a_2) = \chi(1, a_2)$. If one defines a function

$$\widehat{A_1 \times A_2} \to \widehat{A_1} \times \widehat{A_2}, \quad \chi \mapsto (\chi_1, \chi_2),$$

then one can easily verify this is an injective homomorphism. In addition, one has

$$|\widehat{A_1 \times A_2}| = |A_1 \times A_2| = |A_1|\,|A_2| = |\widehat{A_1}|\,|\widehat{A_2}| = |\widehat{A_1} \times \widehat{A_2}|,$$

and from this we conclude the map we've defined is actually an isomorphism.

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

Solution. Write $A = \langle a \rangle$ and $n = |A|$. Notice that for any $\chi \in \widehat{A}$ one has

$$\chi(a)^n = \chi(a^n) = \chi(1) = 1,$$

so $\chi(a) \in S^1$ is an n-th root of unity. Let M_n denote the n-th roots of unity in S^1, which we know to be a cyclic group of order n. Our previous remark means that we have a function

$$\widehat{A} \to M_n, \quad \chi \mapsto \chi(a).$$

We claim this is an injective homomorphism; if this is the case, then we are done as it proves $\widehat{A}$ is a cyclic group, and we know that $|\widehat{A}| = |A|$. To see the claim, we first need to show it is a homomorphism, which amounts to the claim that $(\chi\chi')(a) = \chi(a)\chi'(a)$, and this is simply from the definition of the group operation on $\widehat{A}$. For injectivity, one has that $\chi(a) = 1$ implies $\chi(a^k) = \chi(a)^k = 1$ for any k, which implies χ is the trivial homomorphism, i.e. the identity element of $\widehat{A}$. This shows injectivity and so we are done.

Notice that there is not a single choice of isomorphism $A \simeq \widehat{A}$ we have come up with in this proof; rather, we have that both A and $\widehat{A}$ are cyclic of the same order, we know that if we let a be a generator of A and χ a generator of $\widehat{A}$, then we can get an isomorphism $A \simeq \widehat{A}$ by sending $a \mapsto \chi$. The fact that this depends heavily on some choices of generators is sometimes phrased as the two groups being *non-canonically* isomorphic. You should compare this with the case of the isomorphism $A \simeq \widehat{\widehat{A}}$, which really is an explicit isomorphism (that does not require any choices); the latter one would often call *canonical*.

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

Solution. By the classification of finite abelian groups, one has $A \simeq \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r}$ for some integers $d_i \in \mathbb{Z}^+$. Then using the previous two parts one has

$$\widehat{A} \simeq \widehat{\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r}} = \widehat{\mathbb{Z}_{d_1}} \times \cdots \times \widehat{\mathbb{Z}_{d_r}} \simeq \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r} \simeq A.$$

2. Suppose A_i's are square matrices with entries in a unital commutative ring R. Prove that
$$\det\begin{pmatrix} A_1 & * & \cdots & * \\ & A_2 & \cdots & * \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & A_n \end{pmatrix} = \prod_{i=1}^{n} \det A_i.$$

