ALGEBRA

ISAIAH DAILEY

Contents

1. Groups

Definition 1.1. A *semigroup* is a set with an associative operation. A *monoid* is a semigroup with an identity element. A *group* is a monoid with inverses. An *abelian* group is a commutative group.

Definition 1.2. For $n \geq 3$, write D_{2n} for the dihedral group of order $2n$ with presentation $\langle r, s \mid r^n, s^2, rsrs^{-1} \rangle$. The elements of D_{2n} are $e, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}$.

Definition 1.3. The quarternion group Q_8 has elements $\pm 1, \pm i, \pm j, \pm k$ with group structure given by

$$-1 \cdot x = -x \ \forall x \in Q_8, \quad (-1)^2 = 1, \quad ij = k, \quad jk = i, \quad ki = j.$$

Definition 1.4. A subset H of a group G is a *subgroup* if H is nonemtpy and $xy^{-1} \in H$ whenever $x, y \in H$.

Definition 1.5. The *special linear group* of a field F is the subgroup $\mathrm{SL}_n(F) \subseteq \mathrm{GL}_n(F)$ of matrices A with $\det A = 1$.

Definition 1.6. The *alternating group* in n elements is the subgroup $A_n \leq S_n$ consisting of even permutations.[1] A_n has order $n!/2$.

Definition 1.7. Let $H \leq G$ be a subgroup, then we write G/H (resp. $H\backslash G$) for the set of left (resp. right) cosets of H in G.

Proposition 1.8. *Let $H \leq G$.*

1. *For any $x, y \in G$, there is a bijection $xH \to yH$ given by $xh \mapsto yh$.*
2. *For any $x \in G$, there is a bijection $xH \to Hx^{-1}$ defined by $xh \mapsto h^{-1}x^{-1}$.*
3. *There is a bijection $G/H \to H\backslash G$ given by $xH \mapsto Hx^{-1}$.*

Definition 1.9. Given a subgroup H of a group G, we define the index of H in G to be the quantity $|G : H| := |G/H| = |H\backslash G|$.

Date: August 18, 2024.

[1] A permutation $\sigma \in S_n$ is said to be *even* if σ can be written as a composition of an even number of two-element swaps.

Proposition 1.10. *Given a subgroup $H \leq G$, we have $|G| = |G : H| \cdot |H|$. More generally, if $K \leq H \leq G$, we have $|G : K| = |G : H| \cdot |H : K|$.*

Theorem 1.11 (Lagrange's Theorem)**.** *If G is a finite group and $H \leq G$, then $|H|$ and $|G : H|$ divide $|G|$. In particular, $|g| := |\langle g \rangle|$ divides $|G|$ for all $g \in G$.*

As a consequence of Lagrange's theorem, if $|G|$ is prime then G is cyclic.

Example 1.12. S_3 and D_6 are isomorphic, given by $\phi : D_6 \to S_3$ given by $\phi(r) = (1\,2\,3)$ and $\phi(s) = (1\,2)$.

Definition 1.13. A subgroup $H \leq G$ is said to be *normal* if $xHx^{-1} = H$ for all $x \in G$, equivalently, if $xH = Hx$ for all $x \in G$. We write $H \trianglelefteq G$ to mean H is a normal subgroup of G.

Warning 1.14. The relation $\trianglelefteq$ is NOT a transitive relation on subgroups!

Definition 1.15. If $H \trianglelefteq G$, then G/H be comes a group by the operation $xH \cdot yH = xyH$.

Proposition 1.16. *A subgroup $H \leq G$ is normal iff it is the kernel of some homomorphism.*

Proposition 1.17. *Let G be a group with subgroups $A, B \leq G$, then their intersection $A \cap B$ is also a subgroup.*

Definition 1.18. Let G be a group with subgroups $A, B \leq G$, then define

$$AB := \{ab \in G \mid a \in A,\, b \in B\}.$$

The set AB is *not* generally a subgroup.

Example 1.19. Consider $G = D_6$ generated by $\{r, s\}$ with $r^3 = s^2 = (sr)^2 = 1$. Let $A = \langle s \rangle$ and $B = \langle sr \rangle$, both subgroups of order 2. Then $AB = \{e, s, sr, r\}$, which is not a subgroup since $r^2 \notin AB$.

Exercise 1.20. Show that AB is a subgroup of G iff $AB = BA$.

Definition 1.21. Given a subset $S \subseteq G$, we write $N_G(S)$ for the *normalizer* of S in G, that is,

$$N_G(S) := \{g \in G \mid gSg^{-1} = S\}.$$

Proposition 1.22. *Let $S \subseteq G$, then*

- *$N_G(S)$ is a subgroup of G.*
- *If $H \leq G$ is a subgroup, then $H \trianglelefteq N_G(H)$.*
- *$N_G(H)$ is the "largest" subgroup of G that H is normal inside of.*
- *$N_G(H) = G$ iff $H \trianglelefteq G$.*

Theorem 1.23 (The Second ("Diamond") Isomorphism Theorem)**.** *Suppose $A, B \leq G$ and $A \leq N_G(B)$. Then*

(1) AB is a subgroup of G (equivalently, $AB = BA$).

(2) $B \trianglelefteq AB$,

(3) $A \cap B \trianglelefteq A$,

(4) $A/(A \cap B) \cong AB/B$.

$$
\begin{tikzcd}
 & & & G \\
AB/B & & & N_G(B) \arrow[u, hook] \\
 & & & AB \arrow[u, hook] \\
A/A\cap B \arrow[uu, "\cong"] & & A \arrow[ur, hook] \arrow[uur, hook, bend left] & & B \arrow[ul, hook', "\trianglelefteq"'] \arrow[uul, hook', bend right, "\trianglelefteq"'] \\
 & & & A\cap B \arrow[ul, hook', "\trianglelefteq"] \arrow[ur, hook]
\end{tikzcd}
$$

Corollary 1.24. *If $A \leq G$ and $B \trianglelefteq G$, then AB is a subgroup of G.*

Theorem 1.25 (The Third Isomorphism Theorem)**.** *Let $H, K \trianglelefteq G$ with $H \leq K$. Then*

(1) $K/H \trianglelefteq G/H$, and

(2) $G/K \cong (G/H)/(K/H)$ via the assignment $xK \mapsto (xH)\overline{K}$ (where $\overline{K} = K/H \subseteq G/H$).

$$
\begin{tikzcd}
 & G/K \arrow[r, "\cong"] & (G/H)/(G/K) \\
 & G \arrow[u, two heads] \arrow[r, two heads] & G/H \arrow[u, two heads] \\
H \arrow[ur, hook, "\trianglelefteq"] \arrow[r, hook, "\trianglelefteq"] & K \arrow[u, hook, "\trianglelefteq"'] \arrow[r, two heads] & K/H \arrow[u, hook, "\trianglelefteq"']
\end{tikzcd}
$$

Intuitively, the following theorem says the following: Let $N \trianglelefteq G$ be a normal subgroup, then the quotient map $\pi : G \twoheadrightarrow G/N$ induces a lattice isomorphism (an inclusion-preserving bijection) between the set of subgroups of G containing N, and the set of subgroups of G/N. Moreover, this isomorphism restricts to an isomorphism on the normal subgroups, and given subgroups $A, B \leq G$ with $N \leq A \cap B$, we have $(A \cap B)/N = (A/N) \cap (B/N)$.

Theorem 1.26 (The Fourth ("Lattice") Isomorphism Theorem)**.** *Let $N \trianglelefteq G$ be a normal subgroup. Then we have inverse bijections*

$$
\begin{tikzcd}
\{A \leq G \mid N \leq A\} \arrow[rr, leftrightarrow, "\sim"] & & \{\overline{A} \leq G/N\} \\
A \arrow[rr, mapsto] & & A/N \\
\pi^{-1}\overline{A} & & \overline{A} \arrow[ll, mapsto]
\end{tikzcd}
$$

where $\pi^{-1}\overline{A} = \{g \in G \mid \pi(g) \in \overline{A}\}$. Furthermore, for $A, B \leq G$ with $N \leq A \cap B$, we have

(1) $A \leq B$ iff $A/N \leq B/N$.

(2) If $A \leq B$ then $|B : A| = |B/N : A/N|$.

(3) $(A \cap B)/N = (A/N) \cap (B/N)$.

(4) $A \trianglelefteq G$ iff $A/N \trianglelefteq G/N$.

Definition 1.27. A **group presentation** is a pair (S, R) consisting of a set S and a subset $R \subseteq F(S)$ (where $F(S)$ denotes the free group on S). The group *presented* by this data is defined to be

$$\langle S \mid R \rangle := F(S)/N,$$

where N is the *normal closure* of R in $F(S)$, that is, the smallest normal subgroup of $F(S)$ containing R.

Given a group G, we say that (S, R) is a *presentation* of G if there exists an isomorphism $G \cong \langle S \mid R \rangle$ of groups. We say that G is *finitely presentable* if it has a presentation (S, R), where S and R are both finite.

Example 1.28. The dihredral group D_{2n} of order $2n$ has presentation $\langle r, s \mid r^n, s^2, srsr \rangle$.

Proposition 1.29. *For $n \geq 1$, we have*

$$S_n \cong \langle s_1, \ldots, s_{n-1} \mid R \rangle,$$

where R consists of the relations

$$\begin{aligned} s_i^2 &= 1, & &\text{for } i = 1, \ldots, n-1, \\ (s_i s_j)^2 &= 1, & &\text{when } |i - j| \geq 2, \\ (s_i s_{i+1})^3 &= 1, & &\text{for } i = 1, \ldots, n-1. \end{aligned}$$

Definition 1.30. Given an object X in a category $\mathcal{C}$ and a group G, a *left group action* of G on X is a group homomorphism $\phi : G \to \mathrm{Aut}(X)$, denoted by $G \curvearrowright X$. A right group action is a group homomorphism $\phi : G^{\mathrm{op}} \to \mathrm{Aut}(X)$.

Definition 1.31. A set equipped with a G-action is called a *G-set*.

Example 1.32. For any object X and group G, the trivial map $G \to \mathrm{Aut}(X)$ yields the *trivial action* of G on X, in which G simply acts via identities on X.

Example 1.33. Given $H \leq G$, the set G/H of left cosets of H admits a natural G action by

$$g \cdot xH := gxH.$$

Similarly, the set $H \backslash G$ of right cosets of H admits a natural G action by the rule

$$g \cdot Hx := Hxg^{-1}.$$

Example 1.34. Every group acts on itself by conjugation via the map $\mathrm{conj} : G \to \mathrm{Aut}(G)$ defined by

$$\mathrm{conj}_g(x) := gxg^{-1}.$$

Definition 1.35. Let $\phi : G \to \mathrm{Aut}(X)$ be a left G-action on an object X.

(1) The *kernel* of the action is the kernel of the homomorphism ϕ, i.e., it is the set $\{g \in G \mid \phi_g = \mathrm{id}_X\}$.

(2) The action is *faithful* if the kernel is trivial.

If X is a set, then we have the following further definitions.

(1) Given $x \in X$, the *stabilizer* of x (denoted by $\mathrm{Stab}(x)$ or just G_x) is the set $\{g \in G \mid g \cdot x = x\}$.

(2) The action is *free* if all the stabilizers G_x are trivial.

Proposition 1.36. *Suppose X is a G-set, and $x, y \in X$ satisfying $y = g \cdot x$ for some $g \in G$. Then*

$$G_y = gG_xg^{-1}.$$

Example 1.37. Consider the tautological action of $G = S_n$ on $X = \{1, \dots, n\}$, so the corresponding homomorphism $G \to \mathrm{Sym}(X)$ is the identity. We have that:

- The kernel of the action is trivial, so it is a faithful action.
- The action is free iff $n \geq 3$.
- If $n > 1$, each G_x is isomorphic to S_{n-1}, but each is a *distinct* subgroup of S_n.
- The G_x are conjugate to each other: if $\sigma \in S_n$ such that $\sigma(x) = y$, then $G_y = \sigma G_x \sigma^{-1}$.

Theorem 1.38 (Cayley's Theorem)**.** *Every group is isomorphic to a subgroup of some permutation group* $\mathrm{Sym}(X)$.

Proof. Given G, it suffices to provide a faithful action on some set X, so that the induced homomorphism $\phi : G \to \mathrm{Sym}(X)$ is injective, and therefore identifies G with a subgroup of $\mathrm{Sym}(X)$. This is easy: equip $X = G$ with the natural left G action given by $g \cdot x := gx$. Then this action is faithful, since $gx = x$ for all $x \in X$ certainly implies $g = e$. $\square$

Proposition 1.39. *If G is a finite group and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal. In particular, index 2 subgroups of finite groups are always normal.*

Proof. Let $H \leq G$ be a subgroup of index p, and consider the left action of G on $X = G/H$, which gives a homomorphism $\phi : G \to \mathrm{Sym}(G/H) \cong S_p$. Let $K = \ker \phi$ of this action. We know K is normal, since it is a kernel, so it suffices to show that $K = H$. Note that clearly $K \leq H$, so it further suffices to show that $|H : K| = 1$. By the first isomorphism theorem, G/K is isomorphic to a subgroup of S_p, so that $|G : K|$ divides $|S_p| = p!$, by Lagrange's theorem. We have that $|G : K| = |G : H||H : K| = p|H : K|$, so $|H : K|$ divides $p!/p = (p-1)(p-2)\cdots 2 \cdot 1$. However, since $|H : K|$ divides $|G|$, we know that no prime smaller than p divides $|H : K|$. Thus $|H : K| = 1$, as desired. $\square$

Definition 1.40. Consider a group action $G \curvearrowright X$, where X is a set. Define a relation $\sim$ on X by

$$x \sim y \iff \exists g \in G,\ g \cdot x = y.$$

This is an equivalence relation on X, and the equivalence classes of this relations are called *orbits*. We write $\mathrm{Orb}(x)$, Gx, or $G \cdot x$ for the orbit which contains x, so that $\mathrm{Orb}(x) = \{g \cdot x \mid g \in G\}$.

An action is *transitive* if it has exactly one orbit.

Example 1.41. G acts transitively on G/H.

Theorem 1.42 (The Orbit/Stabilizer Theorem)**.** *Suppose X is a G-set, and $x \in X$. Then there is a bijection*

$$G/\operatorname{Stab}(x) \xrightarrow{\sim} \mathrm{Orb}(x), \qquad g\operatorname{Stab}(x) \mapsto g \cdot x.$$

Thus for an orbit $\mathcal{O}$, we have $|\mathcal{O}| = |G : \operatorname{Stab}(x)|$ for any $x \in \mathcal{O}$.

Corollary 1.43. *Let G act on a finite set X. Then we have*

$$|X| = \sum_{k=1}^{r} |G : \operatorname{Stab}(x_k)|,$$

where $x_1, \dots, x_r \in X$ are representatives of the orbits of the action (that is, $\mathrm{Orb}(x_i) \cap \mathrm{Orb}(x_j) = \emptyset$ when $i \neq j$, and $\bigcup_{k=1}^{r} \mathrm{Orb}(x_k) = X$),

Theorem 1.44 (Cauchy's Theorem)**.** *Let G be a finite group. If a prime p divides $|G|$, then G has an element of order p.*

Definition 1.45. A group G is *simple* if its only normal subgroups are $\{e\}$ and G. By convention the trivial group is *not* simple.

Example 1.46. Let p be a prime. Then the cyclic group $G = C_p$ of order p is simple.

Proposition 1.47. *The alternating group A_n on n elements is simple for $n \geq 5$.*

Proof sketch. Elements of A_n are the even permutations, and it is straightforward to check that A_n is also generated by its subset of 3-cycles. Then one checks that any normal subgroup N of A_n which contains some 3-cycle contains every 3-cycle, and therefore satisfies $N = A_n$.

Thus, in order to prove A_n is simple, it suffices to show that if $N \trianglelefteq A_n$ is a non-trivial normal subgroup, it must contain at least one 3-cycle. This is where the assumption that $n \geq 5$ is needed. □

Example 1.48. The group A_4 is not simple: the subgroup $N = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ generated by the products of disjoint 2-cycles is normal.

Definition 1.49. Consider the conjugation action of G on itself: $\cong_g (x) = gxg^{-1}$.

- The *orbits* for the conjugation action are the conjugacy classes; we denote the conjugacy class of an element $x \in G$ by $\mathrm{Cl}(x) := \{gxg^{-1} : g \in G\}$.
- The *stabilizer* of $x \in G$ under the conjugation action is the *centralizer subgroup* of x:
$$C_G(x) := \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}.$$
- The kernel of the conugation action is precisely the *center*
$$Z_G := \{g \in G \mid gx = xg \ \forall x \in G\}.$$
- Note that $\mathrm{Cl}(e) = \{e\}$ and $C_G(e) = G$, so that the conjugation action is neither free nor transitive (unless $G = \{e\}$).

Theorem 1.50 (The Class Equation)**.** *For a finite group G, we have*
$$|G| = |Z_G| + \sum_{k=1}^{r} |G : C_G(g_k)|,$$
where $g_1, \ldots, g_r$ are representatives of the distinct conjugacy classes of G not contained in the center Z_G.

Moreover, each term on the right divides $|G|$.

Definition 1.51. Let p be a prime. A *p-group* is a non-trivial finite group whose order is a power of p.

Proposition 1.52. *Every p-group has a non-trivial center.*

Proof. The class equation for G gives
$$p^d = |Z_G| + \sum_{k=1}^{r} |G : C_G(g_k)|.$$
Since $C_G(g_k) \neq G$, we have that p divides each $|G : C_G(g_k)|$. Therefore p divides $|Z_G|$. Since $|Z_G| \geq 1$ we may conclude that p divides $|Z_G|$. □

Corollary 1.53. *If $|G| = p^2$ for some prime p then G is abelian.*

Proof. First we note a general fact: If G/Z_G is cyclic, then G is abelian. To see this, pick $g \in G$ which projects to a generator of G/Z_G. Then every element in G can be written as $g^k x$ for some $k \in \mathbb{Z}$ and $x \in Z_G$. Then every element in G can be written as $g^k x$ for some $k \in \mathbb{Z}$ and $x \in Z_G$. Since $(g^i x)(g^j y) = g^{i+j} xy$ whenever $x, y \in Z_G$, we see that G is abelian.

If $|G| = p^2$, then by the previous result $|Z_G| \in \{p, p^2\}$, whence $|G/Z_G| \in \{1, p\}$ and thus is cyclic. □

Definition 1.54. Given a group G, the image of the homomorphism $\mathrm{conj} : G \to \mathrm{Aut}(G)$ is the group

$$\mathrm{Inn}(G) := \{\mathrm{conj}_g \mid g \in G\} \leq \mathrm{Aut}(G),$$

and its elements are called *inner automorphisms* of G. The first isomorphism theorem then gives an isomorphism

$$G/Z_G \cong \mathrm{Inn}(G).$$

Proposition 1.55. $\mathrm{Inn}(G)$ *is a normal subgroup of* $\mathrm{Aut}(G)$*.*

Definition 1.56. The group of *outer automorphisms* of G is given by the quotient

$$\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G).$$

Definition 1.57. Given a subgroup $H \leq G$, its *centralizer* is the subgroup $C_G(H) := \{g \in G \mid gh = hg \ \forall h \in H\}$.

Proposition 1.58. *Let $N \trianglelefteq G$ be a normal subgroup, then the conjugation action of G on N yields a group homomorphism $\kappa : G \to \mathrm{Aut}(N)$. Then*

$$\kappa^{-1}(\mathrm{Inn}(N)) = C_G(N)N,$$

which is a normal subgroup of G.

Remark 1.59. In the language of the above proposition, we know that κ induces an injective homomorphism

$$\overline{\kappa} : G/C_G(N)N \hookrightarrow \mathrm{Out}(N),$$

so any elements of $G \setminus C_G(N)N$ give rise to non-inner automorphisms of N.

Proposition 1.60. $|\mathrm{Aut}(C_n)| = \phi(n)$*, where ϕ is the* Euler ϕ function *for which $\phi(n)$ is the number of integers in $\{1, \ldots, n\}$ which are relatively prime to n.*

Definition 1.61. A *p-Sylow subgroup* of a finite group G is a subgroup $P \leq G$ which is a p-group, and is such that $|G : P|$ is prime to p. Equivalently, if $G = p^a m$ with $(p, m) = 1$ and $a \geq 1$, then a p-Sylow subgroup is a subgroup of order p^a.

Note: With this convention, the trivial subgroup is not p-Sylow for any prime p.

Write $\mathrm{Syl}_p(G)$ for the set of p-Sylow subgroups of G, and write $n_p(G) := |\mathrm{Syl}_p(G)|$. Note that G acts on $\mathrm{Syl}_p(G)$ by conjugation: if $P \leq G$ is a p-Sylow subgroup, so is gPg^{-1} for any $g \in G$.

In the following three theorems, p will be a chosen prime, and G will be a finite group of order $p^a m$, where $a \geq 1$ and $p \nmid m$.

Theorem 1.62 (Sylow 1)**.** *The group G has a p-Sylow subgroup, i.e.,* $\mathrm{Syl}_p(G) \neq \emptyset$*.*

Theorem 1.63 (Sylow 2)**.** *Any two p-Sylow subgroups of G are conjugate, i.e., G acts transitively on* $\mathrm{Syl}_p(G)$ *by conjugation.*

Theorem 1.64 (Sylow 3)**.** *If P is any p-Sylow subgroup of G, then $n_p = |G : N_G(P)|$. Furthermore, $n_p | m$ and $n_p \equiv 1 \bmod p$.*

Lemma 1.65. *Let P, Q be subgroups of a group G with $|P| = p$ and $|Q| = q$ prime and distinct. Further suppose that PQ is a subgroup of G (for example, if $P \subseteq N_G(Q)$ or $Q \subseteq N_G(P)$) and $ab = ba$ for all $a \in P$ and $b \in Q$. Then PQ is isomorphic to the cyclic group C_{pq} of order pq.*

Proof. Since P and Q have prime order, we can write $P = \langle x \rangle$ and $Q = \langle y \rangle$ where $|x| = p$ and $|y| = q$. Set $z = xy$. If $z^k = e$, then $x^k = y^{-k}$ because x and y commute, so that $x^k \in P \cap Q$, which is trivial, since $|P \cap Q|$ has to divide both p and q, which are distinct primes. Hence we must have $x^k = e = y^k$, meaning $|z| = pq$, and we see that PQ is cyclic. $\square$

Proposition 1.66. *If $p < q$ are primes and $q \not\equiv 1 \bmod p$, then every group of order pq is cyclic.*

Proof. By Sylow 3, $n_q | p$ and $n_q \equiv 1 \bmod q$. If $n_q > q$, then $n_q > p$, a contradiction of the fact that $n_q | p$. Hence we must have $n_q = 1$. Let $Q \leq G$ be the unique q-Sylow subgroup of G. Note that since $n_q = 1$ and any conjugate of Q is also a q-Sylow subgroup, we have that Q is a normal subgroup of G. Since $|Q| = q$ is prime, we can write $Q = \langle y \rangle$, where y has order q. Pick any subgroup $P \leq G$ of order p, and write $P = \langle x \rangle$. P acts on Q via conjugation, yielding a map $\kappa : P \to \operatorname{Aut}(Q)$; the order of $\kappa(P)$ must divide both $|P| = p$ and $|\operatorname{Aut}(Q)| = q - 1$ by Lagrange's, and clearly $|\kappa(P)| \leq |P| = p$, so that $|\kappa(P)| \in \{1, p\}$. Since $q \not\equiv 1 \bmod p$, p does not divide $q - 1$, so that we must have $|\kappa(P)| = 1$, meaning $\kappa(P) = \{e\}$. Therefore $ab = ba$ for all $a \in P$ and $b \in Q$. It then follows by Proposition 1.39 and Lemma 1.65 that PQ is a subgroup of G which is isomorphic to C_{pq}. Since $|G| = pq$, it follows that $G = PQ \cong C_{pq}$, as desired. □

Proposition 1.67. *If $|G| = 30$, G has unique 3- and 5-Sylow subgroups and contains a normal subgroup isomorphic to C_{15}.*

Proof. By the Sylow theorems, $n_3 | 10$, $n_3 \equiv 1 \bmod 3$, $n_5 | 6$, and $n_5 \equiv 1 \bmod 5$. Thus $n_3 \in \{1, 10\}$ and $n_5 \in \{1, 6\}$. If $n_3 = 10$ and $n_5 = 6$, then since each subgroup in Syl_3 and Syl_5 are cyclic of prime order, there would be at least $2 \cdot 10 = 20$ distinct order 3 elements in G, and $4 \cdot 6 = 24$ distinct order 5 elements in G, an impossibility since $|G| = 30 < 44$. Thus, one of n_3 and n_5 is 1. Let $P \in \mathrm{Syl}_3$ and $Q \in \mathrm{Syl}_5$, so that since $n_3 = 1$ or $n_5 = 1$, at least one of P or Q is normal in G, so that by the second isomorphism theorem we know that PQ is a subgroup of G. Moreover, $|PQ| \leq 15$ and 3 and 5 divide $|PQ|$, so we must have $|PQ| = 15$. Thus PQ is an index 2 subgroup of G, so PQ is normal in G. By Proposition 1.66, since $|PQ| = 15 = 3 \cdot 5$ and $5 \not\equiv 1 \bmod 3$, we have that PQ is cyclic, as desired. Sylow 3 directly gives that $n_3(PQ) = n_5(PQ) = 1$, so that P and Q are the unique 5- and 3-Sylow subgroups in PQ. We claim this implies $n_3(G) = n_5(G) = 1$. If we had $n_3(G) = 10$, then G would have at least $2 \cdot 10 = 20$ distinct order 3 elements, so that in particular PQ would have to contain at least 5 elements of order 3, meaning PQ would have to contain at least $\lceil 5/2 \rceil = 3$ subgroups of order 3, a contradiction of the fact that $n_3(PQ) = 1$. A similar argument yields that $n_5(G) = 1$, as desired. □

Proposition 1.68. *Let G be a group of order 12. If G does not have a normal 3-Sylow subgroup, then $G \cong A_4$.*

Proof. We have that $n_3 | 4$ and $n_3 \equiv 1 \bmod 3$ by the third Sylow theorem, so either $n_3 = 1$ or $n_3 = 4$. Since G does not have a normal 3-Sylow subgroup, we must have that $n_3 = 4$. The group G acts on $\mathrm{Syl}_3(G)$ by conjugation, yielding a homomorphism

$$\phi : G \to \mathrm{Sym}(\mathrm{Syl}_3(G)) \cong S_4.$$

First we aim to show this map is injective, so that G is isomorphic to a subgroup of order 12 of S_4.