Solution. Using a straightforward induction argument, it suffices to prove the $n = 2$ case. In this case we write A for the matrix in question, and write its entries as $A = [v_{ij}]_{1\le i,j\le m}$ so
$$A_1 = \begin{pmatrix} v_{11} & \cdots & v_{1\ell} \\ \vdots & \ddots & \vdots \\ v_{\ell 1} & \cdots & v_{\ell\ell} \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} v_{\ell+1,\ell+1} & \cdots & v_{\ell+1,m} \\ \vdots & \ddots & \vdots \\ v_{m1} & \cdots & v_{mm} \end{pmatrix}$$
for some ℓ with $v_{ij} = 0$ whenever $i \in [1, \ell]$ and $j \in [\ell + 1, m]$. Recall by definition the determinant of our matrix is a sum over products of elements $v_{\sigma(j)j}$ for $\sigma \in S_m$ and $j \in [1, m]$; notice if $\sigma(\{1, \ldots, \ell\}) \not\subseteq \{1, \ldots, \ell\}$ then there exists some $j \in [1, \ell]$ with $\sigma(j) \in [\ell + 1, m]$ and so $v_{\sigma(j)j} = 0$. As a result one has
$$\det A = \sum_{\sigma\in S_m} \operatorname{sgn}(\sigma) \prod_{j=1}^{m} v_{\sigma(j)j} = \sum_{\substack{\sigma\in S_m \\ \sigma(\{1,\ldots,\ell\})=\{1,\ldots,\ell\}}} \operatorname{sgn}(\sigma) \prod_{j=1}^{m} v_{\sigma(j)j}.$$
Now notice that an element $\sigma \in S_m$ with $\sigma(\{1, \ldots, \ell\}) = \{1, \ldots, \ell\}$ also satisfies $\sigma(\{\ell+1, \ldots, m\}) = \{\ell + 1, \ldots, m\}$. As a result any such σ is equal to $\sigma_1\sigma_2$ for $\sigma_1 \in S_{\{1,\ldots,\ell\}}$ and $\sigma_2 \in S_{\{\ell+1,\ldots,m\}}$ (and conversely, any such product $\sigma = \sigma_1\sigma_2$ satisfies $\sigma(\{1, \ldots, \ell\}) = \{1, \ldots, \ell\}$), so we can upgrade the above equality to
$$\begin{aligned}
\det A &= \sum_{\sigma_1\in S_{\{1,\ldots,\ell\}},\sigma_2\in S_{\{\ell+1,\ldots,m\}}} \operatorname{sgn}(\sigma_1\sigma_2) \prod_{j=1}^{m} v_{(\sigma_1\sigma_2)(j)j} \\
&= \sum_{\sigma_1\in S_{\{1,\ldots,\ell\}},\sigma_2\in S_{\{\ell+1,\ldots,m\}}} \big(\operatorname{sgn}(\sigma_1) \prod_{j=1}^{\ell} v_{\sigma_1(j)j}\big)\big(\operatorname{sgn}(\sigma_2) \prod_{j=\ell+1}^{m} v_{\sigma_2(j)j}\big) \\
&= \Bigg(\sum_{\sigma_1\in S_{\{1,\ldots,\ell\}}} \operatorname{sgn}(\sigma_1) \prod_{j=1}^{\ell} v_{\sigma(j)j}\Bigg) \Bigg(\sum_{\sigma_2\in S_{\{\ell+1,\ldots,m\}}} \operatorname{sgn}(\sigma_2) \prod_{j=\ell+1}^{m} v_{\sigma_2(j)j}\Bigg) \\
&= \det(A_1)\det(A_2).
\end{aligned}$$

3. Recall 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 $A \in M_n(F)$ is nilpotent. Prove that the characteristic polynomial of A is x^n, and deduce that $A^n = 0$.

   Solution. By assumption $A^k = 0$ for some $k \in \mathbb{Z}^+$. This means $p(A) = 0$ for $p(x) = x^k \in F[x]$; as a result one has that $m_{A,F}(x)|x^k$. By unique factorization we see that $m_{A,F}$ is a power of x. Now if we consider a rational canonical form of A (or, rather, let $T : F^n \to F^n$ be the linear map determined by A with respect to the standard basis and consider a rational canonical form of T), then we obtain polynomials $p_1|p_2|\cdots|p_r$ with $p_r = m_{T,F} = m_{A,F}$ and $f_A = f_T = \prod_i p_i$. From the fact that $p_i|m_{A,F}$ for each i we have that each p_i is a power of x, but then also $f_A = \prod_i p_i$ is a power of x as well. But $\deg(f_A) = n$ so we find $f_A(x) = x^n$ as desired. The latter claim follows because any matrix satisfies its characteristic polynomial.

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

Solution. Recall that R/P is an integral domain, so one can consider $F = Q(R/P)$ for which one has an embedding $A/P \hookrightarrow F$. If we consider the composition of ring homomorphisms

$$M_n(R) \to M_n(R/P) \hookrightarrow M_n(F),$$

and call this π, then one sees that $\pi(A)$ is nilpotent because A is, and then (a) implies that $\pi(A)^n = 0$ in $M_n(F)$, i.e. $\pi(A^n) = 0$ in $M_n(F)$, which implies $\pi(A^n) = 0$ in $M_n(R/P)$, which implies all entries of A^n are inside P.

(c) Suppose R is a unital commutative ring which has no nonzero nilpotent elements. Suppose $A \in M_n(R)$ is nilpotent. Prove that $A^n = 0$.

Solution. We know from (b) that if P is any prime ideal of R, then all entries of A^n lie in R, in other words each entry of A^n lies in the intersection of all prime ideals of R, which we've seen in class is exactly the set of nilpotent elements of A. Because A has no nonzero nilpotent elements, we conclude that all entries of A^n are zero, i.e. $A^n = 0$.

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 t_a is an F-linear map.

(a) Prove that the minimal polynomial of τ_a is $p(x) := x^n - N_{E/F}(a)$.

Solution. One can show with a straightforward induction on k that $\tau_a^k(e) = (\prod_{i=0}^{k-1} \sigma^i(a))\sigma^k(e)$. In particular one finds $\tau_a^n(e) = (\prod_{i=0}^{n-1} \sigma^i(a))\sigma^n(e) = N_{E/F}(a)e$; we conclude $\tau_a^n - N_{E/F}(a)$ is the zero linear transformation, so the minimal polynomial of τ_a divides $x^n - N_{E/F}(a)$. We claim this is the smallest possible degree; for this, suppose one has

$$c_{n-1}\tau_a^{n-1} + \cdots + c_1\tau_a + c_0 \,\mathrm{id} = 0$$

for $c_i \in F$. Recalling our description of τ_a^k and writing $a_k := \prod_{i=0}^{k-1} \sigma^i(a)$, we have for $e \in E$

$$0 = c_{n-1}\tau_a^{n-1}(e) + \cdots + c_0 \,\mathrm{id}(e) = (a_{n-1}c_{n-1})\sigma^{n-1}(e) + \cdots + (a_1c_1)\sigma(e) + (a_0c_0)e.$$

Now thinking of the σ^k as homomorphisms $E^\times \to E^\times$ (which are distinct for $k = 0, \ldots, n-1$) and using independence of characters, we deduce that each $a_kc_k = 0$ for $k \in [0, n-1]$; now noticing that $a_k \neq 0$, we have $c_k = 0$ for each k. This shows our original claim that τ_a does not satisfy any polynomial of degree $< n$, so we conclude $x^n - N_{E/F}(a)$ is the minimal polynomial of τ_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.

Solution. We have seen in class that there is a rational canonical form of τ_a of the form

$$\begin{pmatrix} C(d_1) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & C(d_r) \end{pmatrix}$$

where $d_i \in F[x]$ satisfy $d_1|d_2|\cdots|d_r$, $d_r = m_{\tau_a,F}$ and $f_{\tau_a} = \prod_{i=1}^r d_i$. Using (a) then we see $d_r = p$, and the latter claim in particular says $d_r|f_{\tau_a}$, but we have $\deg(d_r) = \deg(p) = n = \deg(f_{\tau_a})$, so we conclude by comparing degrees that $f_{\tau_a} = d_r = p$ and $r = 1$. In particular we see that $C(d_r) = C(p)$ 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 $e \in E$.

Solution. If $N_{E/F}(a) = 1$, using (a) one has $p(x) = x^n - 1$, and so

$$C(p) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

As a result we see that $C(p)(\mathbf{e}_i) = \mathbf{e}_{i+1}$ for each i (with $C(p)(\mathbf{e}_n) = \mathbf{e}_1$), and from this it is clear that $C(p)(\mathbf{e}_1 + \cdots + \mathbf{e}_n) = \mathbf{e}_1 + \cdots + \mathbf{e}_n$.

This tells us that the matrix $C(p)$ has a fixed point, so τ_a must also have a fixed point; if we call it e then $\tau_a(e) = e$ means $a\sigma(e) = e$, or $a = \frac{e}{\sigma(e)}$, as desired.

(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.

Solution. For $a = 1$ we see σ has a rational canonical form given by $C(p)$ where $p(x) = x^n - 1$, i.e. (as above)

$$C(p) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0. \end{pmatrix}$$

The rational canonical form of a linear transformation is a matrix representation with respect to a particular basis, which means there is an F-basis $\mathfrak{B} = \{e_0, e_1, \ldots, e_{n-1}\}$ of E with respect to which $C(p)$ represents σ. But one can clearly see from the matrix reprentation that $e_1 = \sigma(e_0)$, and then $e_2 = \sigma(e_1) = \sigma^2(e_0)$, and similarly $e_i = \sigma^i(e_0)$ for each $i \in [0, n-1]$, which shows this matrix $\mathfrak{B}$ is of the desired form.