If $P \in \mathrm{Syl}_3(G)$, then $|G : N_G(P)| = n_3 = 4$, meaning $|N_G(P)| = 3$, so that $P = N_G(P)$. The kernel of ϕ consists of the elements of g which normalize all 3-Sylow subgroups of G, and so are in the intersection of all 3-Sylow subgroups. This implies $\ker \phi$ is trivial, so ϕ is injective, as desired.

It remains to show that $\phi(G) = A_4$, which can be done in a number of ways. For instance, G must contain exactly 8 elements of order 3, while there are exactly 8 elements of order 3 in S_4, and they generate A_4. □

Proposition 1.69. *Suppose $|G| = 60$ and $n_5(G) > 1$. Then G is simple.*

Proof. By the third Sylow theorem, we have $n_5 \in \{1, 6\}$, so $n_5 = 6$ by assumption. Now, let H be a non-trivial proper normal subgroup of G. We split into cases.

Case 1. If 5 divides $|H|$, then H contains a 5-Sylow subgroup; being normal, it must contain every 5-Sylow subgroup of G. Thus $|H| \geq 1 + 4 \cdot 6 = 25$, so $|H| = 30$. But we have shown above that every group of order 30 has a unique 5-Sylow subgroup, so this is not possible.

Case 2. If 5 does not divide $|H|$, then $|H|$ divides 12. Now we claim that G must contain a normal subgroup of order 3 or 4. If H itself is not of one of these orders, then $|H| = 6$ or $|H| = 12$. If $|H| = 6$ (resp. $|H| = 12$), then Sylow 3 yields $n_3(H) = 1$ (resp. $n_4(H) = 1$), so H admits a normal 3-Sylow subgroup (resp. a normal 4-Sylow subgroup). Since H is normal, it follows that $n_3(G) = 1$ (resp. $n_4(G) = 1$) as well, so indeed G contains a normal subgroup of order 3 or 4, call it K.

Now G/K has order 15 or 20, and in each case Sylow 3 yields $n_5(G/K) = 1$, so G/K has a normal 5-Sylow subgroup. By the fourth (lattice) isomorphism theorem, the preimage of such a 5-Sylow subgroup with be a normal subgroup of G with order divisible by 5, contradicting the above. □

In general, subgroups of f.g. groups are not f.g.!

Example 1.70. Let $G = F(a, b)$ be the free group on two generators. Write $x_n := a^n b a^{-n} \in G$, and let $H = \langle x_n, n \in \mathbb{Z}\rangle$. Then H is not finitely generated.

Definition 1.71. A poset $(P, \leq)$ has the *ascending chain condition (acc)* if, for every countable sequence $(x_k)_{k\in\mathbb{N}}$ with $x_k \leq x_{k+1}$, there exists m such that $x_k = x_m$ for all $k \geq m$.

A group G has *the ascending chain condition for subgroups* if the set of subgroups ordered by inclusion has the acc.

Proposition 1.72. *TFAE*

(1) G has the acc for subgroups

(2) All subgroups of G are f.g.

Proposition 1.73. *Let $N \trianglelefteq G$. TFAE*

(1) G has the acc for subgroups

(2) Both N and G/N have the acc for subgroups.

Proposition 1.74. *Every f.g. abelian group has the acc for subgroups. In particular, every subgroup of a f.g. abelian group is also f.g.*

Definition 1.75. Let G be a group. We say that an element $a \in G$ is *torsion* if it has finite order, and write $G_{\text{tors}} \subseteq G$ for the subset of torsion elements. A group G is *torsion free* if $G_{\text{tors}} = \{e\}$. A group G is *torsion* if $G_.\text{tors} = G$

Proposition 1.76. *If G is an abelian group then G_{tors} is a subgroup of G.*

Proposition 1.77. *If G is abelian, then G/G_{tors} is torsion free.*

Proposition 1.78. *Every f.g. torsion abelian group is finite.*

Proposition 1.79 (Product Recognition)**.** *Let G be a group, and suppose $G_1, \ldots, G_n \trianglelefteq G$ are* normal *subgroups such that*

(1) $G_1 \cdots G_n = G$, and

(2) $G_k \cap (G_1 \cdots G_{k-1} G_{k+1} \cdots G_n) = \{e\}$ for $k = 1, \ldots, n$.

Then the function

$$\phi : G_1 \times \cdots \times G_n \to G \qquad (g_1, \ldots, g_n) \mapsto g_1 \cdots g_n$$

is an isomorphism of groups.

Proposition 1.80. *If $G = G_1 \times \cdots \times G_n$ and $N_k \trianglelefteq G_k$ for $k = 1, \ldots, n$, then $N = N_1 \times \cdots \times N_n$ is a normal subgroup of G, and there is an isomorphism*

$$G/N \cong (G_1/N_1) \times \cdots \times (G_n/N_n).$$

Theorem 1.81. *Every f.g. abelian group G is isomorphic to one of the form*

$$G \cong F \times \mathbb{Z}^r, \qquad |F| < \infty, \qquad \mathbb{Z}^r = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ copies}}, \qquad r \geq 0.$$

The factors are unique, in the sense that if G admits two such isomorphisms $G \cong F \times \mathbb{Z}^r \cong F' \times \mathbb{Z}^{r'}$, then $F \cong F'$ and $r = r'$.

Theorem 1.82. *Every finite abelian group G is isomorphic to one of the form*

$$G \cong \mathbb{Z}/n_1 \times \cdots \mathbb{Z}/n_s,$$

where

- *$s \geq 0$, each $n_i \geq 2$, $n_{i+1} \mid n_i$ for all $i = 1, \ldots, s-1$.*

Furthermore, the decomposition is unique up to isomorhpism of the factors.

Definition 1.83. A complete set of invariants for a f.g. abelian group

$$G \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_s \times \mathbb{Z}^r$$

are the free rank r and the list $n_1, \ldots, n_s$ of invariant factors. G is finite iff $r = 0$.

Theorem 1.84 (Elementary divisor decomposition)**.** *For every finite abelian group G of order $n = p_1^{a_1} \cdots p_k^{a_k}$, where the $p_1 < \cdots < p_k$ are distinct primes, there is*

(1) an isomorphism $G \cong A_1 \times \cdots \times A_k$, with $|A_i| = p_i^{a_i}$ and $a_i \geq 1$, such that

(2) for each A_i, there is an isomorphism

$$A_i \cong \mathbb{Z}/p_i^{b_{i1}} \times \cdots \times \mathbb{Z}/p_i^{b_{is_i}},$$

with $b_{i1} \geq \cdots \geq b_{is_i}$ and $b_{i1} + \cdots + b_{is_i} = a_i$.

Furthermore, this decomposition is unique, in the sense that if G admits isomorphisms $G \cong B_1 \times \cdots \times B_\ell$ with $|B_i| = a_i^{a_i}$ with q_i prime and $a_j \geq 1$, then $k = \ell$, $p_i = q_i$, and $A_i \cong B_i$.

Definition 1.85. The decomposition described in (1) above is called the *primary decomposition* of G. Part (2) is just giving the invariant factor decomposition of each A_i.

The list of numbers $p_1^{b_{11}}, \ldots p^{b_{ks_k}}$ are the *elementary divisors* of the group G. The list of elementary divisors is a complete isomorphism invariant of a finite abelian group G.

Definition 1.86. Let H, K, G be groups. We say that G is an *extension* of K by H if there exists a normal subgroup $H' \trianglelefteq G$ and isomorphisms $H \cong H'$ and $K \cong G/H'$, equivalently, an exact sequence of groups

$$0 \to H \to G \to K \to 0.$$

The extension is *split* if there is aditionally a subgroup $K' \leq G$ such that the map $K' \to G/H'$ sending $x \mapsto xH'$, equivalently, if there is a homomorphism $s : K \to G$ such that $p \circ s = \mathrm{id}_K$ (in which case $K' = s(K)$).

Example 1.87. Given groups K and H, you can always extend K by H via the *trivial extension*, defined by

$$G := H \times K, \qquad H' := H \times \{e\}..$$

The trivial extension is always split, by $K' = \{e\} \times K$.

Example 1.88. Let $H = K = C_2$. Then both $G_1 = C_2 \times C_2$ and $G_2 = C_4$ are extensions of K by H

$$H' := \{e, a\} \trianglelefteq G_1 = C_2 \times C_2 = \langle a \mid a^2 \rangle \times \langle b \mid b^2 \rangle = \{e, a, b, ab\}, \qquad G_1/H' = \{\bar{e}, \bar{b}\},$$

and

$$H' = \{e, c^2\} \trianglelefteq G_2 = C_4 = \langle c \mid c^4 \rangle = \{e, c, c^2, c^3\}, \qquad G-2/H' = \{\bar{e}, \bar{c}\}.$$

The first extension is split, using $K' = \{e, b\} \leq G_1$, but the second extension is not split.

Definition 1.89. The *extension problem* for groups is to classify, for given H and K, all possible extensions of K by H, up to isomorphism.

Theorem 1.90. *Let H, K be groups, and $\alpha : K \to \mathrm{Aut}(H)$ a homomorphism. Let G be the set $H \times K$, and define a product on G by the rule*

$$(h_1, k_1)(h_2, k_2) := (h_1\alpha(k_1)(h_1), k_1k_2).$$

Then we have the following

(1) *G is a group, with identity element (e, e) and inverses $(h, k)^{-1} := (\alpha(k^{-1})(h^{-1}), k^{-1})$.*

(2) *The subsets $H' = H \times \{e\}$ and $K' = \{e\} \times K$ are subgroups, and there are isomorphisms $H \xrightarrow{\sim} H'$ and $K \xrightarrow{\sim} K'$ defined by $h \mapsto (h, e)$ and $k \mapsto (e, k)$ respectively.*

We now identify H with H' and K with K' via these isomorphisms in the following.

3. *$H \trianglelefteq G$.*
4. *$H \cap K = \{e\}$ and $G = HK$.*
5. *We have $khk^{-1} = \alpha(k)(h)$ for all $h \in H$ and $k \in K$.*

We denote this group G by $H \rtimes G$, or by $H \rtimes_\alpha K$ if we want to make the action of K on H explicit.

Example 1.91. Let $H = F(a)$ and $K = \langle b \mid b^2\rangle$. Let $\phi : K \to \mathrm{Aut}(H)$ be the homomorphism defined by $\phi(b)(a) = a^{-1}$. We obtain a semi-direct product $G = H \rtimes K$. If we identify H and K with the obvious subgroups of G, this means that

$$G = \{a^n \mid n \in \mathbb{Z}\} \coprod \{a^n b \mid n \in \mathbb{Z}\}, \qquad bab^{-1} = a^{-1}.$$

In fact, G is the infinite dihedral group.

Example 1.92. Let $G \subseteq \mathrm{Sym}(\mathbb{R}^n)$ be the set of all functions $\phi : \mathbb{R}^n \to \mathbb{R}^n$ of the form

$$\phi(x) = Ax + b, \qquad A \in \mathrm{GL}_n(\mathbb{R}), \qquad b \in \mathbb{R}^n.$$

This can be shown to be a subgroup. It is a semi-direct product of its subgroups

$$H = \{\phi \mid \phi(x) = x + b,\ b \in \mathbb{R}^n\}, \qquad K = \{\phi \mid \phi(x) = Ax,\ A \in \mathrm{GL}_n(\mathbb{R})\}.$$

Definition 1.93. A *composition series* for a group G is a finite chain of subgroups

$$\{e\} = M_0 \le M_1 \le \cdots \le M_{r-1} \le M_r = G, \qquad r \ge 0,$$

such that

(1) M_{k-1} is a normal subgroup of M_k, for each $k = 1, \ldots, r$, and

(2) the quotient M_k/M_{k-1} is a simple group.

The groups $M_1/M_0, M_2/M_1, \ldots, M_r/M_{r-1}$ are called the *composition factors* of the composition series.

Proposition 1.94. *Every finite group has a composition series.*

Theorem 1.95 (Jordan-Hölder)**.** *Suppose G is a group with a composition series. Then the composition factors of a composition series are unique up to change of permutation. That is, if*

$$\{e\} = M_0 \le \cdots \le M_r = G, \qquad \{e\} = N_0 \le \cdots \le N_s = G$$

are two composition series, then $r = s$ and there exists $\sigma \in S_r$ such that $M_k/M_{k-1} \cong N_{\sigma(k)}/M_{\sigma(k)-1}$ for all $k = 1, \ldots, n$.

Definition 1.96. A group G is *solvable* if it admits a finite chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G,$$

with each $G_k \trianglelefteq G_{k+1}$, such that each quotient G_k/G_{k-1} is abelian. In particular, a finite group G is solvable if its composition factors are abelian, i.e., all cyclic of prime order.

Example 1.97.
- If $N \trianglelefteq G$ and both N and G/N are solvable, then G is solvable.
- Abelian groups are solvable
- Dihedral groups are solvable, since $C_n \trianglelefteq D_{2n}$ with $D_{2n}/C_n \cong C_2$.
- The quarternion group Q_8 is solvable: it has a composition series
$$\{\pm 1\} < \langle i \rangle < Q_8.$$
- S_4 is solvable, since $N = \langle (1\ 2)(3\ 4),\ (1\ 3)(2\ 4) \rangle \trianglelefteq S_4$ and $S_4/N \cong S_3 \cong D_6$.

Definition 1.98. Given elements $x, y \in G$, we write

$$[x, y] := xyx^{-1}y^{-1} \in G$$

for the *commutator* of x and y. For subsets $S, T \subseteq G$, we write

$$[S, T] := \langle [x, y],\ x \in S,\ y \in T \rangle$$

for the subgroup generated by such commutators. In particular, the *commutator subgroup* of G is the subgroup $[G, G]$ generated by all commutators.

Remark 1.99. $[G, G]$ is a normal subgroup of G. The quotient group $G/[G, G]$ is abelian, and is called the *abelianization* of G.

Proposition 1.100. *If $H \trianglelefteq G$, then G/H is abelian iff $[G, G] \leq H$.*

Definition 1.101. The *derived series* of a gorup G is the sequence of subgroups $G^{(k)}$ defined by
- $G^{(0)} = G$,
- $G^{(1)} = [G, G]$,
- $G^{(k)} = [G^{(k-1)}, G^{(k-1)}]$, $k \geq 2$.

We obtain a descending chain of subgroups, each of which is normal in the previous:

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \cdots.$$

Proposition 1.102. *G is solvable iff $G^{(s)} = \{e\}$ for some s.*

Corollary 1.103. *If G is solvable, then so is any subgroup or quotient group of G.*

Definition 1.104. Given a group G, its *upper central series* is defined by
- $Z_0(G) = \{e\}$,
- $Z_1(G) = Z(G)$,
- $Z_{k+1}(G)$ is the preimage under the quotient map $\pi : G \to G/Z_k(G)$ of $Z(G/Z_k(G))$, for all $k \geq 1$.

We ovtain a possibly infinite sequence of subgroups

$$\{e\} = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots \leq G,$$

each of which is normal in G.

Definition 1.105. A group G is *nilpotent* if there exists a c such that $Z_c(G) = G$. The smallest such c is called the *nilpotence class* of G.

Proposition 1.106. *If G is nilpotent, so is any quotient group G/N, and the nilpotence class of G is $\geq$ the nilpotence class of G/N.*

Proposition 1.107. *$Z_k(G_1 \times \cdots \times G_s) = Z_k(G_1) \times \cdots \times Z_k(G_s)$. In particular, if $G_1, \ldots, G_s$ are nilpotent, then so is $G = G_1 \times \cdots \times G_s$.*

Proposition 1.108. *Let p be a prime and G a p-group of order p^a, $a \geq 1$. Then G is nilpotent, and if $a \geq 2$, it has nilpotence class $\leq a - 1$.*

Theorem 1.109. *Let G be a finite group with $p_1, \ldots, p_s$ the distinct primes dividing its order. Then TFAE.*

(1) G is nilpotent.

(2) If $H < G$, then $H < N_G(H)$ (i.e., every proper subgroup of G is proper in its normalizer, or equivalently, G is the only subgroup which is its own normalizer).

(3) $|\mathrm{Syl}_{p_i}(G)| = 1$ for all $i = 1, \ldots, s$ (or equivalently, G has a normal p_i-Sylow subgroup for all $i = 1, \ldots, s$).

(4) $G \cong P_1 \times \cdots P_s$, where $P_i \in \mathrm{Syl}_{p_i}(G)$.

Corollary 1.110. *Any finite abelian group is a product of its Sylow subgroups.*

2. Rings & Modules

Definition 2.1. A *ring* is a set R with binary operations $+$ and $\cdot$ satisfying

- $(R, +)$ is an abelian group with unit 0.
- $(R, \cdot)$ is a semigroup.
- The product $\cdot$ distributes over $+$: $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

If $\cdot$ has a unit element, then R is called a *ring with identity*, and the multiplicative unit will be denoted by 1.

We will only care about rings with identity, so we will simply write "ring" to mean "ring with identity". The *trivial ring* is the unique ring with $1 = 0$.

Definition 2.2. Let R be a ring.

- $a \in R$ is a *unit* if there exists $b \in R$ such that $ab = 1 = ba$. If such a b exists it is obviously unique.
  We write $R^\times$ for the set of units in R, which is a group under $\cdot$.
- $a \in R$ is an *zero divisor* if $a \neq 0$ and there exists $b \in R \setminus \{0\}$ such that either $ab = 0$ or $ba = 0$.
- $a \in R$ is a *non-zero divisor*, or *cancellable*, if $a \neq 0$ and it is not a zero-divisor.

Definition 2.3.
- A *division ring* (or *skew-field*) is a ring with $1 \neq 0$ such that every nonzero element is a unit.
- A field is a commutative division ring.
- An *integral domain* (or just *domain*) is a commutative ring with $1 \neq 0$ and no zero divisors.

Proposition 2.4. *Every finite domain is a field.*

Proof. Since every $a \in R \setminus \{0\}$ is cancellable, the map $x \mapsto ax$ from $R \to R$ is injective. Since $|R| < \infty$ it is bijective by the pigeonhole principle, so there exists some $b \in R$ such that $ab = 1$. $\square$

Definition 2.5. A *subring* of a ring R is a subset $S \subseteq R$ which is a subgroup w.r.t. $+$ and is closed under $\cdot$. It's called a *subring with identity* if in addition $1 \in S$. (Warning: a subring $S \subseteq R$ can have an identity element which is not equal to 1).

Example 2.6. The ring $\mathbb{H}$ of *quarternions* is the set $\mathbb{R}^4$ of 4-tuples of real numbers, where we write "$a + bi + cj + dk$" instead of "(a, b, c, d)". Addition is componentwise, and multiplication is defined using the distributive law and the identities

$$i^2 = j^2 = k^2 = -1 \qquad ij = k = -ji \qquad jk = i = -kj \qquad ki = j = -ik.$$

The quarternions form a division ring.

Definition 2.7. A ring homomorphism is a function preserving addition and multiplication. If the rings have identity, then a homomorphism might not preserve the identity, although usually we will want them to.

Definition 2.8. Let R be a ring and $I \subseteq R$ a subset. We say that I is

- a *left ideal* if I is a subgroup of $(R, +)$ and if $rI \subseteq I$ for all $r \in R$.
- a *right ideal* if I is a subgroup of $(R, +)$ and if $Ir \subseteq I$ for all $r \in R$.
- a *two-sided ideal* if I is both a left and a right ideal.

We will sometimes call two-sided ideals simply *ideals*.

Note if R is commutative then all three of these notions are the same.

If R has an identity, then the *unit ideal* of R is the unique ideal I containing the identity, in which case $I = R$.

Theorem 2.9 (Second isomorphism theorem for rings)**.** *Let $A \subseteq R$ be a subring, and $I \subseteq R$ be an ideal. Then*

(1) $A + I$ is a subring of R.

(2) I is an ideal of $A + I$.

(3) $A \cap I$ is an ideal of A.

(4) $A/(A \cap I) \cong (A + I)/I$ via $x + (A \cap I) \mapsto x + I$.

Theorem 2.10 (Third isomorphism theorem for rings)**.** *Let $I, J \leq R$ be ideals with $I \subseteq J$. Then*

(1) J/I is an ideal in R/I, and

(2) $R/J \cong (R/I)/(R/J)$ via $x + J \mapsto (x + I) + (J/I)$.

Definition 2.11. Let R be a commutative ring with identity, and suppose $A, B \leq R$ are ideals. Then we say A and B are *comaximal* if $A + B = R$, equivalently, if $1 = a + b$ for some $a \in A$ and $b \in B$.

Theorem 2.12 (The Chinese Remainder Theorem)**.** *If $A_1, \ldots, A_n$ are pairwise comaximal ideals in a commutative ring R with identity, then $A_1 \cdots A_n = A_1 \cap \cdots \cap A_n$, and*

$$R/A_1 \cdots A_n \to (R/A_1) \times \cdots \times (R/A_n)$$

sending

$$r + A_1 \cdots A_n \mapsto (r + A_1, r + A_2, \ldots, r + A_n)$$

is a well-defined isomorphism.

Example 2.13. Let $a_1, \ldots, a_n$ be pairwise coprime integers, and $a = a_1 \cdots a_n$. Then $\mathbb{Z}/(a) \cong \mathbb{Z}/(a_1) \times \cdots \times \mathbb{Z}/(a_n)$.

Definition 2.14. A *Euclidean domain* is an integral domain R such that there exists a function $N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that

- for any $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ such that

$$a = qn + r \quad \text{with either } r = 0 \text{ or } N(r) < N(b).$$

Example 2.15. The Gaussian integrs $\mathbb{Z}[i] \subseteq \mathbb{C}$ form a Euclidean domain.

Define
$$N(a+bi) := |a+bi|^2 = (a+bi)(a-bi) = a^2+b^2.$$
Note that $N(\alpha\beta) = N(\alpha)N(\beta)$. Now let $\alpha = a+bi$ and $\beta = c+di$ in $\mathbb{Z}[i]$, then in $\mathbb{C}$ we have
$$\frac{\alpha}{\beta} = r+si = \frac{ac-bd}{c^2+d^2} + \frac{ad+bc}{c^2+d^2}i, \qquad \text{so} \qquad r = \frac{ac-bd}{c^2+d^2} \text{ and } s = \frac{ad+bc}{c^2+d^2} \text{ in } \mathbb{Q}.$$
The number α/β is distance at most $\sqrt{2}/2 = 1/\sqrt{2}$ from some element of $\mathbb{Z}[i]$, which are exactly the points in the integer lattice inside $\mathbb{C}$, so we may choose $p, q \in \mathbb{Z}$ such that $|r-p|, |s-q| \le 1/2$. Then
$$\left|\frac{\alpha}{\beta} - (p+qi)\right|^2 \le |r-p|^2 + |s-q|^2 \le \frac{1}{2}$$
and thus
$$|\alpha - (p+qi)\beta|^2 \le \frac{|\beta|^2}{2}.$$
Therefore setting $\gamma = \alpha - (p+qi)\beta \in \mathbb{Z}[i]$, we have
$$\alpha = (p+qi)\beta + \gamma, \qquad |\gamma|^2 < |\beta|^2.$$
Thus $\mathbb{Z}[i]$ is a Euclidean domain.

Definition 2.16. In a domain R, a *greatest common divisor (gcd)* of $a, b \in R$ with $b \neq 0$ is any element $d \in R$ such that (i) $a, b \in (d)$, and $a, b \in (e) \implies d \in (e)$.

Proposition 2.17. *[GCD algorithm in a Euclidean domain] Given a Euclidean domain R and elements $a, b \in R$, there is an algorithm for computing a gcd of a and b, called the* Euclidean algorithm*. The algorithm works by constructing a sequence of elements of R that begins with the two given elements $r_{-2} = a$ and $r_{-1} = b$ and will eventually terminate with 0:*
$$\{r_{-2} = a, r_{-1} = b, r_0, r_1, \ldots, r_{n-1}, r_n = 0\},$$
where $N(r_{k+1}) < N(r_k)$. The element r_{n-1} will then be the GCD. Explicitly, assuming r_{k-2} and r_{k-1} have been found, one should choose r_k so that
$$r_{k-2} = q_k \cdot r_{k-1} + r_k, \qquad \textit{with } N(r_{k-1}) > N(r_k) \ge 0.$$

Proof. Note that since □

Definition 2.18. Let R be a domain. We can clasify elements of R into exactly one of the following types.

- *Zero.* Just 0.
- *Units.* Elements which have a multiplicative inverse.
- *Reducible elements.* $r \in R$ which is not 0 or a unit, such that $r = ab$ for some a, b which are not 0 or units.
- *irreducible elements.* $r \in R$ which are not 0 or a unit or reducible.

Definition 2.19. We say $a, b \in R$ are *associate* (or *same up to units*) if there exists a unit $u \in R^\times$ such that $b = ua$. Being associate is an equivalence relation on R.

We say that $a \mid b$ iff $(a) \subseteq (b)$. Equivalently if there is $c \in R$ such that $b = ac$.

Proposition 2.20. *Let $a, b \in R$ a domain. TFAE.*

(1) a and b are assocaite.

(2) $a \mid b$ and $b \mid a$.

(3) $(a) = (b)$.

Lemma 2.21. *Let $p \in R$ which is not zero and not a unit. Then $p \in R$ is irreducible iff for all $a \in R$, $(p) \subsetneq (a)$ implies $(a) = R$. That is, p is irreducible iff (p) is maximal amongst proper* principal *ideals.*

In particular if R is a PID, then $p \in R$ is irreducible iff $p \neq 0$ and (p) is maximal.

Corollary 2.22. *If p, q are irreducible elements in a domain, then $p \mid q$ iff p and q are the same up to units.*

Definition 2.23. In a domain R, an element $p \in R$ is *prime* iff $p \neq 0$ and (p) is not a prime ideal. THat is, iff p is nonzero and not a unit, and if $p \mid ab$ implies either $p \mid a$ or $p \mid b$.

Proposition 2.24. *In a domain, prime elements are irreducible.*

Proposition 2.25. *In a PID, an element is prime iff it is irreducible.*

Definition 2.26. A *unique factorization domain* (UFD) is a domain such that every non-zero non-unit $r \in R$ satisfies

(1) $r = p_1 \cdots p_n$ for some irreducibles $p_1, \ldots, p_n \in R$, $n \geq 1$, and
(2) this decomposition is unique up to associates, i.e., if $r = p_1 \cdots p_n = q_1 \cdots q_m$ for irreducibles p_i, q_j, then $m = n$ and there is a a permutation $\sigma \in S_n$ such that $q_k = u_k p_{\sigma(k)}$ for some unit u_k, for $k = 1, \ldots, n$.

Proposition 2.27. *In a UFD, prime and irreducible are equivalent.*

Theorem 2.28. *Every PID is a UFD.*

Definition 2.29. Let R be an integral domain. Say that R has the *ascending chain condition (acc) for principal ideals* if for any collection $(I_k)_{k \in \mathbb{Z}_{\geq 0}}$ of principal ideals in R such that

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots,$$

there exists some n such that $I_k = I_n$ for all $k \geq n$.

Lemma 2.30. *Every PID has the acc for principal ideals.*

Proposition 2.31. *Let R be a domain. If R has the acc for principal ideals, then every nonzero nonunit in R is a finite product of irreducible elements.*

Proposition 2.32. *Let R be an integral domain. If all irreducible elements in R are prime elements, then factorization in irreducibles (when it exists) is unique up to units and reordering.*

Lemma 2.33. *Let $\alpha \in \mathbb{Z}[i]$. If $N(\alpha) \in \mathbb{Z}$ is a prime number, then α is irreducible in $\mathbb{Z}[i]$.*

Proposition 2.34. *If R is commutative with unit, $S \subseteq R$ is a subring (with 1), and $P \leq R$ is a prime ideal, then $S \cap P$ is a prime ideal of S.*

Proposition 2.35. *Let $p \in \mathbb{Z}$ be a prime number, and let $\alpha \in \mathbb{Z}[i]$ be an irreducible element. TFAE*

(1) α is an irreducible divisor of p in $\mathbb{Z}[i]$.
(2) $p\mathbb{Z} = (\alpha) \cap \mathbb{Z}$.

Suppose $\alpha \in \mathbb{Z}[i]$ is irreducible with $(\alpha) \cap \mathbb{Z} = p\mathbb{Z}$ with p a prime integer. We have $p = \alpha\beta$ for some $\beta \in \mathbb{Z}[i]$. Taking norms gives

$$p^2 = N(\alpha)N(\beta).$$

Since α is not a unit, there are two cases

- $N(\alpha) = p^2$, $N(\beta) = 1$, so that β is a unit and thus p and α are associate, so $\alpha \in \{\pm p, \pm pi\}$.

- $N(\alpha) = p$, $N(\beta) = p$, so that both α and β are irreducible, and $p = \alpha\beta$ is an irreducible factorization of p. Thus these are the only two irreducible divisors up to associates, by uniqueness of irreducible factorizations.

As a conclusion, if p is a prime number, then an element $\alpha = a + bi \in \mathbb{Z}[i]$ is an irreducible divisor of p iff one of the following mutually exclusive cases occurs:

(1) $\alpha = \pm p$ or $\alpha = \pm pi$, or

(2) $a^2 + b^2 = p$.

Thus p is prime in $\mathbb{Z}[i]$ iff the equation $a^2 + b^2 = p$ has an integer solution $(a, b) \in \mathbb{Z}^2$.

Lemma 2.36 (Lagrange). *Let p be a prime number of the form $p = 4m + 1$, with $m \in \mathbb{Z}$. Then there exists some $n \in \mathbb{Z}$ such that $p \mid (n^2 + 1)$.*

Theorem 2.37 (Fermat). *A rational prime p is a sum of two squares iff $p = 2$ or $p \equiv 1 \bmod 4$.*

Corollary 2.38. *A prime number p is prime/irreducible in $\mathbb{Z}[i]$ iff $p \neq 2$ and $p \not\equiv 1 \bmod 4$.*

Proposition 2.39. *A positive integer n has the form $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ iff its prime factorization (in $\mathbb{Z}$) $n = p_1^{k_1} \cdots p_r^{k_r}$ (primes p_i pairwise disticnct) is such that: if $p_i \equiv -1 \mod p$, then k_i is even.*

Corollary 2.40. *A positive integer n has the form $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ iff its prime factorization (in $\mathbb{Z}$) $n = p_1^{k_1} \cdots p_r^{k_r}$ (primes p_i pairwise distinct) is such that: if $p_i \equiv -1 \bmod p$, then k_i is even.*

Definition 2.41. Let $\{a_1, \ldots, a_n\}$ be a finite subset of a domain R. Then $d \in R$ is a GCD of the set iff

(1) $(a_1, \ldots, a_n) \subseteq (d)$, and

(2) if $(a_1, \ldots, a_n) \subseteq (e)$ for some $e \in R$, then $(d) \subseteq (e)$.

Proposition 2.42. *If R is a UFD, then every finite subset of R has a GCD.*

Proposition 2.43. *Let R be a UFD, $\{a_1, \ldots, a_n\}$ a finite set of elements in R, and $d, c \in R$ with $c \neq 0$. Then d is a GCD of $\{a_1, \ldots, a_n\}$, if and only if dc is a GCD of $\{a_1 c, \ldots, a_n c\}$.*

Definition 2.44. We say a subset $\{a_1, \ldots, a_n\}$ of a domain R is *relatively prime* if 1 is a GCD for the set. If d is a GCD of a subset $\{a_1, \ldots, a_n\}$ of a UFD, then $\{a_1/d, \ldots, a_n/d\}$ is a relatively prime subset.

Proposition 2.45. *If R is a UFD, $F = \operatorname{Frac} R$ is the fraction field of R, and $c \in F^\times = F \setminus \{0\}$, then we can write $c = a/b$ for $a, b \in R$ with $\{a, b\}$ relatively prime. Furthermore, any two such exrepssions $c = a/b = a'/b'$ differ by a unit: i.e., there exists $u' \in R^\times$ such that $a' = ua$ and $b' = ub$.*

Definition 2.46. For a domain S, we write $\operatorname{Irred}(S) \subseteq S$ for the subset of irreducible elements.

Proposition 2.47. *If $f, g, h \in R[x]$ are such that $f = gh$, then $f \in R \setminus \{0\}$ iff $g, h \in R \setminus \{0\}$.*

Definition 2.48. Let $f = \sum_{k=0}^{n} c_k x^k \in R[x]$. We say that f is *primitive* if the set $\{c_0, \ldots, c_n\}$ of its coefficients is relatively prime. For example, every monic polynomial is primitive.

Proposition 2.49. *Let R be a UFD and let $f \in R[x]$ with $f \neq 0$. Then there exist $a \in R$ and $g \in \operatorname{Prim}(R[x])$ such that*

$$f = ag.$$

Furthermore, this factorization is unique up-to-units in R. That is, if

$$f = ag = a'g', \qquad a, a' \in R, \qquad g, g' \in \operatorname{Prim}(R[x]),$$

then there exists $u \in R^\times$ such that $a' = ua$, $g' = u^{-1}g$.

Proposition 2.50. *Let R be a UFD, let $F := \operatorname{Frac} R$, and let $f \in F[x]$ with $f \neq 0$. Then there exists $c \in F^\times$ and $g \in \operatorname{Prim}(R[x])$ such that $f = cg$, and furthermore this factorization is unique up-to-units in R. That is, if*

$$f = cg = c'g' \in F[x], \qquad c, c' \in F, \qquad g, g' \in \operatorname{Prim}(R[x]),$$

then there exists $u \in R^\times$ such that $c' = uc$ and $g' = u^{-1}g$.

Proposition 2.51 (Gauss' Lemma)**.** *Let f, g be two primitive polynomials over a UFD. Then fg is primitive. I.e., if R is a UFD, then $\operatorname{Prim}(R[x])$ is multiplicatively closed.*

Proposition 2.52. *Let R be a UFD and suppose $f = gh \in R[x]$. Then $f \in \operatorname{Prim}(R[x])$ if $g, h \in \operatorname{Prim}(R[x])$.*

Proposition 2.53. *If R is a UFD, $F := \operatorname{Frac} R$, and*

$$f = gh \in \operatorname{Prim}(R[x]), \qquad g, h \in F[x],$$

there exist

$$c \in F^\times, \qquad , g', h' \in \operatorname{Prim}(R[x]) \qquad \text{such that} \quad g = c^{-1}g', \qquad h = ch', \qquad f = g'h'.$$

Corollary 2.54. *If R is a UFD and $F := \operatorname{Frac}(R[x])$, then $f \in \operatorname{Prim}(R[x])$ is irreducible iff it is irreducible in $F[x]$.*

Corollary 2.55. *If R is a UFD, a nonunit $f \in \operatorname{Prim}(R[x])$ admits a factorization $f = p_1 \cdots p_r$ into primitive irreducibles $p_1, \ldots, p_r$, and this factorization is unique up to reordering and units.*

Theorem 2.56. *Let R be a UFD. Then $R[x]$ is also a UFD. Furthermore, every irreducible $f \in R[x]$ is one of exactly two types.*

(1) $f \in R$ and f is irreducible in R.

(2) $f \in \operatorname{Prim}(R[x])$ and f is irreducible in $F[x]$, where $F := \operatorname{Frac} R$.

Proposition 2.57. *Let F be a field. If $f \in F[x]$ and $a \in F$ is such that $f(a) = 0$, then $f = (x - a)g$ for some $g \in F[x]$.*

Corollary 2.58. *Let F be a field. If $f \in F[x]$ with $\deg f \in \{2, 3\}$, then f is irreducible iff it has a root in f.*

Definition 2.59. Let F be a field, and $f \in F[x]$. Say that $c \in F$ is a *root of multiplicity m* if $m \in \mathbb{Z}_{\geq 0}$ is the largest integer such that $(x - c)^m \mid f$ in $F[x]$.

Proposition 2.60. *If $f \in F[x]$ with $\deg f = n$, then f has at most n roots in F, even if "counted up to multiplicity".*

Proposition 2.61. *Suppose F is the fraction field of a UFD R, and consider a polynomial in $R[x]$ of the form*

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \qquad a_k \in R, \qquad \deg f = n.$$

If $c \in F$ is a root of f, and if $c = r/s$ with $r, s \in R$ is a fraction in lowest terms, then

$$r \mid a_0 \qquad \text{and} \qquad s \mid a_n.$$

In particular, if f is monic, then any roots of f in F are elements $c \in R$ which divide a_0.

The numerator divides the constant term, the denominator divides the leading term.

Example 2.62. The polynomial $f = x^3 - 3x - 1 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$, since by the above the only possible roots are ± 1, but $f(\pm 1) \neq 0$. Because f is monic and thus primitive, it is also irreducible in $\mathbb{Z}[x]$.

Proposition 2.63. *Let R be an integral domain, and $I < R$ a proper ideal. Let $f \in R[x]$ be a monic polynomial of positive degree. If its image $\overline{f} \in (R/I)[x]$ is irreducible in $(R/I)[x]$, then f is irreducible in $R[x]$.*

Example 2.64. Let $R = \mathbb{Q}[x]$ and $I = (x)$. Consider $f = x^3 + y^2 + 3x^2y + 17xy + 1 \in R[y] = \mathbb{Q}[x, y]$. As a polynomial with coefficients in $\mathbb{Q}[x]$, this is monic. Note that $(R/I)[y] \cong \mathbb{Q}[y]$, and reducing mod I amounts to setting $x = 0$, and gives $\overline{f} = y^2 + 1$, which is irreducible in $\mathbb{Q}[y]$, so f is irreducible.

Proposition 2.65 (Eisenstein's criterion)**.** *Let R be a domain with prime ideal $P \subseteq R$, and let $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$ be a monic polynomial over R. If $a_0, \ldots, a_{n-1} \in P$ and $a_0 \notin P^2$, then f is irreducible in $R[x]$.*

Example 2.66 (The cyclotomic polynomial Φ_p)**.** Let $R = \mathbb{Z}$ and $P = (p)$ for some prime p. Then if $f = a_nx^n + \cdots + a_0$ is a monic polynomial in $\mathbb{Z}[x]$ such that $p \mid a_k$ for $k = 0, \ldots, n-1$, and $p \nmid a_0$, then f is irreducible.

For instance, consider $\Phi_p(x) = \sum_{k=0}^{p-1} x^k \in \mathbb{Z}[x]$. This is a factor of

$$x^p - 1 = (x-1)\Phi_p(x),$$

so roots of Φ_p in $\mathbb{C}$ are $\lambda \in \mathbb{C}$ such that $\lambda^p = 1$ but $\lambda \neq 1$.

Let

$$f(x) = \Phi_p(x+1) = \sum_{k=0}^{p-1} \binom{p}{k+1} x^k = x^p + px^{p-1} + \cdots + \frac{p(p-1)}{2}x + p$$

(where the second equality follows by the hockey-stick identity). This has the Eisenstein property for p, so f is irreducible in $\mathbb{Z}[x]$, and thus in $\mathbb{Q}[x]$. (Note: this argument uses the fact that the function $\mathbb{Q}[x] \to \mathbb{Q}[x]$ defined by $f(x) \mapsto f(x+1)$ is an isomorphism of rings, and thus takes irreducible elements to irreducible elements.)

Proposition 2.67. *Let F be a field and $G \leq F^\times$ a finite subgroup of its abelian group of units. Then G is a cyclic group.*

Definition 2.68. Let R be commutative with unit. We say that R is *Noetherian* if it has the ascending chain condition for ideals. That is, if $(I_k)_{k \in \mathbb{N}}$ is an increasing sequence of ideals (so $I_k \subseteq I_{k+1}$ for all $k \in \mathbb{N}$), then there exists some $n > 0$ such that $I_k = I_n$ for all $k \geq n$.

Theorem 2.69. *Let R be commutative with unit. Then R is noetherian iff every ideal in R is f.g.*

Theorem 2.70 (Hilbert basis theorem)**.** *Let R be a Noetherian ring, then $R[x_1, \ldots, x_n]$ is Noetherian.*

Proposition 2.71. *Let M be a cyclic R-module (meaning M has a generating set of size 1). Then there is an isomorphism of R-modules $M \cong R/I$ for some left ideal $I \leq R$.*

Proposition 2.72. *Let $N_1, \ldots, N_k \subseteq M$ be submodules, and set $N := N_1 + \cdots + N_k$. Then TFAE.*

1. *The map $\phi : N_1 \oplus \cdots \oplus N_k \to N$ defined by $\phi(x_1, \ldots, x_k) := x_1 + \cdots + x_k$ is an isomorphism of modules.*
2. *$N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$ for all $j = 1, \ldots, k$.*
3. *Every $x \in N$ can be written* uniquely *in the form $x = x_1 + \cdots + x_k$ with $x_j \in N_j$.*

Definition 2.73. Let R be a ring with 1 (but possibly non-commutative). Suppose M is a right R-module and N is a left R-module. Then an *R-balanced bilinear function* $\beta : M \times N \to A$ is a bilinear function of abelian groups which also satisfies

$$\beta(mr, n) = \beta(m, rn) \text{ for } m \in M,\ n \in N,\ r \in R.$$

Note if $R = \mathbb{Z}$, then any bilinear map is already balanced.

If R is commutative, then left and right R-modules are the same. In this case, if A is also an R-module, then a map $\beta : M \times N \to A$ is *R-bilinear*, if

$$\beta(mr, n) = \beta(m, rn) = r\beta(m, n) \text{ for } m \in M,\ n \in N,\ r \in R.$$

Definition 2.74. Let R be a ring with 1. Let M and N be right and left R-modules, respectively. Then there exists an abelian group $M \otimes_R N$ equipped with a group homomorphism $s : M \times N \to M \otimes_R N$. Moreover, s is the universal R-bilinear map out of $M \times N$, i.e., it yields a bijection between R-balanced bilinear map $M \times N \to A$ and group homomorphisms $M \otimes_R N \to A$. The abelian group $M \otimes_R M$ is called the *tensor product* of M and N over R.

We write $m \otimes n$ for the image of (m, n) under s. Elements of this form are called *simple tensors*.

Proposition 2.75. *Let R be commutative with* 1*. If M and N are free R-modules on bases $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_m\}$ respectively, then $M \otimes_R N$ is a free R-module on the basis $\{u_i \otimes v_j\}_{i=1,\ldots,n,\, j=1,\ldots,m}$.*

Proposition 2.76. *Let R be commutative with* 1*. If M and N are R-modules, generated by subsets S and T respectively, and $M' \subseteq M$ and $N' \subseteq N$ are submodules generated by subsets $U \subseteq M'$ and $V \subseteq N'$, then*

$$M/M' \otimes_R N/N' \cong (M \otimes_R N)/R\{s \otimes v,\ u \otimes t \mid s \in S,\, t \in T,\, u \in U,\, v \in V\}.$$

Definition 2.77. Let R be a domain. An element x in an R-module M is *torsion* if there exists a nonzero $r \in R$ such that $rx = 0$. We say a module M is *torsion* if $M_{\text{tors}} = M$ and is *torsionfree* if $M_{\text{tors}} = \{0\}$.

Lemma 2.78. *Let R be an integral domain. The collection $M_{\text{tors}} \subseteq M$ of torsion elements is a submodule. The quotient module M/M_{tors} is torsionfree.*

Proposition 2.79. *Let R be a domain. Given an R-submodule $N \subseteq M$, the quotient module M/N is torsion iff for all $x \in M$ there exists $c \in R \setminus \{0\}$ such that $cx \in N$.*

Definition 2.80. Let R be a domain and M an R-module. Say that an indexed collection $(x_i \in M)_{i \in I}$ is R-linearly dependent (or just R-dependent) if there exists an indexed collection $(r_i \in R)_{i \in I}$ with $0 < |\{i \in I \mid r_i \neq 0\}| < \infty$ and $\sum_i r_i x_i = 0$. Otherwise the collection is *R-linearly independent*, or just R-independent.

Lemma 2.81. *Let R be a domain and M an R-module. A subset $S \subseteq M$ is R-independent iff the submodule $N = RS$ generated by S is free, with S a free basis of N.*

Definition 2.82. Let R be a domain. The collection of R-independent subsets $S \subseteq M$ is ordered by $\subseteq$. Say that an R-independent subset $S \subseteq M$ is *maximally R-independent* if it is maximal with respect to this ordering, i.e., if whenever $S \subseteq T \subseteq M$ with T an R-independent subset, then $S = T$.

Lemma 2.83. *Let R be a domain. An R-independent subset $S \subseteq M$ is maximal iff M/N is a torsion module where $N = RS$.*

Proposition 2.84. *Every module over an integral domain admits a maximal R-independent subset.*

Proposition 2.85. *Let R be a domain and M an R-module. Suppose we have sequences of elements $v_1, \ldots, v_m$, $w_1, \ldots, w_n$ in M such that*

- *$v_1, \ldots, v_m$ is R-independent, and*
- *$M/R\{w_1, \ldots, w_n\}$ is a torsion module.*

Then

(1) $m \leq n$, and

(2) after reording $w_1, \ldots, w_n$, we have that $M/R\{v_1, \ldots, v_m, w_{m+1}, \ldots, w_n$ is a torsion module.

Proposition 2.86. *Let R be a domain and M an R-module. Let $S \subseteq M$ be a finite subset of size n such that M/RS is torsion. Then there exists a maximal R-independent subset of size $m \leq n$, and every maximal R-independent subset of M has size m.*

We call this m the rank *of M.*

Proposition 2.87. *Let R be an integral domain, M an R-module with $N \subseteq M$ a submodule. If N has finite rank n, and M/N has finite rank m, then M has finite rank $m+n$.*

In particular, if A and B are modules of finite rank, then $\operatorname{rank}(A \oplus B) = \operatorname{rank} A + \operatorname{rank} B$.

Definition 2.88. Let R be a ring with 1 (not necessarily commutative). Given a left R-module M, the *annihilator* of M is the subset

$$\operatorname{Ann}(M) := \{x \in R \mid xM = 0\} = \{x \in R \mid xm = 0 \text{ for all } m \in M\}.$$

Proposition 2.89. $\operatorname{Ann}(M)$ *is a right ideal in R.*

Proposition 2.90. *If $M \cong N$ are isomorphic left R-modules, then* $\operatorname{Ann} M = \operatorname{Ann} N$.