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 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 $[a]_{\mathfrak{B}_0} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$.

Solution. From the description of $[\sigma]_{\mathfrak{B}_0}$ one can quickly see that

$$[\sigma]_{\mathfrak{B}_0} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} c_n \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} \quad \text{and} \quad [\sigma^2]_{\mathfrak{B}_0} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} c_{n-1} \\ c_n \\ \vdots \\ c_{n-2} \end{pmatrix},$$

and continuing one sees that

$$[T_{E/F}]_{\mathfrak{B}_0} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} c_1 + \cdots + c_n \\ c_1 + \cdots + c_n \\ \vdots \\ c_1 + \cdots + c_n \end{pmatrix}.$$

Thus if $a \in E$ with $[a]_{\mathfrak{B}_0} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$, one has

$$T_{E/F}(a) = 0 \iff [T_{E/F}]_{\mathfrak{B}_0} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0 \iff c_1 + \cdots + c_n = 0.$$

(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.

Solution. This is the same as solving the system of equations

$$\begin{aligned} x_2 - x_1 &= c_1 \\ x_3 - x_2 &= c_2 \\ &\vdots \\ x_n - x_{n-1} &= c_{n-1} \\ x_1 - x_n &= c_n \end{aligned}$$

for values $x_1, \ldots, x_n \in F$. If one lets x_1 be any value, then the rest of the values are automatically determined from the equations and determine a valid solution; for example if we take for simplicity $x_1 = 0$ then $x_2 = c_1$, $x_3 = c_1 + c_2$ and for each i, $x_i = c_1 + \cdots + c_{i-1}$, and in particular $x_n = c_1 + \cdots + c_{n-1} = -c_n$ which shows the final necessary equality holds above.

(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 $\sigma(e) - e = a$.

Notice the matrix from part (b) represents the linear transformation $\sigma - \mathrm{id}$ with respect to the basis $\mathfrak{B}_0$ from (a). If $T_{E/F}(a) = 0$ then from (a) one has $[a]_{\mathfrak{B}_0} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ with $c_1 + \cdots + c_n = 0$, and then (b) guarantees an element $\mathbf{x} \in F^n$ with $[\sigma - \mathrm{id}]_{\mathfrak{B}_0}\mathbf{x} = [a]_{\mathfrak{B}_0}$. One has $\mathbf{x} = [e]_{\mathfrak{B}_0}$ for some $e \in E$, and then for this e we see that $(\sigma - \mathrm{id})(e) = a$, i.e. $\sigma(e) - e = a$ as desired.

10. Week 1

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.

      Solution. Notice that A^n is generated by $\mathbf{e}_i$'s as an A-module. Hence A^n is a finitely generated A-module. By Theorem 38.1.2, every finitely generated module over a Noetherian ring is a Noetherian module. Hence A^n is a Noetherian A-module.

(ii) Show that there is an integer n_0 such that for every integer $i \geq n_0$, $\ker f^{(n_0)} = \ker f^{(i)}$.

Solution. We have an increasing chain of submodules of A^n given by

$$\ker f \subseteq \ker f^{(2)} \subseteq \cdots \subseteq \ker f^{(n)} \subseteq \cdots,$$

so part (a) implies that there is some n_0 for which $\ker f^{(n_0)} = \ker f^{(i)}$ as desired.

(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 $\mathbf{x} = 0$.

Solution. Because f is surjective, then so is $f^{(n)}$ for any n; in particular $f^{(n_0)}$ is surjective so there exists some $\mathbf{y} \in A^n$ such that $\mathbf{x} = f^{(n_0)}(\mathbf{y})$. But then notice that $f^{(2n_0)}(\mathbf{y}) = f^{(n_0)}(f^{(n_0)}(\mathbf{y})) = f^{(n_0)}(\mathbf{x}) = 0$, so $\mathbf{y} \in \ker f^{(2n_0)}$. But from part (b) we have $\ker f^{(2n_0)} = \ker f^{(n_0)}$, so $\mathbf{y} \in \ker f^{(n_0)}$, and then $\mathbf{x} = f^{(n_0)}(\mathbf{y}) = 0$.

(iv) Prove that f is an isomorphism.

Solution. In part (c) we showed that $\ker f^{(n_0)} = 0$, but then also $\ker f = 0$, i.e. f is injective, hence an isomorphism.