Proposition 2.91. *Let R be a ring and $I, J \subseteq R$ 2-sided ideals. Then $R/I \cong R/J$ as left R-modules iff $I = J$.*

Proposition 2.92. *Every f.g. module over a PID is isomorphic to a finite direct sum of cyclic modules.*

Theorem 2.93 (Modules over a PID: Invariant factor form)**.** *Let R be a PID and M a f.g. R-module.*

- *There exists $t \geq 0$ and a chain of proper ideals $R \supsetneq (a_1) \supseteq \cdots \supseteq (a_t)$ such that*
$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_t).$$
- *The number t and the sequence $(a_1), \ldots, (a_t)$ of ideals are unique, in the sense that if also $M \cong R/(a'_1) \oplus \cdots \oplus R/(a'_{t'})$ with $R \supsetneq (a'_1) \supseteq \cdots \supseteq (a'_{t'})$, then $t = t'$ and $(a_k) = (a_k)'$ for all k.*

Remark 2.94. Write $t = s + r$ with $0 \leq s, r \leq t$ where $(a_1), \ldots, (a_s) \neq (0)$ and $(a_{s+1}) = \cdots = (a_{s+r}) = (0)$. Then this becomes

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_s) \oplus R^r,$$

where each $R/(a_1), \ldots, R/(a_s)$ is a torsion cyclic module, and $\operatorname{rank} M = r$. This is how the invariant factor composition is usually presented.

The ideals $(a_1), \ldots, (a_s)$ are called the *invariant factors*, and $r = \operatorname{rank} M$.

Theorem 2.95 (Modules over a PID: Elementary divisor form)**.** *Let R be a PID, and M a f.g. R-module.*

- *There exist $r, u \geq 0$, and a sequence of elements $p_1^{k_1}, \ldots, p_u^{k_u} \in R$ (not necessarily distinct) with p_i prime and $k_i \geq 1$, such that*
$$M \cong R^r \oplus R/(p_1^{k_1}) \oplus \cdots \oplus R/(p_u^{k_u}).$$
- *The numbers r and u are unique, and the sequence $p_1^{k_1}, \ldots, p_u^{k_u}$ is unique up to reordering and units, in the sense that if also $M \cong R^{r'} \oplus R/(q_1^{\ell_1}) \oplus \cdots \oplus R/(q_{u'}^{\ell_{u'}})$, then $r = r'$, $u = u'$, and the sequence $q_1^{\ell_1}, \ldots, q_u^{\ell_u}$ is the same as $p_1^{k_1}, \ldots, p_u^{k_u}$ up to reordering and units.*

Remark 2.96. In the elementary divisor form, we also have $r = \operatorname{rank} M$. The list $p_1^{k_1}, \ldots, p_u^{k_u}$ are called *elementary divisors*.

Proposition 2.97. *Let R be a PID, M a free R-module of rank m, and $N \subseteq M$ a submodule. Then*

1. *N is a free R-module of some rank $n \leq m$, and*
2. *There exists*
   - *a free basis $x_1, \ldots, x_m$ of M, and*
   - *elements $a_1, \ldots, a_n \in R$ with $(a_1) \supseteq \cdots \supseteq (a_n) \supsetneq (0)$, such that*
   - *$y_1 = a_1 x_1, \ldots, y_n = a_n x_n$ is a free basis of N.*

Lemma 2.98. *Let R be a commutative ring, and M an R-module. Suppose $I \leq R$ is an ideal such that $I \subseteq \operatorname{Ann} M$. That is, $IM = 0$, or more concretely, $am = 0$ for all $a \in I$ and $m \in M$. Then M admits the structure of an R/I-module, defined so that*

$$(r + I)m := rm.$$

Furthermore, if $M \cong N$ as R-modules, and if $IM = 0$, then also $IN = 0$ and the isomorphism is also an isomorphism of R/I-modules.

Proposition 2.99. *Let R be a commutative ring.*

1. *If $\phi : M \to N$ is an isomorphism of R-modules, then ϕ restricts to an isomorphism $IM \to IN$ of submodules. It further induces an isomorphism $M/IM \to N/IN$ on quotient modules, which is an isomorphism of R/I-modules.*
2. *If $M = M_1 \oplus \cdots \oplus M_n$ is an internal diret sum decomposition of an R-module, then $IM = IM_1 \oplus \cdots \oplus IM_n$, and thus $M/IM \cong M/IM_1 \oplus \cdots \oplus M/IM_n$ as R/I-modules.*
3. *If M is a f.g. R-module, then M/IM is f.g. as both an R-module and an R/I-module.*
4. *If M is a f.g. R-module, and $I \leq R$ is a f.g. ideal, then IM is also a f.g. R-module.*

Definition 2.100. Let R be a PID and $p \in R$ a prime, and consider a f.g. module M. Note that $p^{k+1}M = p(p^k M) \subseteq p^k M$. THus we obtain a chain of submodules

$$M = p^0 M \supseteq p^1 M \supseteq p^2 M \supseteq \cdots,$$

each of which is also f.g. We therefore get quotients

$$M/pM, \qquad pM/p^2M, \qquad p^3M/p^2M, \ldots,$$

each of which is a f.g. R/p-module.

Note that since p is irreducible, R/p is a field. For $k \geq 1$ define

$$\alpha_{p^k}(M) := \dim_{R/p} p^{k-1}M/p^kM.$$

Proposition 2.101.

1. *The function α_{p^k} is an isomorphism invariant of f.g. R-modules.*
2. *If $M \cong M_1 \oplus \cdots \oplus M_n$, then $\alpha_{p^k}(M) = \alpha_{p^k}(M_1) + \cdots + \alpha_{p^k}(M_n)$.*
3. *If $M \cong R/(a)$ for some $a \in R$, then*

$$\alpha_{p^k}(M) = \begin{cases} 1 & \text{if } p^k \mid a, \\ 0 & \text{if } p^k \nmid a. \end{cases}$$

In particular, when $a = 0$, this says that $\alpha_{p^k}(R) = 1$.

Remark 2.102. As a consequence of the above proposition, if

$$M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m), \qquad a_k \in R \setminus \{0\},$$

we have

$$\alpha_{p^k}(M) = r + \text{number of } j \in \{1, \ldots, m\} \text{ such that } p^k \mid a_j.$$

Now define

$$\beta_{p^k}(M) = \alpha_{p^k}(M) - \alpha^{p^{k+1}}(M).$$

Then for the above M, we have

$$\beta_{p^k}(M) = \text{number of } j \in \{1, \dots, m\} \text{ such that } p^k \mid a_j \text{ and } p^{k+1} \nmid a_j.$$

By construction, α_{p^k} and thus β_{p^k} are isomorphism invariants, and we have shown that, for any elementary divisor decomposition

$$M \cong R^r \oplus R/(p_1^{k_1}) \oplus \cdots \oplus R/(p_u^{k_u}),$$

we have that $\beta_{p^k}(M)$ =the number of elementary divisors in $p_1^{k_1}, \dots, p_u^{k_u}$ which are the same as p^k up-to-units.

Definition 2.103. Recall that given a *linear operator*, i.e., a pair $(V, T : V \to V)$ where V is an F-vector space and T is an F-linear map, we can give V the structure of an $R = F[x]$-module, so that

$$fv := f(T)v, \qquad f \in F[x], \qquad v \in V.$$

We will write V_T for this $F[x]$-module.

Conversely, every $F[x]$-module M is of the form V_T for some (V, T), where V is the underlying F-vector space of the module M (so $V = M$ as an abelian group), and T is defined by $T(v) := xv$. So $F[x]$-modules are really the same as F-linear operators.

There is a further dictionary:

- Submodules of V_T correspond to *T-invariant subspaces*, i.e., vector spaces $W \subseteq V$ such that $T(W) \subseteq W$.
- Homomorphisms $\phi : V_T \to W_U$ of $F[x]$-modules correspond to linear maps which *intertwine* U and V, i.e., linear maps $\phi : V \to W$ such that $\phi \circ T = U \circ \phi$.
- V_T and V_U are isomorphic as $F[x]$-modules iff the linear operators T and $U is$ are *similar*, i.e., if there exists a linear isomorphism $\phi : V \to V$ such that $U = \phi \circ T \circ \phi^{-1}$.
- Given (V, T), the space V is f.d. over F if and only if V_T is f.g. and torsion as an $F[x]$-module.

Given (V, T) f.d., consider the annihilator ideal $\mathrm{Ann}(V_T) = (f) \subseteq F[x]$. By the classification theorem, we can write $V_T \cong \bigoplus_{k=1}^m R/(f_k)$ for some nonzero f_k, and therefore $0 \neq f_1 \cdots f_m \in \mathrm{Ann}(V_T)$, so that $f \neq 0$. We usually assume f is monic, in which case we call f the *minimal polynomial* of T.

Proposition 2.104. *Consider (V, T) with V f.d., and f the minimal polynomial of T. For any $c \in V$ TFAE.*

(1) There exists $v \in V$ with $v \neq 0$ such that $Tv = cv$. That is, c is an eigenvalue of T.

(2) $f(c) = 0$.

Remark 2.105. Given any $F[x]$-module decomposition

$$V_T \cong M_1 \oplus \cdots \oplus M_m = F[x]/(f_1) \oplus \cdots \oplus F[x]/(f_m),$$

we can give a block matrix representation of T of the form

$$\left(\begin{array}{c|c|c|c} B_1 & & & \\ \hline & B_2 & & \\ \hline & & \ddots & \\ \hline & & & B_m \end{array}\right)$$

by choosing an F-basis $e_1, \dots, e_n$ of V, so that the first batch of basis elements are in M_1, the second batch in M_2, and so on. We'll describe some choices for cyclic modules.

Given $V_T = F[x]/(f)$ with $f = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$ a monic polynomial over F, we can use the basis

$$e_1 = \overline{1}, \quad e_2 = \overline{x}, \quad \ldots, \quad e_i = \overline{x}^{i-1}, \quad \ldots, \quad e_k = \overline{x}^{k-1}.$$

Then the matrix describing the operator T in this basis is the $k \times k$ *companion matrix*

$$C_f = \begin{pmatrix} 0 & 0 & \ldots & \ldots & 0 & -b_0 \\ 1 & 0 & \ldots & \ldots & 0 & -b_1 \\ 0 & 1 & \ldots & \ldots & 0 & -b_2 \\ \vdots & \vdots & \ddots & & \vdots & \vdots \\ \vdots & \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & \ldots & 1 & -b_{k-1} \end{pmatrix}$$

A matrix is in *rational canonical form* if it is a diagonal block matrix whose non-trivial bloxks are companion matrices $C_{f_1}, \ldots, C_{f_m}$ for non-constant monic polynomials f_k such that $f_1 \mid f_2 \mid \cdots \mid f_m$.

Theorem 2.106 (Rational canonical form)**.** *Given an operator (V, T) on a f.d. vector space, there exists a basis w.r.t. which the matrix A of T is in rational canonical form. Furthermore, the rational canonical form of the matrix is unique.*

In particular, if the blocks of the rational canonical form of T are the companion matrices associated to non-constant monic polynomials $f_1 \mid f_2 \mid \cdots \mid f_m$, then the f_j's are called the invariant factors *of T, in the sense that*

$$V_T \cong \bigoplus_{j=1}^{m} F[x]/(f_j)$$

is an invariant factor decomposition of the $F[x]$-module V_T.

Remark 2.107. Note that the characteristic polynomial of the companion matrix is

$$\det(xI - C_f) = f(x),$$

and thus if $V_T \cong \bigoplus_{k=1}^{m} F[x]/(f_k)$ with f_k monic, then the characteristic polynomial of T is

$$\det(xI - T) = f_1(x) \cdots f_m(x).$$

If f is the minimal polynomial of T, then $f_1 \cdots f_m \in \operatorname{Ann}(V_T) = (f)$.

Putting together the above results, we have the following result

Proposition 2.108. *Let V be an n-dimensional F-vector space, and let $T : V \to V$ be a linear transformation. Then*

(1) The characteristic polynomial of T is the product of all the invariant factors of T.

(2) (Cayley-Hamilton) The minimal polynomial of T divides the characteristic polynomial of T.

(3) The characteristic polynomial of T divides some power of the minimal polynomial of T. In particular, these polynomials have the same roots, not counting multiplicities.

Given the characteristic and minimal polynomials of a 2×2 or 3×3 matrix over F, the above proposition is completely enough to determine the invariant factors of the matrix.

Definition 2.109. If $V_T = F[x]/(x - c)^k$, then in terms of the basis

$$e_1 = (\overline{x} - c)^{k-1}, \quad e_2 = (\overline{x} - c)^{k-2}, \quad \ldots, \quad e_{k-1} = \overline{x} - c, \quad e_k = 1,$$

the matrix describing T is the $k \times k$ *Jordan matrix*

$$J_k(c) := \begin{pmatrix} c & 1 & 0 & \cdots & \cdots & 0 & 0 \\ 0 & c & 1 & \cdots & \cdots & 0 & 0 \\ 0 & 0 & c & \cdots & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \cdots & c & 1 \\ 0 & 0 & 0 & \cdots & \cdots & 0 & c \end{pmatrix}$$

with c's along the diagonal, 1's along the first superdiagonal, and 0's elsewhere.

Thus for an operator T whose characteristic (or minimal) polynomial is a product of linear factors in $F[x]$ (e.g., if F is algebraically closed), the elementary divisors of T will all have the form $(x-c_i)^{k_i}$ with $c_i \in F$ and $k_i \geq 1$, in which case there exists a basis such that T is represented in *Jordan canonical form*, i.e., as a diagonal block matrix whose blocks are Jordan matrices, and which is unique up to reordering the Jordan blocks.

3. Galois theory

Definition 3.1. Let $F \subseteq K$ be a field extension. Then we define the *degree* of the extension K/F to be

$$[K : F] := \dim_F K.$$

The extension is *finite* if $[K : F] < \infty$.

Proposition 3.2 (Tower law)**.** *Suppose we have field inclusions $F \subseteq K \subseteq L$. Then*

$$[L : F] = [L : K][K : F].$$

Definition 3.3. Given fields K and L, write $\operatorname{Emb}(K, L)$ for the set of ring homomorphisms (field embeddings) $K \hookrightarrow L$.

Definition 3.4. If K/F and L/F are field extensions, a *homomorphisms of extensions* is a ring map $\phi : K \to L$ such that $\phi|_F = \mathrm{id}_F$.

Definition 3.5. Let F be a field. Write $\operatorname{Irred}(F) \subseteq F[x]$ for the set of *monic and irreducible* polynomials over F.

Remark 3.6. Let $f \in \operatorname{Irred}(F)$, and identify F with its image under the canonical map $F \hookrightarrow K := F[x]/(f)$. Then K is a field (since (f) is maximal in $F[x]$) and $[K : F] = \deg f$.

Definition 3.7. Let F be a field, and define $F(x) := \operatorname{Frac} F[x]$. Then $[F(\alpha) : F] = \infty$.

Definition 3.8. Given a field extension K/F and a subset $S \subseteq K$, we write $F(S) \subseteq K$ for the subfield of K generated by $F \cup S$, i.e., $F(S)$ is the intersection of all subfields of K containing F and S.

Definition 3.9. An extension K/F is *simple* if $K = F(\alpha)$ for some element $\alpha \in K$.

Example 3.10. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Proof. Clearly we have $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$ as $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a field containing $\mathbb{Q}$ and $\sqrt{2} + \sqrt{3}$. To see the opposite inclusion, we need to show that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. To see this, note

$$\begin{aligned} \frac{5}{2} \cdot \frac{1}{\sqrt{2} + \sqrt{3}} + \frac{1}{2}\left(\sqrt{2} + \sqrt{3}\right) &= \frac{5}{2} \cdot \frac{\sqrt{2} - \sqrt{3}}{5} + \frac{1}{2}\left(\sqrt{2} + \sqrt{3}\right) \\ &= \frac{1}{2}\left(\sqrt{2} - \sqrt{3} + \sqrt{2} + \sqrt{3}\right) = \sqrt{2}. \end{aligned}$$

and

$$\begin{aligned}-\frac{5}{2}\cdot\frac{1}{\sqrt{2}+\sqrt{3}}+\frac{1}{2}\left(\sqrt{2}+\sqrt{3}\right) &= -\frac{5}{2}\cdot\frac{\sqrt{2}-\sqrt{3}}{5}+\frac{1}{2}\left(\sqrt{2}+\sqrt{3}\right)\\ &= \frac{1}{2}\left(-\sqrt{2}+\sqrt{3}+\sqrt{2}+\sqrt{3}\right)=\sqrt{3}.\end{aligned}$$ □

Definition 3.11. Let K/F be a field extension, and suppose $\alpha \in K$. Consider the subfield $F(\alpha) \subseteq K$ generated by F over α. Observe that we can always evaluate a polynomial $f \in F[x]$ at α. There are two cases.

(1) There exists a nonzero $f \in F[x]$ such that $f(\alpha) = 0$. In this case we say that α is *algebraic* over F.

(2) There does not exist a nonzero $f \in F[x]$ such that $f(\alpha) = 0$. In this case we say that α is *transcendental* over F.

Proposition 3.12. *Let $\alpha \in K$ be algebraic over F. Then there exists a unique irreducible monic polynomial $m \in \mathrm{Irred}(F)$ such that $m(\alpha) = 0$. Furthermore, a polynomial $f \in F[x]$ has a root iff $m \mid f$ in $F[x]$.*

This m is called the minimal polynomial *of α over F.*

Proposition 3.13. *If $\alpha \in K$ is transcendental over F, then there is a unique isomorphism of F-extensions*

$$\phi : F(x) \xrightarrow{\sim} F(\alpha), \qquad \textit{such that } \phi(x) = \alpha.$$

As a consequence, $[F(\alpha) : F]$ is finite.

Proposition 3.14. *Suppose K/F is a field extension with $K = F(\alpha)$ for some $\alpha \in K$. There are two cases:*

(1) $[K : F] < \infty$. Then α is algebraic over F, and there is a unique isomorphism of F-extensions of the form

$$\phi : F[x]/(f) \to K, \qquad f = m_{\alpha/F} \in \mathrm{Irred}(F), \qquad \phi(\overline{x}) = \alpha.$$

(2) $[K : F] = \infty$. Then α is transcendental over F, and there is a unique isomorphism of F-extensions of the form

$$\phi : F(x) \to K, \qquad \phi(x) = \alpha.$$

Definition 3.15. An extension K/F is *finite* if $[K : F] < \infty$. It is *finitely generated* if $K = F(\alpha_1, \dots, \alpha_n)$ for some finite list of elements $\alpha_1, \dots, \alpha_n \in K$.

Proposition 3.16. *Let L/F be an extension and $\alpha_1, \dots, \alpha_n \in L$ a finite list of elements. Let $K = F(\alpha_1, \dots, \alpha_n)$. Then TFAE:*

(1) $[K : F] < \infty$.

(2) Every element $\beta \in K$ is algebraic over F for all $k = 1, \dots, n$.

Furthermore, if any of these hold, then $[K : F] \leq d_1 \cdots d_n$, where d_j is the degree of the minimal polynomial of α_j over F.

Lemma 3.17. *Let $F \subseteq K \subseteq L$ and $\alpha \in L$ such that α is algebraic over F and $[K : F] < \infty$. Then*

$$[K(\alpha) : K] \leq [F(\alpha) : F] \qquad \textit{and} \qquad [K(\alpha) : F(\alpha)] \leq [K : F].$$

Definition 3.18. Given subfields $F \subseteq K, K' \subseteq L$, the *composite extension* is the subfield of L generated over F by $K \cup K'$. It is usually written $KK' \subseteq L$.

Clearly if $K = F(\alpha_1, \dots, \alpha_m)$ and $K' = F(\beta_1, \dots, \beta_n)$, then $KK' = F(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$.

Proposition 3.19. *If K/F and K'/F are subextensions of L/F which are finite over F, then*

$$[KK' : K] \leq [K' : F], \qquad [KK' : K'] \leq [K : F], \qquad [KK' : F] \leq [K : F][K' : F].$$

Definition 3.20. We say K/F is *algebraic* if every $\alpha \in K$ is algebraic in F.

Proposition 3.21. *If L/F is an extension and $\alpha, \beta \in L$ are algebraic over F, then $\alpha + \beta, \alpha\beta, -\alpha, \alpha^{-1}$ are algebraic over F.*

Proof. Since $F(\alpha)/F$ and $F(\beta)/F$ are finite extensions, the composite extension $F(\alpha, \beta)/F$ is also finite and thus algebraic. Since $\alpha + \beta$, $\alpha\beta$, $-\alpha$, and $\alpha^{-1} \in F(\alpha, \beta)$, these are algebraic elements. □

Definition 3.22. An *algebraic number* is an $\alpha \in \mathbb{C}$ which is algebraic over $\mathbb{Q}$, i.e., is the root of some nonzero $f \in \mathbb{Q}[x]$.

Write $\mathbb{Q}^{\text{alg}}$ for the set of algebraic numbers. Then $\mathbb{Q}^{\text{alg}}$ is a subfield of $\mathbb{C}$ by the above proposition.

Remark 3.23. Given r distinct primes $p_1, \ldots, p_r$, one can check that $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r}) : \mathbb{Q}] = 2^r$. Thus it follows by the tower rule that $\mathbb{Q}^{\text{alg}}/\mathbb{Q}$ is an infinite extension.

Proposition 3.24. *If $F \subseteq K \subseteq L$ such that K/F and L/K are algebraic extensions, then L/F is an algebraic extension.*

Definition 3.25. We say that a field K is *algebraically closed* if every nonconstant $f \in K[x]$ has a root in K.

If f has a root $c \in K$ then f factors as $(x - c)g \in K[x]$. Thus if K is algebraically closed then every nonzero polynomial over K *splits* over K, i.e., is a product of degree 1 polynomials.

Example 3.26. The complex numbers $\mathbb{C}$ form an algebraically closed field.

Example 3.27. The field $\mathbb{Q}^{\text{alg}}$ is algebraically closed. To see this, suppose $f \in \text{Irred}(\mathbb{Q}^{\text{alg}})$. This has a root $\alpha \in \mathbb{C}$, and I want to show it is in $\mathbb{Q}^{\text{alg}}$. But we have a sequence of algebraic extensions $\mathbb{Q} \subseteq \mathbb{Q}^{\text{alg}} \subseteq \mathbb{Q}^{\text{alg}}(\alpha)$, and therefore $\mathbb{Q}^{\text{alg}}(\alpha)/\mathbb{Q}$ is algebraic, i.e., $\alpha \in \mathbb{Q}^{\text{alg}}$.

Proposition 3.28. *A field K is algebraically closed iff for any algebraic extension L/K we have $L = K$.*

Definition 3.29. An *algebraic closure* is an extension $\overline{F}/F$ which is algebraic, and is such that every non-constant polynomial $f \in F[x]$ splits over $\overline{F}$, i.e., is a product of degree 1 factors.

Proposition 3.30. *Given an extension K/F, we have that K is an algebraic closure of F iff (i) K/F is algebraic, and (ii) K is algebraically closed. Algebraic closures are algebraically closed.*

Proposition 3.31. *If K/F is an extension and K is algebraically closed, then K contains a unique algebraic closure $\overline{F}$ of F, which is equal to the subset of elements which are algebraic over F.*

Proposition 3.32. *Let K/F be an extension with* $\text{char}(F) \neq 2$ *and $[K : F] = 2$. Then $K = F(\sqrt{d})$ for some $d \in F$ which is not a square in F.*

Proof. Pick some $\alpha \in K \setminus F$, then since $[K : F] = 2$, we have $K = F(\alpha)$. Let f be the mimimal polynomial of α over F, so $f = x^2 + bx + c$ for some $b, c, \in F$. Let $d = b^2 - 4c$. Then

$$(2\alpha + b)^2 = 4\alpha^2 + 4b\alpha + b^2 = 4(-b\alpha - c) + 4b\alpha + b^2 = b^2 - 4c = d,$$

so we can set $\sqrt{d} = 2\alpha + b \in K$. Clearly $\sqrt{d} \notin F$, since otherwise we would have $\alpha = (-b + \sqrt{d})/2 \in F$. Thus $K = F(\sqrt{d})$. □

Remark 3.33. If $\operatorname{char} F = 2$, then if we try to do this it turns out that $\sqrt{d} = b \in F$, so it does not generate K over F.

Definition 3.34. We say that a finite extension K/F is *2-radical* if there exists a finite tower of subfields of the form

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = K, \qquad [K_j : K_{j-1}] = 2.$$

Example 3.35. In each of

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[8]{2}) \subseteq \mathbb{Q}(sqrt[16]2) \subseteq \mathbb{Q}(\sqrt[32]{2}) \subseteq \cdots$$

and

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right) \subseteq \mathbb{Q}\left(\sqrt{1+\sqrt{1+\sqrt{2}}}\right) \subseteq \mathbb{Q}\left(\sqrt{1+\sqrt{1+\sqrt{1+\sqrt{2}}}}\right) \subseteq \cdots,$$

each intermediate extension has degree 2.

Remark 3.36. If K/F is 2-radical then $[K : F] = 2^r$ for some r, but the converse is not true.

Proposition 3.37. *If K/F and K'/F are finite subextensions of L/F which are 2-radical, then the composite extension KK'/F is 2-radical.*

Proof. Factor K/F as a sequence of degree 2 extensions $K_j = K_{j-1}(\alpha_j)$ with $K_0 = F$ and $K_r = K$. Then we have a chain of extensions

$$K' = K'K_0 \subseteq K'K_1 \subseteq K'K_2 \subseteq \cdots \subseteq K'K_n = KK'.$$

Each intermediate extension is a simple extension since $K'K_j = K'K_{j-1}(\alpha_j)$, and we know that $[K'K_j : K'K_{j-1}] \leq [K_j : K_{j-1}] = 2$. $\square$

Definition 3.38. Given $F \subseteq \mathbb{C}$, let

$$F^{2\text{rad}} := \bigcup_{\substack{F \subseteq L \subseteq \mathbb{C} \\ L/F \text{ is 2-radical}}} L.$$

Thus $\alpha \in F^{2\text{rad}}$ iff there exists a finite 2-radical extension L/F with $\alpha \in L$. We see that $F^{2\text{rad}}$ is a subfield of $\mathbb{C}$, using that if L, L' are 2-radical extensions over F then so is LL'.

Definition 3.39. A field K is said to be *squareroot closed* if every element of K has a square root in K.

Proposition 3.40. *For $F \subseteq \mathbb{C}$, the subfield $F^{2\text{rad}}$ is the smallest subfield of $\mathbb{C}$ containing F which is squareroot closed.*

Definition 3.41. Let $\mathcal{P}$ be a set of points in $\mathbb{C}$, and suppose $\mathcal{P}$ contains at least two points. Then given $\alpha \in \mathbb{C}$, we say α is *construcible from* $\mathcal{P}$ if α can be obtained as the intersection of lines and circles drawn as follows:

- you can draw a line between any two distinct points of $\mathcal{P}$, and
- you can draw a circle with center at a point a of $\mathcal{P}$ and radius $r = |b - a|$ where b is some other point belonging to $\mathcal{P}$.

We say α is just *constructible* if it is constructable from $\mathcal{P} = \{0, 1\}$.

Theorem 3.42. *Let $\mathcal{P} \subseteq \mathbb{C}$, and suppose $\mathcal{P}$ contains 0 and 1. Then a point $\alpha \in \mathbb{C}$ is construcible from $\mathcal{P}$ iff $\alpha \in F^{2\text{rad}}$, where $F \subseteq \mathbb{C}$ is the subfield generated by $\mathcal{P}$.*

Here are some impossibility results which follow from this, using only the fact that $\alpha \in \mathbb{Q}^{2\text{rad}}$ must have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^r$.

- *Cannot duplicate the cube.* Given r we want to product $r\sqrt[3]{2}$, i.e., to construct $\alpha = \sqrt[3]{2}$. But $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.
- Cannot trisect every angle. In particular $\theta = 2\pi/3$ cannot be trisected. This amounts to showing that $\zeta := e^{2\pi i/9}$ is not constructible.

  We know that $\zeta^9 = 1$, but $\zeta^3 \neq 1$. Since $0 = \zeta^9 - 1 = (\zeta^3 - 1)(\zeta^6 + \zeta^3 + 1)$, we see that ζ is a root of $f = x^6 + x^3 + 1 \in \mathbb{Q}[x]$, so $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leq 3$. Let $\alpha = \zeta + \zeta^{-1} \in \mathbb{Q}(\zeta)$. Using $f(\zeta) = 0$, you can show that

  $$\alpha^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} = 3\alpha - 1.$$

  So α is a root of $g = x^3 - 3x + 1 \in \mathbb{Q}[x]$. By the rational root test this has no root in $\mathbb{Q}$ so. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Since $[\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$, we see that 3 divides $[\mathbb{Q}(\zeta) : \mathbb{Q}]$.
- *Cannot square the circle.* That is, given a circle with radius r, produce a square with side $\sqrt{\pi}r$. But $\sqrt{\pi}$ is not constructible. If it were, than it would be algebraic over $\mathbb{Q}$, and thus $\pi \in \mathbb{Q}(\sqrt{\pi})$ would be algebraic over $\mathbb{Q}$, but by Lindemann's theorem it is not.
- *Cannot construct the regular heptagon.* Show that $\zeta := e^{2\pi i/7} \in \mathbb{Q}^{2\text{rad}}$. Its minimal polynomial over $\mathbb{Q}$ is $\Phi_7 = x^6 + \cdots + x + 1$, so $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$.

Definition 3.43. Let $f \in F[x]$ with $f \neq 0$. A *splitting field* of f is an extension Σ/F such that
- f *splits* over Σ, i.e., $f = c(x - \alpha_1) \cdots (x - \alpha_n)$ for some $c, \alpha_1, \ldots, \alpha_n \in \Sigma$ with $c \neq 0$, and
- Σ is generated over F by the roots of f, i.e., $\Sigma = F(\alpha_1, \ldots, \alpha_n)$. (Equivalently: the only subfield of Σ over which f splits is Σ itself.)

Proposition 3.44. *If L/F is an extension and $f \in F[x]$ splits over L, then the subfield $\Sigma = F(\alpha_1, \ldots, \alpha_n)$ generated by the roots of f in L is a splitting field of f.*

Proof. Obvious. □

Example 3.45. If $f = (x^2 + 1)(x^2 - 5) \in \mathbb{Q}[x]$, then $\Sigma = \mathbb{Q}(i, \sqrt{5})$ is a splitting field.

Proposition 3.46. *Let F be a field. Then every nonzero $f \in F[x]$ admits a splitting field.*

Corollary 3.47. *If Σ/F is a splitting field of $f \in F[x]$, then $[\Sigma : F] \leq n!$, where $n = \deg f$.*

Example 3.48 (Cyclotomic extensions)**.** Let $\zeta \in L$ be a primitive n^{th} root of unity, i.e., an element of order n in $L^\times$. Then for $F \subseteq L$, the subfield $K = F(\zeta)$ is the splitting field of $f = x^n - 1$.

This is because the elements $1, \zeta, \ldots, \zeta^{n-1}$ are pairwise distinct (since $|\zeta| = n$), and are all clearly roots of f contained in K. Thus $f = (x-1)(x-\zeta) \cdots (x-\zeta^{n-1})$ and clearly K is generated over F by the roots.

The degree of the extension $[F(\zeta) : F]$ will be less than n since $f = (x - 1)g$ (unless $n = 1$).

Let $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$. The field $\mathbb{Q}(\zeta_n)$ is called a *cyclotomic field*. We know that if $n = p$ is prime, then $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, since Φ_p is irreducible over $\mathbb{Q}$.

Example 3.49. Let $f = x^p - 2 \in \mathbb{Q}[x]$ where p is a prime number. Note that f is irreducible by Eisenstein's criterion.

If α is a root of this (e.g., $\sqrt[p]{2} \in \mathbb{R}$), so is $\alpha\zeta^k$, where ζ is some fixed primitive p^{th} root of unity. That is, the roots of f in $\mathbb{C}$ are

$$\alpha,\ \alpha\zeta,\ \alpha\zeta^2,\ \ldots,\ \alpha\zeta^{p-1}.$$

As these are distinct (since $\zeta^k \neq 1$ if $p \nmid k$), thede are distinct roots of f, so $\Sigma = \mathbb{Q}(\alpha, \zeta)$ is a splitting field of f (note that $\zeta = (\alpha\zeta)\alpha^{-1}$ can be written in terms of roots of f, so it must be in the splitting field). Since $[\Sigma : \mathbb{Q}(\zeta)] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] = p$, we have

$$[\Sigma : \mathbb{Q}] \leq (p - 1)p,$$

but it is necessarily divisible by both p and $p-1$, so (since these are relatively prime) $[\Sigma : \mathbb{Q}] = p(p-1)$.

Definition 3.50. Given a polynomial
$$f = a_0 + a_1 x + \cdots + a_n x^n \in F[x],$$
define its *formal derivative* by the formula
$$Df := a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1} \in F[x].$$
It is straightforward to see that $D(f+g) = Df + Dg$, $D(fg) = (Df)g + f(Dg)$, $Dc = 0$, and $D(cf) = cD(f)$ if $f, g \in F[x]$ and $c \in F$.

Definition 3.51. We say that a nonzero polynomial $f \in F[x]$ is *separable* if f and Df are relatively prime in $F[x]$.

Exercise 3.52. Show that if $f = gh \in F[x]$ and f is separable than so are g and h.

Proof. Write $f = \sum_{j=0}^{n} a_j x^j$, then since f and Df are relatively prime, there exists $u, v \in F[x]$ such $uf + v(Df) = 1$. Then we have
$$(uh + vDh)g + vhDg = ugh + v((Dg)h + gDh) = ugh + vD(gh) = uf + vDf = 1,$$
so that indeed g and Dg are coprime, so g is separable. Similarly h is separable, by symmetry. $\square$

Remark 3.53. If $F \subseteq K$ and $f \in F[x]$, then f is separable over F iff it is separable over K.

To see this: If f is separable over F, then $1 = uf + vDf$ for some $u, v \in F[x] \subseteq K[x]$, so f is separable over K as well. On the other hand, if f is separable over K, then any common divisor $d \in F[x]$ of $\{f, Df\}$ is also a common divisor of these in $K[x]$, so $d \in F^{\times}$, and thus f is separable over F.

Exercise 3.54. Show that if $\phi : F \to K$ is a homomorphism of fields, then $f \in F[x]$ is a separable polynomial iff $\phi(f) \in K[x]$ is a separable polynomial.

Proposition 3.55. *Let L/F be any extension over which $f \in F[x]$ splits. Then f is separable iff f has no multiple roots in L, iff f and Df have no common roots in L.*

Example 3.56. The polynomial $f = x^4 + 2x^2 + 1 \in \mathbb{Q}[x]$ has $Df = 4x^3 + 4x$. It is not hard to see (e.g., using the Euclidean algorithm) they have a common factor $x^2 + 1$. Thus f is not separable. In fact, $f = (x^2+1)^2$ over $\mathbb{Q}$, and $f = (x-i)^2(x+i)^2$ over $\mathbb{C}$, so all roots are multiple.

Example 3.57. The polynomial $f = x^n - 1$ is separable over $\mathbb{Q}$ since $Df = x^{n-1}$ and $x \nmid f$. Thus f has n distinct roots over $\mathbb{C}$, as we know.

Proposition 3.58. *A nonzero polynomial $f \in F[x]$ is separable iff for some irreducible factorization $f = g_1 \cdots g_n$ over F, we have that (i) each g_k is separable, and (ii) there are no repeated factors, i.e., if $i \neq j$ then $g_i \nmid g_j$.*

Proposition 3.59. *Suppose $f \in F[x]$ is irreducible. Then f is separable iff $Df \neq 0$.*

In particular, if $\operatorname{char} F = 0$, all irreducible polynomials over F are separable.

Example 3.60. Consider a field F of prime characteristic p and $f := x^p - a \in F[x]$, where $a \in F$. Then $Df = px^{p-1} = 0$, meaning f is not separable.

Example 3.61. Consider the field $F = \mathbb{F}_p(t)$ of rational functions over $\mathbb{F}_p$ and let $f = x^p - t$. Then f is irreducible over F but not separable.

Proposition 3.62. *Let $F(\alpha)/F$ be a finite extension, where α has minimal polynomial $m \in F[x]$. Suppose we are given an embedding of fields $\lambda : F \hookrightarrow F'$, and an extension L/F'. Let $m' := \lambda(m) \in F'[x]$. Then for any root $\beta \in L$ of m', there exists a unique embedding $\mu : F(\alpha) \to L$ such that $\mu|_F = \lambda$ and $\mu(\alpha) = \beta$.*

$$\begin{tikzcd} F(\alpha) \arrow[r, tail, dashed, "\alpha\mapsto\beta", "\mu"'] & L \\ F \arrow[u] \arrow[r, "\lambda"] & F' \arrow[u] \end{tikzcd}$$

In fact, there is a bijection

$$\left\{ \begin{array}{c} \mu : F(\alpha) \to L \\ \textit{such that } \mu|_F = \lambda \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \beta \in L \\ \textit{such that } m'(\beta) = 0 \end{array} \right\}$$

$$\mu \longmapsto \mu(\alpha)$$

Proof. Fix the data given in the setup of the proposition, so $F(\alpha)/F$ is a finite extension, $m \in F[x]$ is the minimal polynomial of α, $\lambda : F \to F'$ is an embedding of fields, L/F' is an extension, and $\beta \in L$ is a root of $m' := \lambda(m)$. Then we want to construct an embedding $\mu : F(\alpha) \to L$ which restricts to λ on F and satisfies $\mu(\alpha) = \beta$.

Recall we have an isomorphism $F(\alpha) \cong F[x]/(m)$, so by the universal property of the quotient a map $F(\alpha) \to L$ is the data of a map $F[x] \to L$ whose kernel contains (m). By the universal property of the polynomial ring, a map $F[x] \to L$ is the data of a map $F \to L$ and a chosen element to send x to. Thus, there is a unique map $\widetilde{\mu} : F[x] \to L$ which restricts to the composition $F \xrightarrow{\lambda} F' \hookrightarrow L$ on F and sends $x \mapsto \beta$. Moreover, clearly $m \in \ker \widetilde{\mu}$, as $\widetilde{\mu}(m) = \lambda(m)(\beta) = m'(\beta) = 0$. Hence by the universal property of the quotient, $\widetilde{\mu}$ factors through a map $\mu : F(\alpha) \to L$ which restricts to λ on F and sends α to β, and μ is the unique such map $F(\alpha) \to L$ with these properties. $\square$

It is worth writing out the above proposition in the case $\lambda = \mathrm{id}_F$.

Corollary 3.63. *Let $F(\alpha)/F$ be a finite extension, where α has minimal polynomial $m \in F[x]$. Suppose we are given an extension L/F. Then for any root $\beta \in L$ of m, there exists a unique embedding $F(\alpha) \hookrightarrow L$ such that $\mu|_F = \mathrm{id}_F$ and $\mu(\alpha) = \beta$.*

$$\begin{tikzcd} F(\alpha) \arrow[rr, tail, dashed, "\alpha\mapsto\beta", "\mu"'] & & L \\ & F \arrow[ul, no head] \arrow[ur, no head] & \end{tikzcd}$$

That is, there is a bijection

$$\left\{ \begin{array}{c} \mu : F(\alpha) \to L \\ \textit{such that } \mu|_F = \mathrm{id}_F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \beta \in L \\ \textit{such that } m(\beta) = 0 \end{array} \right\}$$

$$\mu \longmapsto \mu(\alpha)$$

Example 3.64. Let $f := x^3 - 2 \in \mathbb{Q}[x]$, and let $\alpha := \sqrt[3]{2}$. Then there are *three* distinct embeddings $\mu : \mathbb{Q}(\alpha) \to \mathbb{C}$, corresponding to the roots α, $\alpha\omega$, and $\alpha\omega^2$, where $\omega = e^{2\pi i/3}$.

The above proposition has the following consequence.

Remark 3.65. Given a finite extension K/F, we have a recipe for constructing homomorphisms of extensions $K \to L$ over F: Write K/F as a composite of simple extensions

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n, \qquad K_j = K_{j-1}(\alpha_j),$$

and *inductively* construct homomorphisms $\phi_j : F(\alpha_1, \ldots, \alpha_n) \to L$ extending ϕ_{j-1}. At each step there is one choice: $\phi(\alpha_j) \in L$ can be any root of $m_{\alpha_j/K_{j-1}}$.

Proposition 3.66. *Consider*

- *an isomorphism of fields* $\lambda : F \xrightarrow{\sim} F'$,
- *a nonzero polynomial* $f \in F[x]$,
- *a splitting field* Σ/F *of* f,
- *an extension* L/F' *over which* $f' := \lambda(f) \in F'[x]$ *splits.*

Then there exists a homomorphism $\phi : \Sigma \to L$ *such that* $\phi|_F = \lambda$. *The image* $\phi(\Sigma)$ *of* ϕ *is a splitting field of* f' *over* F'.

Proof. We use induction on $\deg f$. If f is constant then $\Sigma = F$ and we take $\phi = \lambda$. So suppose $\deg f \geq 1$, so that $\deg f' = \deg f \geq 1$.

Let α_1 be some root of f in Σ, and let $m = m_{\alpha_1/F} \in \mathrm{Irred}(F)$ be its minimal polynomial. Then $f = mg$ for some $g \in F[x]$. Under $\lambda : F[x] \to F'[x]$ we get a factorization $f' = m'g'$ with $m' = \lambda(m)$. By the hypothesis f' splits over L, so we choose a root $\beta_1 \in L$ of m'. Then by the previous proposition there exists a unique field embedding $\phi_1 : F(\alpha_1) \to F'(\beta_1)$ such that $\phi_1|_F = \lambda$ and $\phi_1(\alpha_1) = \beta_1$. It is straightforward to see that ϕ_1 is in fact an isomorphism (the same proposition can be used ton construct a map $F'(\beta_1) \to F(\alpha_1)$ which restricts to λ^{-1} on F' and sends β_1 to α_1, and it is straightforward to check that this map and ϕ_1 are inverses).

We can factor $f = (x - \alpha_1)h$ over $F(\alpha_1)$. Now note that we are in the same situation: We have

- an isomorphism of fields $\phi_1 : F(\alpha_1) \to F'(\beta_1)$
- a nonezro polynomial $h \in F(\alpha_1)[x]$
- a splitting field $\Sigma/F(\alpha_1)$ of h, and
- an extension $L/F'(\alpha_1)$ over which $\phi_1(h)$ splits.

Since $\deg h < \deg f$, induction applies to produce the desired homomorphism ϕ. $\square$

Corollary 3.67. *Let* Σ/F *and* Σ'/F *be two splitting fields for the same nonzero polynomial* $f \in F[x]$. *Then* Σ *and* Σ' *are isomorphic as extensions of* F.

Proof. By the previous proposition there exists a homomorphism $\phi : \Sigma \to \Sigma'$ such that $\phi|_F = \mathrm{id}_F$, and the image $\phi(\Sigma)$ of ϕ is a splitting field of f over F. Since $\phi(\Sigma) \subseteq \Sigma'$, f splits over $\phi(\Sigma)$, and f splits over Σ', it follows by the definition of a splitting field that $\phi(\Sigma) = \Sigma'$, so ϕ is an isomorphism over F, as desired. $\square$

Definition 3.68. Suppose $G \leq \mathrm{Aut}(K)$ is a group of automorphisms of a field K. Then the set $K^G := \{\alpha \in K \mid g(\alpha) = \alpha \ \forall g \in G\}$ is a subfield of K, called the *fixed field* of the action of the group G.

Proposition 3.69. *Let* $f \in F[x]$, *and let* $R := \{\alpha \in K \mid f(\alpha) = 0\}$ *be the set of roots of* f *in some extension* K/F. *Then any* $\phi \in \mathrm{Aut}(K/F)$ *restricts to a permutation of the set* R, *and this defines a group homomorphism*

$$\iota : \mathrm{Aut}(K/F) \to \mathrm{Sym}(R).$$

Furthermore, if $K = F(R)$, *then* ι *is injective, so* $\mathrm{Aut}(K/F)$ *is isomorphic to a subgroup of* $\mathrm{Sym}(R)$.

Proof. Let $\phi \in \mathrm{Aut}(K/F)$, and let $\alpha \in R$. Then we wish to show that $\phi(\alpha) \in R$. This is clear as

$$f(\phi(\alpha)) = \phi(f(\alpha)) = \phi(0) = 0,$$

where the first equality follows because ϕ fixes F, which the coefficients of f belong to.

Now, suppose $K = F(R)$ and $\phi \in \ker \iota$, so $\phi(\alpha) = \alpha$ for all $\alpha \in R$, i.e., ϕ fixes all roots of f. Then $R \subseteq K^G$ and $F \subseteq K^G$, where $G = \langle \phi \rangle \leq \mathrm{Aut}(K/F)$ is the cyclic subgroup generated by ϕ. Since K^G is a subsextension of $K = F(R)$ containing both F and R, we must have that $K^G = K$, so $\phi = \mathrm{id}$. $\square$

We can use the techniques we have developed to compute the automorphism groups of some field extensions.

Example 3.70. Consider $g = x^3 - 2 \in \mathbb{Q}[x]$. This factors

$$g = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) = (x-\alpha)(x-\alpha\omega)(x-\alpha\omega^2),$$

where $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$. Thus $\Sigma = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \subseteq \mathbb{C}$ is the splitting field.

There are *six* distinct embeddings $\Sigma \to \mathbb{C}$. One of them is the "obvious" inclusion, but there are others. We can construct them in two steps, and we will show that the image of any such embedding is Σ itself.

Suppose we are constructing a map $\phi : \Sigma \to \mathbb{C}$. To start, we will construct its restriction $\phi_1 : \mathbb{Q}(\alpha) \to \mathbb{C}$. From an earlier proposition, the data of such a map is a choice of a root of g, so there are three such maps $\phi_1 : \mathbb{Q}(\alpha) \to \mathbb{C}$ which restrict to the identity on $\mathbb{Q}$, and they are uniquely determined by which of α, $\omega\alpha$, and $\omega^2\alpha$ that ϕ_1 sends α to.

Over $\mathbb{Q}(\alpha)$ we have

$$g = (x-\alpha)g_1, \qquad g_1 = x^2 + \alpha x + \alpha^2,$$

so that the roots of g_1 in $\mathbb{C}$ are $\{\omega\alpha, \omega^2\alpha\}$. These are not real numbers, so they are not in $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Thus g_1 is irreducible over $\mathbb{Q}(\alpha)$. If $\phi_1(\alpha) = \omega^k\alpha$, then $\phi_1(g_1) = x^2 + \omega^k\alpha x + \omega^{2k}\alpha^2$, whose roots are $\{\alpha, \omega\alpha, \omega^2\alpha\} \setminus \{\omega^k\alpha\}$. Then the data of a map $\phi_2 : \mathbb{Q}(\alpha, \omega\alpha) \to \mathbb{C}$ extending ϕ_1 is precisely a choice of root belonging to $\{\alpha, \omega\alpha, \omega^2\alpha\} \setminus \{\phi_1(\alpha)\}$ to send $\omega\alpha$ to — there are two such choices.

Now, note that $\mathbb{Q}(\alpha, \omega\alpha) = \Sigma$, as clearly $\mathbb{Q}(\alpha, \omega\alpha) \subseteq \Sigma$, and $\omega = \omega\alpha/\alpha \in \mathbb{Q}(\alpha, \omega\alpha)$, so that $\omega^2\alpha = \omega \cdot \omega\alpha \in \mathbb{Q}(\alpha, \omega\alpha)$. Hence $\phi_2 = \phi$, and $\phi(\omega^2\alpha)$ must be the remaining root of g other than $\phi(\alpha)$ and $\phi(\omega\alpha)$. Moreover, we have

$$\phi(\Sigma) = \phi(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)) = \mathbb{Q}(\phi(\alpha_1), \phi(\alpha_2), \phi(\alpha_3)) = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \Sigma,$$

so we've shown there are $3 \cdot 2 = 6$ ways to construct an embedding $\Sigma \to \mathbb{C}$ over $\mathbb{Q}$, and the image of each of these embeddings is in fact Σ itself. Hence $G := \mathrm{Aut}(\Sigma/\mathbb{Q})$ has size 6, and examnining the possible formulas for $\phi \in G$, we see that $G \cong S_3$, as we've shown for every $\sigma \in S_3$ there exists a unique $\phi \in G$ such that $\phi(\alpha_k) = \alpha_{\sigma(k)}$.