(b) Suppose A is an arbitrary unital commutative ring.

(i) Show that there are $M_f = [a_{ij}] \in M_n(A)$ and $M' = [a'_{ij}] \in M_n(A)$ such that

$$f(x_1, \ldots, x_n) = (\sum_{j=1}^{n} a_{1j}x_n, \ldots, \sum_{j=1}^{n} a_{nj}x_n)$$

and $M_f M' = I_n$. Argue that f is an isomorphism if and only if $M_f \in \mathrm{GL}_n(A)$.

Solution. Let $\mathbf{e}_j = (0, \ldots, 0, 1, 0, \ldots, 0)$ with a 1 in the j-th position; then the a_{ij} desired are exactly the elements such that $f(\mathbf{e}_j) = (a_{1j}, \ldots, a_{nj})$. The formula for f follows from expanding linearly:

$$\begin{aligned} f(x_1, \ldots, x_n) &= f(\sum_j x_j \mathbf{e}_j) = \sum_j x_j f(\mathbf{e}_j) \\ &= \sum_j x_j (a_{1j}, \ldots, a_{nj}) \\ &= (\sum_j a_{1j}x_j, \ldots, \sum_j a_{nj}x_j). \end{aligned}$$

To find the desired elements a'_{ij}, we use the fact that f is linear, so for each j there is some element $(a'_{1j}, \ldots, a'_{nj}) \in A^n$ such that $f(a'_{1j}, \ldots, a'_{nj}) = \mathbf{e}_j$. To see the identity $M_f M' = I_n$, it suffices to check that $(M_f M') \cdot \mathbf{e}_j = \mathbf{e}_j$ for each j (where we consider $\mathbf{e}_j$ as a column vector); this follows from the choice of a'_{ij}, more precisely

$$(M_f M') \cdot \mathbf{e}_j = M_f \cdot (M' \cdot \mathbf{e}_j) = M_f \cdot \begin{pmatrix} a'_{1j} \\ \vdots \\ a'_{nj} \end{pmatrix} = \mathbf{e}_j.$$

The main point of the last claim is that M_f is a matrix representation of the homomorphism f, so M_f is invertible if and only if f is; more precisely, if M_f is an isomorphism, then an inverse matrix M_f^{-1} defines an A-module homomorphism $A^n \to A^n$ by matrix multiplication, which will be an inverse for f, and conversely if f is an isomorphism then we could choose a matrix representation for f^{-1} (in the same way we constructed M_f here), which will be an inverse for M_f.

(ii) Let A' be the subring of A which is generated by the a_{ij}'s and a'_{ij}'s. Argue that

$$M_f \times : M_{n,1}(A') \to M_{n,1}(A'), \quad \mathbf{x} \mapsto M_f \mathbf{x}$$

is a surjective A'-module homomorphism.

Solution. Notice the fact that M_f has entries in A' implies the map is well-defined, i.e. it actually sends elements of $M_{n,1}(A')$ to $M_{n,1}(A')$. Checking the map is a homomorphism is straightforward. For surjectivity we use $M_f M' = I_n$: for any $\mathbf{y} \in M_{n,1}(A')$ one has

$$\mathbf{y} = (M_f M') \cdot \mathbf{y} = M_f \cdot (M' \cdot \mathbf{y}),$$

which shows that $M' \cdot \mathbf{y}$ is a preimage of $\mathbf{y}$ under the given homomorphism (notice that $M' \cdot \mathbf{y} \in M_{n,1}(A')$ holds because M' and $\mathbf{y}$ both have entries all inside A').

(iii) Prove that $M_f \in \mathrm{GL}_n(A')$ and deduce that f is an isomorphism.

Solution. By Theorem 41.3.5, every finitely generated ring is Noetherian, and so A' is Noetherian. But then we see that we can apply part 1(a), where we have seen that in the Noetherian situation, a surjective module homomorphism $(A')^n \to (A')^n$ is an isomorphism. Thus $M_f \times : M_{n,1}(A') \to M_{n,1}(A')$ is an isomorphism, so $M_f \in \mathrm{GL}_n(A') \subseteq \mathrm{GL}_n(A)$, and thus $M_f \in \mathrm{GL}_n(A)$ which we have remarked in part (i) implies f is an isomorphism.