Example 3.71. Consider $g = (x^2-2)(x^2-3) \in \mathbb{Q}$, with roots $\pm\sqrt{2}$ and $\pm\sqrt{3}$. The splitting field is $\Sigma = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. A similar argument to the previous argument yields that an isomorphism $\phi : \Sigma \to \Sigma$ are uniquely determined by a choice of $\phi(\sqrt{2}) \in \{\pm\sqrt{2}\}$ and $\phi(\sqrt{3}) \in \{\pm\sqrt{3}\}$ (since $x^3 - 2$ remains irreducible over $\mathbb{Q}(\sqrt{2})[x]$ as $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$).

It can be seen that $G = \mathrm{Aut}(\Sigma/\mathbb{Q}) \cong C_2 \times C_2$.

Example 3.72. Consider $g = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$. We see $g \in \mathrm{Irred}(\mathbb{Q})$ by the rational root test, and since g is separable (it is irreducible in characteristic zero) it has three distinct roots $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$. Picking a root at random, we get three choices of homomorphisms $\phi : \mathbb{Q}(\alpha_1) \to \mathbb{C}$, determined by $\phi(\alpha_1) \in \{\alpha_1, \alpha_2, \alpha_3\}$.

What may not be obvious is that g already *splits* over $\mathbb{Q}(\alpha_1)$, in fact, it turns out that the roots of this polynomial are

$$\alpha_1 = \zeta + \zeta^{-1}, \qquad \alpha_2 = \zeta^2 + \zeta^{-2}, \qquad \alpha_3 = \zeta^3 + \zeta^{-3},$$

where $\zeta = e^{2\pi i/7}$ (these are actually all real numbers, all you need to check is that $\zeta^7 = 1$ and $\zeta \neq 1$). Using this you can check that: $\alpha_2 = \alpha_1^2 - 2$, $\alpha_3 = \alpha_2^2 - 2$. Thus $\Sigma = \mathbb{Q}(\alpha_1)$ is already a splitting field of g, and a homomorphism $\Sigma \to \Sigma$ is strictly determined by where it sends α_1. Hence $[\Sigma : \mathbb{Q}] = 3$ and $G = \mathrm{Aut}(\Sigma/\mathbb{Q}) \cong C_3$.

Example 3.73. $x^4 - 2 \in \mathbb{Q}[x]$. Here the roots are $\{\pm\alpha, \pm i\alpha\}$, where $\alpha = \sqrt[4]{2}$. In this case, we can show that $[\Sigma : \mathbb{Q}] = 8$ and $G = \mathrm{Aut}(\Sigma/\mathbb{Q}) \cong D_8$. This can be seen using the chain of extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, i), \qquad [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4, \qquad [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2.$$

(Note that $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ so $i \notin \mathbb{Q}(\alpha)$).

Definition 3.74. An algebraic extension L/F is *normal* if every $f \in \mathrm{Irred}(F)$ which has a root in L splits in L.

Example 3.75. $\mathbb{Q}^{\mathrm{alg}}/F$ for any subfield $F \subseteq \mathbb{Q}^{\mathrm{alg}}$ is a normal extension, since it is an algebraic extension and all polynomials over $\mathbb{Q}^{\mathrm{alg}}$ (and hence over F) split in $\mathbb{Q}^{\mathrm{alg}}$.

Example 3.76. Every degree 2 extension is normal.

Proof. Let L/F be normal with $[L : F] = 2$, and choose $f \in \mathrm{Irred}(F)$ and suppose f has a root $\alpha \in L$. If $\alpha \in F$ then since f is irreducible and monic over F we must have $f = x - \alpha$, so f splits over F (and therefore L) as desired. If $\alpha \in L \setminus F$, then by a degree argument we must have that $L = F(\alpha)$.[2] Then since f is the minimal polynomial of α, we have $L = F(\alpha) \cong F[x]/(f)$ has degree 2 over F, so $\deg f = 2$. Then by the division algorithm, since $\alpha \in L$ is a root of f, f factors as $f = (x - \alpha)g$ for some $g \in L[x]$. But since $\deg f = 2$, we must have $\deg g = 1$, so f splits as desired. □

Example 3.77. $\mathbb{Q}(\sqrt[3]{2}/\mathbb{Q}$ is not normal, since $f = x^3 - 2$ does not split over $\mathbb{Q}$.

Theorem 3.78. *A finite extension L/F is normal iff it is a splitting field for some polynomial $f \in F[x]$.*

Proof part 1: Finite normal extensions are splitting fields: If L/F is a finite normal extension then

$$L = F(\alpha_1, \dots, \alpha_n)$$

for some finite list of elements $\alpha_1, \dots, \alpha_n$ with minimal polynomials $m_1, \dots, m_n \in F[x]$. Let $f = \prod_{k=1}^n m_k \in F[x]$ be their product. Normality of L/F says that each m_k splits over L, and thus f does as well. Since L/F is generated by the α_k's, it is clear that L is a splitting field of f. □

We get the second part as a special case of a more general claim.

Lemma 3.79. *Suppose $F \subseteq L \subseteq M$, where L is a slitting field of some $f \in F[x]$. If $\alpha, \beta \in M$ are roots of the same irreducible polynomial $g \in \mathrm{Irred}(F)$, then $[L(\alpha) : L] = [L(\beta) : L]$.*

Proof. By the tower rule,

$$[L(\alpha) : L] = \frac{[L(\alpha) : F]}{[L : F]} = \frac{[L(\alpha) : F(\alpha)][F(\alpha) : F]}{[L : F]}$$

Thus it suffices to show that $[L(\alpha) : F(\alpha)] = [L(\beta) : F(\beta)]$ and $[F(\alpha) : F] = [F(\beta) : F]$.

[2] We have $[F(\alpha) : F] > 1$ since $F(\alpha) \neq F$, so by the tower rule it follows $2 = [L : F(\alpha)][F(\alpha) : F] > [L : F(\alpha)]$, meaning $[L : F(\alpha)] = 1$, so $L = F(\alpha)$.

To see the latter, note that by an above proposition, since g is the minimal polynomial of α and β, there is an isomorphism of F-extensions $\phi : F(\alpha) \to F(\beta)$ sending $\alpha \mapsto \beta$ (both are isomorphic to $F[x]/(g)$), so it is true that $[F(\alpha) : F] = [F(\beta) : F]$.

To see the former, note that $\phi(f) = f$, since $f \in F[x]$. Moreover, both $L(\alpha)/F(\alpha)$ and $L(\beta)/F(\beta)$, being generated over the ground fields by roots of f, are splitting fields of f. Thus by previous theory ϕ extends to an isomorphism $L(\alpha) \to L(\beta)$, so that $[L(\alpha) : F(\alpha)] = [L(\beta) : F(\beta)]$, as desired. □

Proof of part 2: splitting fields are normal extensions. Suppose L/F is a splitting field of $f \in F[x]$, and $g \in \operatorname{Irred}(F)$ is some irreducible polynomial with root $\alpha \in L$. Form a splitting field Σ/L of the polynomial $g \in F[x] \subseteq L[x]$. If β is any root of g in Σ, the previous lemma says

$$[L(\alpha) : L] = [L(\beta) : L].$$

But $\alpha \in L$ so these are 1, so $\beta \in L$. Thus all roots of g are in L, so g splits over L as desired. □

Corollary 3.80. *A splitting field Σ/F is a splitting field for* any $f \in \operatorname{Irred}(F)$ *which has a root in Σ.*

We can generalize this to infinite extensions.

Theorem 3.81. *An algebraic extension L/F is normal iff it is a splitting field for a set $S \subseteq F[x] \setminus \{0\}$ of polynomials.*

Proof. $\Longrightarrow$ Let S be the set of minimal polynomials of all elements in L/F, then $L = F(S)$ and every $m \in S$ splits over L since the extension is normal.

$\Longleftarrow$ Suppose L/F is a splitting field of a set of polynomials $S \subseteq F[x] \setminus \{0\}$, so L is generated over F by the roots of all $f \in L$. Given $\alpha \in L$ and $g \in \operatorname{Irred}(F)$ with $g(\alpha) = 0$, we see that α must be contained in a subfield generated by a finite set of roots, so $\alpha \in F(R_f) \subseteq L$, where $f = f_1 \cdots f_k$ for some finite list $f_1, \dots, f_k \in S$. Since $F(R_f)/F$ is a splitting field of f, it is normal so g splits over $F(R_f)$, and hence over L. □

Proposition 3.82. *Consider fields $F \subseteq K \subseteq L$. If L/F is normal then L/K is normal.*

Proof. First note that if L/F is algebraic then so is L/K. Now suppose $f \in \operatorname{Irred} F$ with a root $\alpha \in L$. Then since K/F is algebraic there is a minimal polynomial $g = m_{\alpha/F} \in F[x]$ of α over F. Since g has α as a root, over K we must have $f \mid g$. Since L/F is normal we have that g splits over Σ, and therefore its factor f splits over Σ. □

Remark 3.83. It is *not* true that L/F being normal implies K/F is normal. For instance, $F = \mathbb{Q}$, $K = \mathbb{Q}(\alpha)$, $L = \mathbb{Q}(\alpha, \omega)$ with $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$.

Remark 3.84. It is not true that L/K and K/F normal imply L/F is normal For instance, $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, and $L = \mathbb{Q}(\sqrt[4]{2})$. Both L/K and K/F are degree 2 and hence normal, but L/F is not normal since the minimal polynomial $x^4 - 2$ of $\sqrt[4]{2}$ does not split over $L \subseteq \mathbb{R}$.

4. Exercises

Lemma 4.1. *Let G be a p-group for some prime p. Then p divides $|Z(G)|$, and in particular $Z(G)$ is nontrivial.*

Proof. Since G is a p-group, we may write $|G| = p^a$ for some $a \in \mathbb{N}$, i.e., $a \geq 1$. Then by the class equation, we have that

$$|G| = |Z(G)| + \sum_{j=1}^{r} [G : C_G(g_j)],$$

where $g_1, \ldots, g_r$ are representatives of the conjugacy classes of G, and each $[G : C_G(g_j)]$ is > 1 and divides $|G|$, say $[G : C_G(g_j)] = p^{m_j}$, where $1 < m_j$. Thus, we have

$$p^a = |Z(G)| + \sum_{j=1}^{r} p^{m_j} \implies |Z(G)| = p^a - \sum_{j=1}^{r} p^{m_j},$$

and the RHS is clearly divisible by p, so that p divides $|Z(G)|$ as well, yielding the desired result. ☐

Lemma 4.2. *Let $p_1, \ldots, p_r$ be distinct primes, and $m_1, \ldots, m_r$ be positive integers. Set $m := p_1^{m_1} \cdots p_r^{m_r}$. Then*

$$\mathbb{Z}/m \cong \bigoplus_{j=1}^{r} \mathbb{Z}/p_j^{m_j}.$$

Proof. Let

$$G := \bigoplus_{j=1}^{r} \mathbb{Z}/p_j^{m_j},$$

and for $j = 1, \ldots, r$, let $a_j \in G$ be a generator of the j^{th} summand, so that $|a_j| = p_j^{m_j}$. Let $x := a_1 \cdots a_r$, so that

$$|x| = \operatorname{lcm}(a_1, \ldots, a_r) = \operatorname{lcm}(p_1^{m_1}, \ldots, p_r^{m_r}).$$

Since each of the p_j's are distinct primes, it follows that $|x| = p_1^{m_1} \cdots p_r^{m_r} = m$. Thus G has an element of order $m = |G|$, so G is cyclic of order m, as desired. ☐

Lemma 4.3. *Let G be a finite group acting on a finite set X, and suppose $x, y \in X$. Then $|\operatorname{Orb}(x)| = |\operatorname{Orb}(y)| \iff |\operatorname{Stab}(x)| = |\operatorname{Stab}(y)|$.*

Proof. If $|\operatorname{Orb}(x)| = |\operatorname{Orb}(y)|$, then by the Orbit/Stabilizer Theorem we have

$$|\operatorname{Stab}(x)| = |G|[G : \operatorname{Stab}(x)] = |G||\operatorname{Orb}(x)| = |G||\operatorname{Orb}(y)| = |G|[G : \operatorname{Stab}(y)] = |\operatorname{Stab}(y)|.$$

On the other hand, if $|\operatorname{Stab}(x)| = |\operatorname{Stab}(y)|$, we have

$$|\operatorname{Orb}(x)| = [G : \operatorname{Stab}(x)] = |G|/|\operatorname{Stab}(x)| = |G|/|\operatorname{Stab}(y)| = [G : \operatorname{Stab}(y)] = |\operatorname{Orb}(y)|.$$ ☐

Lemma 4.4 (Burnside's Lemma)**.** *Let G be a finite group acting on a finite set X. Then*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

where X/G denotes the collection of G-orbits in X, and given $g \in G$, $X^g := \{x \in X \mid g \cdot x = x\}$.

Proof. First of all, note that

$$\sum_{g \in G} |X^g| = |\{(g, x) \in G \times X \mid g \cdot x = x\}| = \sum_{x \in X} |\operatorname{Stab}(x)|,$$

By the Orbit/Stabilizer theorem, we have $|\operatorname{Stab}(x)| = |G|/|\operatorname{Orb}(x)|$, so that

$$\frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{|G|} \sum_{x \in X} \frac{|G|}{|\operatorname{Orb}(x)|} = \sum_{x \in X} \frac{1}{|\operatorname{Orb}(x)|}.$$

Finally, writing X as the disjoint union of its orbits in X/G, we have

$$\frac{1}{|G|} \sum_{g \in G} |X^g| = \sum_{A \in X/G} \sum_{x \in A} \frac{1}{|A|} = \sum_{A \in X/G} 1 = |X/G|.$$ ☐

Lemma 4.5. *let P and Q be finite groups of coprime order. Then* $\operatorname{Aut}(P \times Q) \cong \operatorname{Aut}(P) \times \operatorname{Aut}(Q)$.

Proof. There is a canonical map

$$\mathrm{Aut}(P) \times \mathrm{Aut}(Q) \to \mathrm{Aut}(P \times Q)$$

sending a pair (σ, τ) to the automorphism $\sigma \times \tau$ defined by $(\sigma \times)\tau(p, q) = (\sigma(p), \tau(q))$. It is straightforward to verify that $\sigma \times \tau$ is an automorphism of $P \times Q$ and that this assignment is an injective homomorphism. It remains to show the assignment is surjective.

Now, let $x \in P$, and write $\eta(x, e) = (p, q)$, where $p \in P$ and $q \in Q$. Then since η is a homomorphism, we have

$$(e, e) = \eta(e, e) = \eta((x, e)^{|x|}) = (p^{|x|}, q^{|x|}),$$

so that $q^{|x|} = e$. Thus $|q|$ divides $|x|$, say $|x| = n|q|$. By Lagrange's, $|x| = n|q|$ divides $|P|$ and $|q|$ divides $|Q|$, so $|q|$ is a common factor of $|P|$ and $|Q|$. Yet $|P|$ and $|Q|$ are coprime, so it follows that $|q| = 1$, which means $q = e$. Thus we've shown that $\eta(P \times \{e\}) \subseteq P \times \{e\}$. A similar argument yields that $\eta(\{e\} \times Q) \subseteq \{e\} \times Q$. Now let σ and τ denote the compositions which fit into the following diagram

$$\begin{tikzcd}
P \arrow[r, hook] \arrow[d, dashed, "\sigma"'] & P \times Q \arrow[d, "\eta"'] & Q \arrow[l, hook'] \arrow[d, dashed, "\tau"] \\
P & P \times Q \arrow[l, two heads] \arrow[r, two heads] & Q
\end{tikzcd}$$

where the top arrows denote the identifications $P \cong P \times \{e\}$ and $Q \cong \{e\} \times Q$. Then given $p \in P$ and $q \in Q$, it follows that

$$\eta(p, q) = \eta(p, e)\eta(e, q) = (\sigma(p), e)(e, \tau(q)) = (\sigma(p), \tau(q)),$$

where the middle equality is where we used the fact that $\eta(P \times \{e\}) \subseteq P \times \{e\}$ and $\eta(\{e\} \times Q) \subseteq \{e\} \times Q$. Thus we've shown that $\eta = \sigma \times \tau$. It is straightforward to see that η is not injective (resp. surjective) unless σ and τ are, so we have shown the desired result. $\square$

Lemma 4.6. *Suppose G and H are finite groups and p a prime dividing $|G|$ but not $|H|$. Then there is a bijection*

$$\mathrm{Syl}_p(G) \xrightarrow{\sim} \mathrm{Syl}_p(G \times H) \qquad \textit{given by} \qquad K \mapsto K \times \{e\}.$$

In particular $n_p(G) = n_p(G \times H)$.

Proof. Let $K \in \mathrm{Syl}_p(G)$, and identify K with $K \times \{e\} \leq G \times H$. Since p does not divide $|H|$, K is also a p-Sylow subgroup of $G \times H$. Thus by Sylow 2, every p-Sylow subgroup of $G \times H$ is conjugate to K. Clearly any conjugate of $K \times \{e\}$ by an element of $G \times H$ lands in $G \times \{e\}$, so every element of $\mathrm{Syl}_p(G \times H)$ is of the form $L \times \{e\}$ for a unique $L \in \mathrm{Syl}_p(G)$, as desired. $\square$

Lemma 4.7. *Suppose G is a finite group, p is a prime number, and n is a positive integer. Then there is a bijection*

$$\mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G \times \mathbb{Z}/p^n) \qquad \textit{given by} \qquad K \mapsto K \times \mathbb{Z}/p^n.$$

In particular $n_p(G) = n_p(G \times \mathbb{Z}/p^n)$.

Proof. Clearly if K is a p-Sylow subgroup of G then $K \times \mathbb{Z}/p^n$ is a p-Sylow subgroup of $H := G \times \mathbb{Z}/p^n$. Thus by Sylow 2 every p-Sylow subgroup of H is a conjugate of $K \times \mathbb{Z}/p^n$, and clearly any conjugate of $K \times \mathbb{Z}/p^n$ is of the form $L \times \mathbb{Z}/p^n$ for some subgroup $L \leq G$ satisfying $|L| = |K|$ (since conjugating $A \times B$ by (a, b) is the same as first conjugating A by a and B by b and then taking their product). $\square$

Lemma 4.8. *The multiplicative group of units $(\mathbb{Z}/p^k)^\times$ is cyclic. Moreover, if $k \geq 2$, given a generator n of $(\mathbb{Z}/p^{k-1})^\times$, there exists some $m \in \mathbb{Z}^{\geq 0}$ such that $n + p^{k-1}m$ is a generator of $(\mathbb{Z}/p^k)^\times$.*

Proof. This result is outside the scope of a standard algebra class, and requires Hensel's lemma. However, if you are asked to prove that $(\mathbb{Z}/p^k)^\times$ is cyclic for some specific prime p and integer $k \geq 2$, it can be useful to know the statement. □

Lemma 4.9. *Let G be a finite group such that $n_p(G) = 1$ for each prime p dividing $|G|$. Then G is isomorphic to a product of its Sylow subgroups, i.e., G is a product of p-groups.*

Proof. Write $|G| = p_1^{n_1} \cdots p_k^{n_k}$ (where the p_i's are distinct primes and the n_i's are positive integers), so that for $i = 1, \ldots, k$ G admits a unique subgroup H_i of order $p_i^{n_i}$ (which is normal by Sylow 2). Then we wish to show that

$$G \cong H_1 \times \cdots \times H_k. \tag{1}$$

For $i = 1, \ldots, k$, define

$$K_i := H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_k,$$

i.e. K_i is the product of all the H_j's for $j \neq i$. Then since each H_i is normal, in order for Equation 1 to hold, by the product recognition theorem it suffices to show that

- $H := H_1 H_2 \cdots H_k = G$, and
- $H_i \cap K_i = \{e\}$ for $i = 1, \ldots, k$.

To see the former, note that by the second isomorphism theorem H_i is a subgroup of H for each i, so that in particular $|H_i| = p_i^{n_i}$ divides $|H|$ for each i. Since the p_i's are distinct primes, it follows that $|H| = p_1^{n_1} \cdots p_k^{n_k} = |G|$, so that $H = G$, as desired.

Now, fix some $i \in \{1, \ldots, k\}$, and note that $H_i \cap K_i$ is a subgroup of both H_i and K_i, so by Lagrange's the order of $H_i \cap K_i$ divides both $|H_i|$ and $|K_i|$. Note that

$$|K_i| \leq \prod_{\substack{j=1,\ldots,k \\ j \neq i}} |H_j| = \prod_{\substack{j=1,\ldots,k \\ j \neq i}} p_j^{n_j},$$

but also for $i \neq j$, H_j is a subgroup of K_i, so that $|H_j| = p_j^{n_j}$ must divide the order of K_i. Again since the p_j's are distinct primes, it follows that

$$|K_i| \geq \prod_{\substack{j=1,\ldots,k \\ j \neq i}} p_j^{n_j},$$

so $|K_i| = \prod_{\substack{j=1,\ldots,k \\ j \neq i}} p_j^{n_j}$. Thus since $|H_i \cap K_i|$ has to divide both $\prod_{\substack{j=1,\ldots,k \\ j \neq i}} p_j^{n_j}$ and $p_i^{n_i}$, which have no common factors, it follows that $|H_i \cap K_i| = 1$, so that $H_i \cap K_i = \{e\}$, as desired. □

1. (May 2022 Q1)
   (a) Let H be a subgroup of a group G. Then G acts on the set $G/H = \{gH \mid g \in G\}$ by left multiplication. This action naturally determines a homomorphism $\alpha : G \to S(G/H)$, where $S(X)$ is the group of permutations on a set X. Prove that the kernel of α is contained in H.

   Proof. If $H = G$ we are done, so suppose H is a proper subgroup of G. Then it suffices to show that if $x \in G \setminus H$, then $x \notin \ker \alpha$. This is clear, as if $x \notin H$, then $xH \neq H$, so that in particular $\alpha(x)(eH) = xH \neq eH$, meaning $\alpha(x)$ is not trivial, so $x \notin \ker \alpha$. □

   (b) Let L be a subgroup of a finite group K such that $[K : L] = p$, where p is the smallest prime that divides the order $|K|$ of K. Prove that L is normal in K. Hint: Use part (a).

   Proof. This is Proposition 1.39. □

(c) Describe all finite groups of order p^2, where p is a prime, up to isomorphism. Prove your answer.

We claim that there are two finite groups of order p^2: $\mathbb{Z}/p^2$ and $\mathbb{Z}/p \oplus \mathbb{Z}/p$.

Proof. Since $|G| = p^2$, $|G|$ is abelian (Corollary 1.53). Now, by the classification theorem for f.g. abelian groups, we can write

$$G \cong \bigoplus_{i=1}^{r} \mathbb{Z}/p_i^{m_i}$$

for some unique collection of primes $p_1, \ldots, p_r$ (not necessarily distinct) and positive integers $m_1, \ldots, m_r$. Given any such decomposition, we must have $p_1^{m_1} \cdots p_r^{m_r} = |G| = p^2$. Then the desired result follows. □

(d) Describe all finite groups of order $425 = 25 \cdot 17$ up to isomorphism. Prove your answer.

There are two:

$$\mathbb{Z}/17 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/5 \qquad \text{and} \qquad \mathbb{Z}/17 \oplus \mathbb{Z}/25.$$

Proof. Let G be a group of order 425. By the third Sylow theorem, $n_{17} \mid 25$ and $n_{17} \equiv 1 \bmod 17$, so $n_{17} \in \{1, 5, 25\} \cap \{1, 18, 35, \ldots\} = \{1\}$. Similarly, $n_5 \mid 17$ and $n_5 \equiv 1 \bmod 5$, so that $n_5 \in \{1, 17\} \cap \{1, 6, 11, 16, 21, \ldots\} = \{1\}$. Thus G contains precisely one subgroup P of order 17 and one subgroup Q of order 25, and they are both normal by the second Sylow theorem. Moreover, $P \cap Q$ is a subgroup of both P and Q, and $|P \cap Q|$ must divide both 17 and 25, which are coprime, so we must have $|P \cap Q| = 1$, meaning $P \cap Q = \{e\}$. Finally, we have that PQ is a subgroup of G (since Q is normal) by the second isomorphism theorem, and P and Q are both subgroups of PQ, so that 17 and 25 must both divide the order of PQ. Moreover, since $PQ \subseteq G$, we have $|PQ| \leq |G| = 25 \cdot 17$. It follows that $PQ = G$. Thus since P, Q are normal, $P \cap Q = \{e\}$, and $PQ = G$, we have that $G = P \times Q$, by the product recognition theorem (Proposition 1.79).

Now, since $|P| = 17$ is prime, P is cyclic of order 17. Moreover, since $|Q| = 25 = 5^2$, we showed above that either $Q = \mathbb{Z}/5 \oplus \mathbb{Z}/5$ or $Q = \mathbb{Z}/25$. Thus we are done. □

2. (May 2022 Q4)

(a) Let G be a finite subgroup of the multiplicative group K^* of a field K. Prove that G is cyclic.

Proof. First of all, we claim that each Sylow subgroup of G is cyclic. To that end, let P be a p-Sylow subgroup of G (where p is some prime dividing the order of G), and let $a \in P$ have maximal order, say $|a| = m$, so $m = p^n$ for some positive integer n. Then $\{1, a, a^2, \ldots, a^{m-1}\}$ are m distinct roots of the polynomial $f := x^m - 1 \in K[x]$, which is of degree m, so they are the only roots of f. Now, let $b \in P$. Then since P is a p-group, b has order p^k for some $k \in \mathbb{Z}_{\geq 0}$. Moreover, by assumption $k \leq n$, so that $b^m = b^{p^n} = (b^{p^k})^{p^{n-k}} = 1$. Thus b is a root of f, meaning $b \in \{1, a, a^2, \ldots, a^{m-1}\}$. Our choice of $b \in P$ was arbitrary, and we showed $b \in \langle a \rangle$, so $P = \langle a \rangle$, as desired.

Now, since G is a finite abelian group, it can be written as a product of its Sylow subgroups, each of which we've shown is cyclic. Thus, G can be written as

$$G = \bigoplus_{i=1}^{r} \mathbb{Z}/p_i^{m_i},$$

where each of the p_i's are distinct primes (since G is abelian, given a fixed prime p dividing G, each p-Sylow subgroup of G is normal, so by the second Sylow theorem $n_p = 1$), so by Lemma 4.2, G is cyclic, as desired. $\square$

(b) Let $k = \mathbb{Z}/p\mathbb{Z}$ be the finite field of order p, p a prime. Let K/k be a finite field extension of degree m. Prove that the elements of K are the roots of the polynomial $X^{p^m} - X$ over k.

Proof. TODO. $\square$

(c) Prove that every irreducible polynomial $f(x) \in k[x]$ is separable.

Proof. TODO. $\square$

3. (August 2021 Q1) Let G be a non-trivial finite group acting on a finite set X. We assume that for all $g \in G \setminus \{e\}$ there exists a unique $x \in X$ such that $g \cdot x = x$.

(a) Let $Y = \{x \in X \mid G_x \neq \{e\}\}$, where G_x denotes the stabilizer of x. Show that Y is stable under the action of G.

Proof. Let $y \in Y$ and $g \in G$. Then by Lemma 4.3, since $\operatorname{Orb}(g \cdot y) = \operatorname{Orb}(y)$ (by definition), it follows that $|\operatorname{Stab}(g \cdot y)| = |\operatorname{Stab}(y)| \geq 2$, so that $g \cdot y$ has a nontrivial stabilizer, as desired. $\square$

(b) Let $y_1, y_2, \ldots, y_n$ be a set of orbit representatives of Y/G (with $|Y/G| = n$), and let $m_i = |G_{y_i}|$. Show that

$$1 - \frac{1}{|G|} = \sum_{i=1}^{n} \left(1 - \frac{1}{m_i}\right).$$

Proof. Note that $|G|/m_i = |\operatorname{Orb}(y_i)|$ by the Orbit/Stabilizer theorem. Thus

$$|G| \sum_{i=1}^{n} \left(1 - \frac{1}{m_i}\right) = n|G| - \sum_{i=1}^{n} \frac{|G|}{m_i} = n|G| - \sum_{i=1}^{n} |\operatorname{Orb}(y_i)| = n|G| - |Y|.$$

Thus, it suffices to show that

$$|G| - 1 = n|G| - |Y|.$$

This follows by Burnside's Lemma (Lemma 4.4), as

$$\begin{aligned}
n|G| - |Y| &= |Y/G||G| - |Y| \\
&= \sum_{g \in G} |Y^g| - |Y| && (Y^g := \{y \in Y \mid g \cdot y = y\}) \\
&= |Y^e| + \sum_{g \in G \setminus \{e\}} |Y^g| - |Y| \\
&\overset{(*)}{=} |Y| + |G \setminus \{e\}| - |Y| \\
&= |G| - 1,
\end{aligned}$$

where $(*)$ denotes where we used the assumption that $|Y^g| = 1$ for all $g \in G \setminus \{e\}$. $\square$

(c) Show that X has (at least) a fixed point under the action of G.

Proof. By part (ii), we have

$$|G| - 1 = n|G| - |Y|$$

which yields

$$|Y| = (n-1)|G| + 1. \tag{2}$$

We claim that Y has at least $n-1$ orbits of size $|G|$. Assuming this were true, since Y has n orbits and $|Y| = (n-1)|G| + 1$, it would follow that the remaining orbit of Y must have order 1, so that the action of G fixes a point of Y, and therefore a point of X, as desired.

Now, to see the claim, note that the order of each orbit of Y divides $|G|$, so if there were two orbits of size $< |G|$, the sum of their orders would be at most $|G|$, which would yield

$$|Y| \leq |G| + (n-2)|G| = (n-1)|G| < (n-1)|G| + 1,$$

a contradiction of Equation 2, as desired. □

4. (January 2021 Q1) Let G be a group of order 2057.
   (a) Snow that $G \simeq P \times Q$, where P is a group of order 17 and Q is a group of order 121. Determine all groups of order 2057 up to isomorphism.

   There are two.

   $$\mathbb{Z}/17 \oplus \mathbb{Z}/121 \qquad \text{and} \qquad \mathbb{Z}/17 \oplus \mathbb{Z}/11 \oplus \mathbb{Z}/11.$$

   Proof. Observe that $2057 = 17 \cdot 121 = 17 \cdot 11^2$, and use the exact same argument given in May 2022, Q1(d). □

   (b) Show that $\mathrm{Aut}(G) \simeq \mathrm{Aut}(P) \times \mathrm{Aut}(Q)$.

   Proof. This is Lemma 4.5. □

   (c) Show that if Q is cyclic, then so is $\mathrm{Aut}(Q)$. What is the order of $\mathrm{Aut}(Q)$ in this case?

   Proof. This is proven in class — if $G \cong \langle a \mid a^n \rangle$, then there is an isomorphism of monoids

   $$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathrm{End}(G) \qquad \text{given by} \qquad [k] \mapsto (a^m \mapsto a^{mk})$$

   (this is easily proven via the universal property of free groups). Thus there is an isomorphism of groups

   $$(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Aut}(G).$$

   We know that $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$, where $\phi(n)$ is the number of positive integers less than or equal to n that are coprime to n.

   It is straightforward to see that $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ if p is prime: given $1 \leq m < p^k$, the only way to have $\gcd(p^k, m) > 1$ is if m is a multiple of p, that is, $m \in \{p, 2p, 3p, \ldots, p^{k-1}p = p^k\}$, and there are p^{k-1} such multiples not greater than p^k. Therefore, the other $p^k - p^{k-1}$ numbers are all relatively prime to p^k. Thus if $Q \cong \mathbb{Z}/121 = \mathbb{Z}/11^2$, we have that $|\mathrm{Aut}(Q)| = |(\mathbb{Z}/11^2)^\times| = 11^2 - 11 = 110$.

   Now, it remains to show that $(\mathbb{Z}/11^2)^\times$ is cyclic. There is an easy way and a hard way to do this. The easy way is to observe that $|(\mathbb{Z}/11^2)^\times| = 110 = 2 \cdot 5 \cdot 11$, so by the classification theorem for finite abelian groups, we must have

   $$(\mathbb{Z}/11^2)^\times \cong \mathbb{Z}/2 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/11,$$

   and 2, 5, and 11 are distinct primes, so $(\mathbb{Z}/11^2)^\times$ is cyclic.

   The hard way is to find an element of $(\mathbb{Z}/11^2)^\times$ of order 110. By Lemma 4.8 it suffices to first find a generator n of $(\mathbb{Z}/11)^\times$, in which case there is guaranteed to exist some $m \geq 0$ such that $n + 11m$ is a generator of $(\mathbb{Z}/11^2)^\times$. This requires one to guess and check via some arduous arithmetic. There are some tricks one can do to make it manageable, however.

First of all, we'll take $n = 2$, since $\gcd(2, 11) = 1$, so that 2 generates $(\mathbb{Z}/11)^\times$. Now the aforementioned lemma guarantees the existince of some $m \geq 0$ such that $2 + 11m$ generates $(\mathbb{Z}/11^2)^\times$. We'll start by checking $m = 0$. So we need to check that 2 has multiplicative order 110 in $\mathbb{Z}/11^2$. Since $110 = 2 \cdot 5 \cdot 11$, it suffices to check that $2^k \not\equiv 1 \bmod 11^2$ for $k = 2 \cdot 5 = 10$, $k = 2 \cdot 11 = 22$, or $k = 5 \cdot 11 = 55$. This requires a string of computations by hand:

- $2^{10} = 1024 \equiv 56 \bmod 121$.
- $2^{22} = (2^{10})^2 \cdot 2^2 \equiv (56)^2 \cdot 4 \bmod 121$.
- $(56)^2 = 3136 \equiv 111 \bmod 121$.
- $2^{22} \equiv 111 \cdot 4 = 444 \equiv 81 \bmod 121$.
- $2^{55} = (2^{10})^5 \cdot 2^5 \equiv (56)^5 \cdot 32 \equiv (111)^2 \cdot 56 \cdot 32 \bmod 121$
- $(111)^2 = 12321 \equiv 100 \bmod 121$.
- $56 \cdot 32 = 1792 \equiv 98 \bmod 121$.
- $2^{55} \equiv 100 \cdot 98 = 9800 \equiv 120 \bmod 121$.

Thus, we will have shown that 2, as an element of $(\mathbb{Z}/11^2)^\times$, has order 110, so that $(\mathbb{Z}/11^2)^\times$ is cyclic, as desired. □

(d) If Q is not cyclic, find an isomorphic description of $\mathrm{Aut}(Q)$ and compute its order.

Proof. If Q is not cyclic, then $Q \cong \mathbb{Z}/11 \oplus \mathbb{Z}/11 = \mathbb{F}_{11}^2$, so that $\mathrm{Aut}(Q) = \mathrm{GL}_2(\mathbb{F}_{11})$. The group $\mathrm{GL}_n(\mathbb{F}_p)$ has order $(p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$. (The first row u_1 of the matrix can be anything but the 0-vector, so there are $p^n - 1$ possibilites for the first row. The second row can be anything but a multiple of the first row, giving $p^n - p$ possibilites. For any choice u_1, u_2 of the first rows, the third row can be anything but a linear combination of u_1 and u_2. The number of linear combinations $a_1u_1 + a_2u_2$ is just the number of choices for the pair (a_1, a_2), and there are p^2 of these. It follows that there are $p^n - p^2$ for the third row. And so on.) Thus $\mathrm{Aut}(Q)$ has order $(11^2 - 1)(11^2 - 11) = 120 \cdot 110 = 13200$. □

5. (August 2020 Q1)

(a) A finite group G is called *cool* if G has precisely four Sylow subgroups (over all primes p). The order $|G|$ of a cool group is called a *cool* number. For example, S_3 is a cool group and 6 is a cool number. Describe the set of all cool numbers. Hint: Use prime factorization in your description.

We claim there are two types of cool numbers:

- **Type I.** Numbers of the form $p^n q^m r^k s^\ell$, where p, q, r, s are distinct prime numbers, and n, m, k, ℓ are positive integers. I.e., numbers with exactly four distinct prime factors.
- **Type II.** Numbers of the form $2^n 3^m$, where n and m are any positive integers.

Proof. To start, we will show any Type I or II number is cool. First, let p, q, r, s be distinct prime numbers, and n, m, k, ℓ be positive integers, and consider the group

$$G = \mathbb{Z}/p^n \oplus \mathbb{Z}/q^m \oplus \mathbb{Z}/r^k \oplus \mathbb{Z}/s^\ell.$$

Because G is abelian, every subgroup of G is normal. Thus we have $n_p = n_q = n_r = n_s = 1$ by the second Sylow theorem, so that G has 4 Sylow subgroups as desired.

Now, let n and m be positive integers and consider the group

$$G = S_3 \times \mathbb{Z}/2^{n-1} \times \mathbb{Z}/3^{m-1}.$$

Clearly $|G| = 6 \cdot 2^{n-1} \cdot 3^{m-1} = 2^n 3^m$. Now we claim that $n_2(G) = 3$ and $n_3(G) = 1$. To see this, note first that $n_3(S_3) = 1$ and $n_2(S_3) = 3$. Then $n_3(S_3 \times \mathbb{Z}/2^{n-1}) = 1$ by Lemma 4.6, since 3 does not divide $|\mathbb{Z}/2^{n-1}|$, and $n_2(S_3 \times \mathbb{Z}/2^{n-1}) = n_2(S_3) = 3$, by Lemma 4.7. A simular argument yields that $n_3(G) = 1$ and $n_2(G) = 3$, as desired.

Now, let G be a group. Then we claim that in order for G to be cool, its order must be Type I or II as defined above. If $|G|$ has more than four distinct prime factors, then G has more than four Sylow subgroups by Sylow 1, so G isn't cool. We showed above that any number with precisely four distinct prime factors is cool. Clearly the trivial group is not cool. Thus, it suffices to consider the cases that $|G|$ has one, two, or three prime factors. In what follows, let p, q, and r be distinct primes, and let n, m, and k be positive integers.

Case 1. $|G| = p^n$. By the third Sylow theorem, we have $n_p \mid 1$, which implies $n_p = 1 \neq 4$, so no p-group is cool.

Case 2. $|G| = p^n q^m$. In order for G to be cool, we must have $n_p + n_q = 4$, so suppose this holds. Then we claim $\{p, q\} = \{2, 3\}$. If $n_p = n_q = 2$, then by Sylow 3 we'd have $n_p = 2 \equiv 1 \bmod p$, i.e., $1 \equiv 0 \bmod p$, but 1 is not a multiple of any prime, so we can't have $n_p = n_q = 2$.

Now, suppose $\{n_p, n_q\} = \{1, 3\}$, say WLOG $n_p = 3$ and $n_q = 1$. Then by Sylow 3, we have $n_p = 3 \equiv 1 \bmod p$, i.e., $2 \equiv 0 \bmod p$, which is only possible if $p = 2$. We'd also have $n_p = 3 \mid q^m$, which is only possible if $q = 3$. Hence $|G| = 2^n 3^m$, so $|G|$ is Type II, as desired.

Case 3. $|G| = p^n q^m r^\ell$. Again, if G is cool, then we can assume WLOG that $n_p = 2$ and $n_q = n_r = 1$. Then by Sylow 3, $n_p = 2 \equiv 1 \bmod p$, i.e., $1 \equiv 0 \bmod p$, an impossibility since $p \neq 1$. Thus if G has 3 prime factors then it is lame. □

(b) For each cool number n that you found in part (a), determine whether every group of order n is nilpotent.

Every Type I cool group is nilpotent, and no Type II cool group is nilpotent.

Proof. Now, let G be a Type I cool group, so that $|G|$ has four distinct prime factors and G has four Sylow subgroups. Then it follows by Lemma 4.9 that G is a product of its Sylow subgroups. Thus G is nilpotent by Theorem 1.109, as desired.

Now, we claim that no Type II cool group is nilpotent. Indeed, we showed above that any Type II cool group satisfies $n_2 = 3$, which means G cannot be nilpotent by Theorem 1.109, as any finite nilpotent group has exactly one p-Sylow subgroup for each prime p dividing its order. □

(c) For each cool number n that you found in part (a), determine whether every cool group of order n is solvable.

Every cool group is solvable.

Proof. Recall every nilpotent group is solvable, so every Type I cool group is solvable. By Burnside's Theorem (proven in Dummit & Foote Section 19.2), every group of order $p^a q^b$ for p and q distinct primes and a and b positive integers is solvable, so Type II cool groups are solvable.

An argument that does not require Burnside's theorem: Let G be a Type II cool group, so that $|G| = 2^n 3^m$ for some positive integers n and m, $n_2(G) = 3$, and $n_3(G) = 1$. Let P be the unique 3-Sylow subgroup of G, which is normal by Sylow 2. Note that G/P has order 2^n, which is a prime power, so G/P is solvable. Moreover P is solvable, because P also has prime power order 3^m. Thus since G/P and P are solvable, G must be solvable as well. □

6. (August 2020 Q2) Suppose a finite group G acts on a set A so that for every nontrivial $g \in G$ there exists a unique fixed point (i.e., there is exactly one $a \in A$, depending on g, such that $g(a) = a$). Prove that this fixed point is the same for all $g \in G$.

   Proof. This is August 2021, Q1(c). □

7. (May 2022 Q2) Make $\mathbb{C}^3$ into a $\mathbb{C}[x]$-module by $f(x)v = f(A)v$, where $v \in \mathbb{C}^3$ and
$$A = \begin{pmatrix} 5 & 3 & 0 \\ 0 & 5 & 0 \\ 0 & 3 & 3 \end{pmatrix}.$$
   Find polynomials $p_i(x)$ and exponents e_i such that $\mathbb{C}^3 \cong \bigoplus_i \mathbb{C}[x]/(p_i^{e_i})$ as $\mathbb{C}[x]$-modules. Justify your answer.

   Proof. We claim that
$$\mathbb{C}^3 \cong \mathbb{C}[x]/((x-5)^2) \oplus \mathbb{C}[x]/(x-3).$$
   Recall that with its $\mathbb{C}[x]$-module structure given by A, $\mathbb{C}^3$ is isomorphic to $\bigoplus_{j=1}^n \mathbb{C}[x]/(f_j)$, where $f_1, f_2, \ldots, f_k$ are invariant factors of the matrix A satisfying:
   - $f_1 \mid f_2 \mid \cdots \mid f_k$,
   - $f_1 f_2 \cdots f_k$ is the characteristic polynomial c_A of A, and
   - $f_k = m_A$ is the minimal polynomial of A.

   We have that the characteristic polynomial of A is given by
$$\det(xI - A) = \det \begin{pmatrix} x-5 & -3 & 0 \\ 0 & x-5 & 0 \\ 0 & -3 & x-3 \end{pmatrix} = (x-5)^2(x-3).$$
   The above conditions give that the minimal polynomial of A is either $(x-5)^2(x-3)$ or $(x-5)(x-3)$ (since the minimal polynomial m_A must divide $c_A = (x-5)(x-3)^2$, and the other invariant factors, which multiply to give c_A/m_A, must each divide m_A). One can directly check that $m_A(x) \neq (x-5)(x-3)$, as
$$(A-5I)(A-3I) = \begin{pmatrix} 0 & 3 & 0 \\ 0 & 0 & 0 \\ 0 & 3 & -2 \end{pmatrix} \begin{pmatrix} 2 & 3 & 0 \\ 0 & 2 & 0 \\ 0 & 3 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 6 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \neq 0,$$
   so the minimal polynomial must be $m_A = (x-5)^2(x-3)$. Thus $m_A = c_A$ is the only invariant factor of A, so that with its $\mathbb{C}[x]$-module structure given by A, we have
$$\mathbb{C}^3 \cong \mathbb{C}[x]/((x-5)^2(x-3)).$$
   Now, note that $x-5$ and $x-3$ are non-associate primes, so that $(x-5)^2$ and $(x-3)$ are coprime. Thus by the Chinese remainder theorem, we further have that
$$\mathbb{C}^3 \cong \mathbb{C}[x]/((x-5)^2) \oplus \mathbb{C}[x]/(x-3),$$
   as desired. □

8. (May 2022 Q3) Completely factor the following polynomials over the given fields (or prove they are irreducible).

   (a) $x^3 + x + 2 \in \mathbb{Z}_3[x]$.

$$f(x) := x^3 + x + 2 \equiv (x^2 + 2x + 2)(x - 2) \bmod 3.$$

Proof. One can check by hand that $f(x) = x^3 + x + 2$ has a root, namely $f(2) = 0$, so $x - 2$ must divide f. Then doing polynomial long division yields

$$(x^2 + 2x + 2)(x - 2) = x^3 + x + 2 \bmod 3.$$

Then one can check $x^2 + 2x + 2$ has no roots in $\mathbb{Z}_3$, and it is quadratic, so it is irreducible. Thus the above is the irreducible factorization of f. ☐

   (b) $x^4 + x^3 + x + 3 \in \mathbb{Z}_5[x]$.

The polynomial is irreducible.

Proof. There might be an easier proof, but this is all I can think of.

Let $f(x) = x^4 + x^3 + x + 3$. One can directly check that $f(j) \not\equiv 0 \bmod 5$ for $j = 0, 1, 2, 3$, so if f factors over $\mathbb{F}_5$, it must do so as a product of quadratics. Suppose it did, so there exists $a, b, c, d \in \mathbb{F}_5$ such that

$$\begin{aligned} x^4 + x^3 + x + 3 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd, \end{aligned}$$

so that

$$a + c = 1, \qquad b + d + ac = 0, \qquad ad + bc = 1, \qquad \text{and} \qquad bd = 3.$$

Substituting $c = 1 - a$ and $d = 3/b$ in the middle two equations yields the system

$$0 = b + \frac{3}{b} + a(1 - a) \qquad \text{and} \qquad 1 = \frac{3a}{b} + b(1 - a).$$

Multiplying the equations by b yields

$$0 = b^2 + 3 + ab - a^2b \qquad \text{and} \qquad 0 = 3a + b^2 - ab^2 - b. \tag{3}$$

Now, it suffices to show that there does not exist any $a, b \in \mathbb{F}_5$ satisfying both of these equations. To show this, we split into cases:

Case 1. If $a = 0$, then the equations become $0 = b^2 + 3$ and $0 = b^2 - b$. Assuming $b^2 - b = 0$, the first equation becomes $b + 3 = 0$, so $b = -3 \equiv 2$. But then we'd have $b^2 - b = 2^2 - 2 = 2 \not\equiv 0 \bmod 5$, a contradiction of the fact that $b^2 - b = 0$ to begin with.

Case 2. If $a = 1$, then the equations become $0 = b^2 + 3 + b - b = b^2 + 3$ and $0 = 3 + b^2 - b^2 - b = 3 - b$. The second equation yields $b = 3$, but then the first equation is unsatisfied, as $b^2 + 3 = 9 + 3 = 12 \not\equiv 0$. Thus it cannot hold that $a = 1$.

Case 3. If $a = 2$, then the equations become $0 = b^2 + 3 + 2b - 4b \equiv b^2 + 3b + 3$ and $0 = 6 + b^2 - 2b^2 - b \equiv -b^2 - b + 1$. The second equation yields $b^2 = 1 - b$, so the first equation the becomes $0 = 1 - b + 3b + 3 = 2b + 4$, so that $b = -2 \equiv 3$. But then the second equation does not hold, as we'd have $-b^2 - b + 1 = -9 - 3 + 1 = -11 \not\equiv 0$.

Case 4. If $a = 3$, then the equations become $0 = b^2 + 3 + 3b - 9b \equiv b^2 - b + 3$ and $0 = 9 + b^2 - 3b^2 - b \equiv 3b^2 - b - 1$. The first equation gives $b^2 = b - 3$, which causes the second equation to become $0 = 3(b-3) - b - 1 \equiv 2b$, so that we must have $b = 0$.

Case 5. Finally if $a = 4$, then the equations become $0 = b^2 + 3 + 4b - 16b \equiv b^2 - 2b - 2$ and $0 = 12 + b^2 - 4b^2 - b \equiv 2b^2 - b + 2$. The first equation yields $b^2 = 2b + 2$, so that the second equation becomes $0 = 2(2b+2) - b + 2 \equiv 3b + 1$, so that $b = 1/3 \equiv 2$. But then the first equation no longer holds, as we'd have $b^2 - 2b - 2 = 4 - 4 - 2 = -2 \not\equiv 0$.

Thus there are no $a, b \in \mathbb{F}_5$ satisfying Equation 3, so it cannot have been true that f factored in the first place. $\square$

(c) $x^4 + x^3 + x^2 + 6x + 1 \in \mathbb{Q}[x]$.

The polynomial is irreducible.

Proof. Since $\mathbb{Z}$ is a UFD (it is in fact a Euclidean domain) with $\operatorname{Frac}\mathbb{Z} = \mathbb{Q}$, in order to show f is irreducible in $\mathbb{Q}[x]$ it suffices to show it is irreducible in $\mathbb{Z}[x]$, as f has coefficients in $\mathbb{Z}$. To that end, one can check via a straightforward computation that

$$f(x+1) = x^4 + 5x^3 + 10x^2 + 15x + 10.$$

It follows by Eisenstein's with $p = 5$ that $f(x+1)$ is irreducible over $\mathbb{Z}$, and thus over $\mathbb{Q}$. Since $f(x) \mapsto f(x+1)$ is a ring automorphism of $\mathbb{Q}[x]$ (with inverse $f(x) \mapsto f(x-1)$), it follows that f is irreducible as well, as desired. $\square$

9. (August 2021 Q2)

(a) Show that $x^6 + 69x^5 - 511x + 363$ is irreducible over the integers.

Proof. This is a hard one. Write f for the polynomial in question. Modulo 3, it's easy to factor, as $f(x) \equiv x^6 - x \bmod 3$. Since both 0 and $1 \equiv -2$ are roots of f in $\mathbb{F}_3$, it follows that $f(x) = x(x+2)g$, where g is a degree 4 polynomial. Performing polynomial long division yields that $g = x^4 + x^3 + x^2 + x + 1$. One can check that g has no roots in $\mathbb{F}_3$, so if g were to factor it would do so as a product of quadratics, say

$$\begin{aligned} g &= x^4 + x^3 + x^2 + x + 1 \\ &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a+c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd, \end{aligned}$$

so that

$$a + c = 1, \qquad ac + b + d = 1, \qquad ad + bc = 1, \qquad \text{and} \qquad bd = 1.$$

Substituting $d = 1/b$ and $c = 1 - a$ in the middle two equations yields

$$a(1-a) + b + \frac{1}{b} = 1, \qquad \text{and} \qquad \frac{a}{b} + b(1-a) = 1.$$

Multiplying both equations by b yields

$$ab - a^2b + b^2 + 1 - b = 0 \qquad \text{and} \qquad a + b^2 - ab^2 - b = 0. \tag{4}$$

Thus in order to show g is irreducible, it suffices to show that there does not exist $a, b \in \mathbb{F}_3$ which satisfy Equation 4. To see this, suppose for the sake of a contradiction that there existed $a, b \in \mathbb{F}_3$ such that Equation 4 holds.

Case 1. If $a = 0$, then the equations become $b^2 + 1 - b = 0$ and $b^2 - b = 0$. The second equation yields $b^2 = b$, so the first equation becomes $b + 1 - b = 0$, i.e., $1 = 0$, a contradiction.

Case 2. If $a = 1$, then the equations becomes $0 = b - b + b^2 + 1 - b = b^2 + 1 - b$ and $0 = 1 + b^2 - b^2 - b = 1 - b$. The second equation yields $b = 1$, so then the first equation becomes $0 = b^2 + 1 - b = 1 + 1 - 1 = 1$, a contradiction.

Case 3. If $a = 2$, then the equations become $0 = 2b - 4b^2 + b^2 + 1 - b \equiv b + 1 \pmod 3$ and $0 = 2 + b^2 - 2b^2b - b \equiv 2 - b^2 - b \pmod 3$. The first equation yields that $b = -1$, so the second equation becomes $0 = 2 - b^2 - b = 2 - 1 + 1 = 2$, and $2 \not\equiv 0 \pmod 3$, so we reach a contradiction.

Thus f has an irreducible factorization over $\mathbb{F}_3$ given by

$$f(x) \equiv x(x + 2)(x^4 + x^3 + x^2 + x + 1) \bmod 3.$$

Thus, if f factors over $\mathbb{Z}$, it must factor as a product of irreducible polynomials of degree $1, 1, 4$, or $1, 5$, or $2, 4$ (since any factorization of f over $\mathbb{Z}$ descends to a factorization over $\mathbb{F}_3$).

Now, consider f over $\mathbb{F}_5$. Taken mod 5, f is given by $x^6 - x^5 - x + 3$. One can check directly that f does not have any roots in $\mathbb{F}_5$, so it has no linear factors. Thus f has no linear factors over $\mathbb{Z}$. Now, suppose for the sake of a contradiction that f factors over $\mathbb{Z}$, so by what we've shown it factors as an irreducible quadratic polynomial p times an irreducible quartic polynomial q. Moreover, by what we have shown above, we must futher have

$$p \equiv x(x + 2) = x^2 + 2x \bmod 3.$$

A similar argument to one given above for $\mathbb{F}_3$ yields that f factors irreducibly as

$$f \equiv x(x + 2)(x^4 + x^3 + 9x^2 + 4x + 3) \bmod 11$$

over $\mathbb{F}_{11}$. Thus it follows that

$$p \equiv x^2 + 2x \bmod 11 \qquad \text{and} \qquad q \equiv x^4 + x^3 + 9x^2 + 4x + 3 \bmod 11$$

Now, write a for the constant term of p and b for the constant term of q, so that $ab = 363 = 3 \cdot 11 \cdot 11$. By what we've shown above, we know that 3 and 11 both divide a, and $b \equiv 3 \bmod 11$. Thus $a \in \{\pm 33, \pm 363\}$ and $b \in \{\pm 1, \pm 11\}$. Yet none of 1, -1, 11, or -11 are equivalent to 3 mod 11. Hene we reach a contradiction, f could not have factored in the first place. $\square$

(b) Show that $x^4 + 5x + 1$ is irreducible over the rationals.

Proof. By the rational root test, any rational root of $f(x) := x^4 + 5x + 1$ must divide 1, and it is straightforward to check that 1 and -1 are not roots of f. Hence, if f factored, it would do so as a product of quadratics, say

$$\begin{aligned} f(x) &= x^4 + 5x + 1 \\ &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd, \end{aligned}$$

for some $a, b, c, d \in \mathbb{Q}$, so that

$$0 = a + c, \qquad 0 = ac + b + d, \qquad 5 = ad + bc, \qquad \text{and} \qquad 1 = bd.$$

Substituting $c = -a$ and $d = 1/b$ in the middle two equations further yields

$$0 = -a^2 + b + \frac{1}{b} \qquad \text{and} \qquad 5 = \frac{a}{b} - ab.$$

Multiplying both equations by b yields

$$0 = -a^2b + b^2 + 1 \qquad \text{and} \qquad 0 = a - ab^2 - 5b. \tag{5}$$

Hence it suffices to show that there does not exist $a, b \in \mathbb{Z}$ which satisfy Equation 5. Supposing there did exist such a pair, note that the second equation yields

$$0 = a(1-b^2) - 5b \implies a = \frac{5b}{1-b^2},$$

so that the first equation becomes

$$0 = -\left(\frac{5b}{1-b^2}\right)^2 b + b^2 + 1 = -\frac{25b^3}{b^4 - 2b^2 + 1} + b^2 + 1.$$

Multiplying by $b^4 - 2b^2 + 1$ and simplifying yields

$$0 = b^6 - b^4 - 25b^3 - b^2 + 1.$$

By the rational root test, any rational solution b to this equation must be an integer dividing 1, yet one can directly check that neither 1 nor -1 satisfy the above equation. Thus there does not exist any $a, b \in \mathbb{Q}$ satisfying Equation 5, meaning f is irreducible over $\mathbb{Q}$, as desired. □

(c) Show that $x^4 + x^3 + x^2 + 6x + 1$ is irreducible over the rationals.

Proof. This is May 2022, Q3(c). □

(d) Calculate the number of distinct, irreducible polynomials over $\mathbb{Z}_5$ that have the form

$$f(x) = x^2 + ax + b, \qquad \text{or} \qquad g(x) = x^3 + \alpha x^2 + \beta x + \gamma \qquad a, b, \alpha, \beta, \gamma \in \mathbb{Z}_5.$$

We will prove more generally that in a finite field of order n, there are:

- $\frac{n^2-n}{2}$ monic, irreducible, quadratic polynomials, and
- $\frac{n^3-n}{3}$ monic, irreducible, cubic polynomials.

Proof. Let F be a finite field of order n. First of all, note there are n^2 monic quadratic polynomials, and n^3 monic cubic polynomials.

Now, we'd like to count the number of reducible, monic, and quadratic polynomials in $F[x]$. Given such a polynomial f, in order for it to factor, it must factor as a product of monic linear polynomials, say as $f(x) = (x-a)(x-b)$ for some $a, b \in F$. There are $\binom{n}{2}$ such polynomials with a and b distinct, and n such polynomials with $a = b$, giving a total of

$$n^2 - \left(\binom{n}{2} + n\right) = \frac{n^2 - n}{2}$$

irreducible, monic, and quadratic polynomials in $F[x]$.

Now, we wish to count the number of reducible, monic, and cubic polynomials in $F[x]$. Given $f \in F[x]$ monic and cubic, for it to factor it must have a linear factor. It follows there are two distinct types

(a) $f(x) = (x-a)(x-b)(x-c)$ with $a, b, c \in F$, and

(b) $f(x) = (x-a)g(x)$, where $a \in F$ and g is an irreducible, monic, quadratic polynomial.

There are three subcases for a polynomial of type (a), based on how many distinct roots it has. There are n ways to choose a type (a) polynomial when $a = b = c$. There are $\binom{n}{2} \cdot 2$ ways to choose a type (a) polynomial with two distinct roots (first pick the two roots from F, then choose which root to double). Finally, there are $\binom{n}{3}$ ways to choose a type (a) polynomial with 3 distinct roots. Hence, there are

$$n + 2 \cdot \binom{n}{2} + \binom{n}{3}$$

polynomials of type (a). To count the number of type (b) polynomials, observe that there are n ways to choose a root $a \in F$, and we know there are $\frac{n(n-1)}{2}$ irreducible quadratic and monic polynomials over F, so there are

$$n \cdot \frac{n(n-1)}{2} = \frac{n^2(n-1)}{2}$$

polynomials of type (b). Thus there are

$$\begin{aligned} n^3 - \left(n + 2\binom{n}{2} + \binom{n}{3}\right) - \frac{n^2(n-1)}{2} \\ &= n^3 - n - n(n-1) - \frac{n(n-1)(n-2)}{6} - \frac{n^3 - n^2}{2} \\ &= \frac{n^3 - n}{3} \end{aligned}$$

irreducible, monic, and cubic polynomials over F, as desired. ☐

10. (August 2021 Q3) Find [all] possible Jordan canonical forms of an 8×8 matrix M over the field $\mathbb{F}_5$ with five elements if it is known that the characteristic polynomial of M is $(x^2+1)^4$ and the minimal polynomial of M is $(x^2+1)^2(x+2)$.

Solution. First of all, note that $x^2 + 1 \equiv (x+2)(x+3) \bmod 5$, so that the characteristic polynomial of M is given by $c(x) = (x+2)^4(x+3)^4$ and the minimal polynomial is given by $m(x) = (x+2)^3(x+3)^2$. Now, we'd like to find the invariant factors $f_1, f_2, \ldots, f_k \in \mathbb{F}_5[x]$ of M. Recall the following facts about the invariant factors:

- f_j is nonconstant and monic for $j = 1, \ldots, k$.
- $f_j \mid f_{j+1}$ for $1 \leq j < k$.
- $f_k = m$.
- $f_1 \cdots f_k = c$.

Putting these facts together, we have that the following is an exhaustive list of possibilities for the invariant factors of M:

(1) $f_1 = (x+2)(x+3)^2$, $f_2 = m$.

(2) $f_1 = (x+3)$, $f_2 = (x+2)(x+3)$, $f_3 = m$.

Now, in order to find the Jordan canonical form of M, we need to find the elementary divisors of M. These are the prime powers dividing the invariant factors (counted individually, for each invariant factor). Thus, the list of elementary divisors of M are given by either

(1) $(x+2), (x+3)^2, (x+2)^3, (x+3)^2$, or

(2) $(x+3), (x+2), (x+3), (x+2)^3, (x+3)^2$.

Thus, the Jordan canonical form of M is an 8×8 diagonal block matrix, where either:

(1) M has 4 Jordan blocks: a 2-Jordan block of size 1, two 3-Jordan blocks of size 2, and a 2-Jordan block of size 3.

(2) M has 5 Jordan blocks: a 2-Jordan block of size 1, two 3-Jordan blocks of size 1, a 3-Jordan block of size 2, and a 2-Jordan block of size 3.

Recall given some $a \in \mathbb{F}_5$, an a-Jordan block of size k is a $k \times k$ matrix with a's along the diagonal, 1's on the first superdiagonal, and 0's elsewhere. For example, if M is of the first type (i.e., if M has four elementary divisors), then the matrix

$$\left(\begin{array}{c|cc|cc|ccc} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 3 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{array}\right)$$

is a Jordan canonical form for M (the Jordan blocks have been outlined).

11. (January 2021, Q2)

(a) Let R be the ring of 3×3 matrices over $\mathbb{Q}$, and let S denote the ring of 2×2 matrices over $\mathbb{Q}$. Is there a surjective ring homomorphism $\phi : R \to S$? Justify your answer.

No.

Proof. We claim that R has a cube root of 2, but S does not. Supposing this were true, suppose for the sake of a contradiction that there existed a surjective ring map $\phi : R \to S$. Let $A \in R$ such that $A^3 = 2$. Then we'd have

$$\phi(A)^3 = \phi(A^3) = \phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 1 + 1 = 2,$$

a contradiction of the fact that S does not admit a cube root of 2.

Now, it remains to prove the claims. First, to see that R has a cube root of 2, consider the $\mathbb{Q}[x]$-module $M := \mathbb{Q}[x]/(x^3 - 2)$, which has dimension 3 as a $\mathbb{Q}$-vector space ($\{\overline{1}, \overline{x}, \overline{x}^2\}$ is a basis). There is a $\mathbb{Q}$-linear map $M \to M$ given by $Tm := x \cdot m$. Note that $T^3 = 2$, as given $m \in M$, we have $T^3(m) = \overline{x}^3 m = 2m$. Hence T is an endomorphism of a 3-dimensional $\mathbb{Q}$-vector space which satisfies $T^3 = 2I$. Then fixing a basis for M yields a matrix A satisfying $A^3 = 2I$, as desired.

To see that S does not have a cube root of 2, suppose for the sake of a contradiction that it did, so there exists some $A \in S$ with $A^3 = 2I$. Let $f(x) := x^3 - 2$, and define $m(x)$ to be the minimal polynomial of A, which is of degree at most 2 because A is a 2×2 matrix (by Cayley-Hamilton). We know that $m(A) = f(A) = 0$, so that m divides f. Since $\deg m < \deg f$, it follows that f is reducible. But this is absurd: by the rational root test any rational root of f has to divide 2, and one can easily check that $\pm 1, \pm 2$ are not roots of f, so that f is irreducible because it is a cubic with no roots. Thus we obtain a contradiction, S could not have had a cube root of 2 in the first place. ∎

(b) Compute $\gcd(17 + i, 24 + 2i)$ in the ring $\mathbb{Z}[i]$.

Solution. Recall $\mathbb{Z}[i]$ is a Euclidean domain with norm function given by $N(\alpha) := |\alpha|^2 = \Re\alpha^2 + \Im\alpha^2$. Thus we may apply the Euclidean algorithm (Proposition 2.17) in order to compute the gcd. Set $r_{-2} = 24 + 2i$ and $r_{-1} = 17 + i$. Assuming we've defined r_{k-2} and r_{k-1} for some $k \geq 0$, since $\mathbb{Z}[i]$ is a Euclidean domain, there exists some $q_k, r_k \in \mathbb{Z}[i]$ with $|r_k|^2 < |r_{k-1}|^2$ and

$$r_{k-2} = r_{k-1}q_k + r_k.$$

Continuing this process inductively yields a sequence of Gaussian integers

$$\{r_{-2}, r_{-1}, r_0, r_1, \ldots, r_{n-1}, r_n = 0\}.$$

Then r_{n-1} will be a GCD of r_{-2} and r_{-1}. Now we just carry out the algorithm:

$$\begin{aligned} 24 + 2i &= (17+i)(2) - 10 && |-10|^2 = (10)^2 < |17+i|^2 = (17)^2 + 1 \\ 17 + i &= (-10)(-2) + (-3+i) && |-3+i|^2 = 3^2 + 1^2 = 10 < 100 = |-10|^2 \\ -10 &= (-3+i)(3+i) + 0 && |0|^2 < |-10|^2. \end{aligned}$$

Thus we can take $r_0 = -10$ (with $q_0 = 2$), $r_1 = -3+i$ (with $q_1 = -2$), and $r_2 = 0$ (with $q_2 = 3+i$). Hence $r_1 = -3+i$ is a GCD of $17+i$ and $24+2i$.

12. (January 2021, Q3) Suppose A is a 9×9 matrix over the field $\mathbb{F}_5$ with 5 elements such that the characteristic polynomial of A is $(x-1)^2(x-3)^4(x^3-1)$ and the minimal polynomial of A is $(x-1)(x-3)^3(x^3-1)$. Compute the following:

 (a) The possible Jordan canonical form (or forms) of A over a suitable extension of $\mathbb{F}_5$;

 Solution. First of all, note that $x^3 - 1$ factors as $(x-1)(x^2+x+1)$. It is straightforward to see that x^2+x+1 is irreducible in $\mathbb{F}_5$, as it is quadratic and has no roots in $\mathbb{F}_5$. Thus we must pass to a splitting field of x^2+x+1, which is $\mathbb{F}_{25} \cong \mathbb{F}_5(\alpha)$, where α is a root of x^2+x+1. It is straightforward to see that x^2+x+1 factors as $(x-\alpha)(x+\alpha+1)$ over $\mathbb{F}_5(\alpha)$.

 Thus the characteristic polynomial of A is

$$c(x) = (x-1)^3(x-3)^4(x-\alpha)(x+\alpha+1)$$

 and the minimal polynomial is

$$m(x) = (x-1)^2(x-3)^3(x-\alpha)(x+\alpha+1)$$

 First we find the invariant factors $f_1, f_2, \ldots, f_k \in \mathbb{F}_5(\alpha)[x]$ of A. Using facts we know about invariant factors, one can check A has precisely two invariant factors, namely $f_1 = (x-1)(x-3)$ and $f_2 = m$. Then the elementary divisors of A are the prime powers dividing the invariant factors (counted individually, for each invariant factor), so they are given by

$$x-1,\ x-3,\ (x-1)^2,\ (x-3)^3,\ x-\alpha,\ x+(\alpha+1)$$

 Hence the Jordan canonical form of A has six Jordan blocks: a 1-Jordan block of size 1, a 3-Jordan block of size 1, a 1-Jordan block of size 2, a 3-Jordan block of size 3, a α-Jordan block of size 1, and a $-(\alpha+1)$-Jordan block of size 1. Thus there are $6! = 720$ Jordan canonical forms for A, given by different possible arrangements of the six distinct Jordan blocks. For example, one such matrix is given by

$$\left(\begin{array}{c|c|cc|ccc|c|c} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -(\alpha+1) \end{array}\right)$$

(b) The possible rational canonical form (or forms) of A.

Solution. Above we found the invariant factors of A were

$$f_1 = (x-1)(x-3) \equiv x^2 - 4x - 2 \bmod 5$$

and

$$\begin{aligned} f_2 &= (x-1)(x-3)^3(x^3-1) \\ &\equiv x^7 - 4x^5 - 3x^3 - x^2 - x - 2 \bmod 5, \end{aligned}$$

so the rational canonical form is the block matrix with blocks the companion matrix of f_1 and the companion matrix of f_2:

$$\left(\begin{array}{cc|ccccccc} 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right)$$

13. (August 2020, Q3)

(a) Compute, if possible, $\gcd(2+8i, 17-17i)$ in the ring $\mathbb{Z}[i]$ of Gaussian integers.

Solution. Perform the Euclidean algorithm for computing a gcd in a domain (which $\mathbb{Z}[i]$ is with norm function $N(\alpha) = |\alpha|^2 = (\Re\alpha)^2 + (\Im\alpha)^2$).

$$\begin{aligned} 17 - 17i &= (2+8i)(-2-3i) + (-3+5i) \\ 2 + 8i &= (-3+5i)(1-i) + 0, \end{aligned}$$

so that $\gcd(2+8i, 17-17i) = -3+5i$.

(b) Determine whether the following polynomials are reducible or irreducible in given rings

(b1) $x^4 + x^2 + 1$ in $\mathbb{Z}_2[x]$, where $\mathbb{Z}_2$ is the field with 2 elements;

Solution. Note that

$$x^4 + x^2 + 1 \equiv (x^2 + x + 1)^2 \bmod 2,$$

so the polynomial is reducible (this is an irreducible factorization, as $x^2 + x + 1$ is quadratic with no roots in $\mathbb{F}_2$).

(b2) $x^4 + 5x^3 + 10x^2 + 15x + 5$ in $R[x]$, where $R = \mathbb{Z}[i]$;

Solution. Consider the element $p = 2 + i \in R$. It is prime/irreducible in R because $N(p) = 2^2 + i^2 = 5$ is prime. Moreover, $p(2-i) = 5$, and p does not divide $(2-i)$ (because $up \neq 2 - i$ for $u \in \{\pm 1, \pm i\}$), so p divides 5 exactly once. Hence p divides the non-leading coefficients of the monic polynomial $x^4 + 5x^3 + 10x^2 + 15x + 5$, and p^2 does not divide the constant term, so by Eisenstein's criterion the polynomial is irreducible.

(b3) $2x^4 + 4x^3 + 8x^2 + 12x + 20$ in $\mathbb{Z}[x]$.

Solution. This polynomial is reducible, it factors as

$$2(x^4 + 2x^3 + 4x^2 + 6x + 10).$$

(this is an irreducible factorization by Eisenstein's with $p = 2$).

14. (August 2020, Q4)

(a) Let A be an $n \times n$ complex matrix and let f and g be the characteristic and minimal polynomials of A, resp. Suppose that $f(x) = g(x)(x - i)$ and $g(x)^2 = f(x)(x^2 + 1)$. Determine all possible Jordan canonical forms of A.

Solution.

$$g(x)^2 = f(x)(x^2 + 1) = f(x)(x + i)(x - i) = g(x)(x - i)^2(x + i),$$

and $\mathbb{C}[x]$ is a domain, so it follows that $g(x) = (x-i)^2(x+i)$ and $f(x) = (x-i)^3(x+i)^2$. Now, we'd like to find the invariant factors $f_1, f_2, \ldots, f_k \in \mathbb{C}[x]$ of A. Recall the following facts about the invariant factors:

- f_j is nonconstant and monic for $j = 1, \ldots, k$.
- $f_j \mid f_{j+1}$ for $1 \leq j < k$.
- $f_k = m$.
- $f_1 \cdots f_k = c$.

Then it follows that the invariant factors of A are given by $f_1(x) = (x - i)(x + i)$ and $f_2(x) = g(x) = (x - i)^2(x + i)$. Thus the elementary divisors are given by:

$$x - i, \quad x + i, \quad (x - i)^2, \quad \text{and} \quad x + i.$$

Hence the Jordan canonical form of A is any 5×5 block diagonal matrix with the following diagonal blocks: Two i-Jordan blocks of size 1, An i-Jordan block of size 2, and a $-i$-Jordan block of size 1. For example, the following matrix is a Jordan canonical form for A:

$$\left(\begin{array}{c|c|c|cc} i & 0 & 0 & 0 & 0 \\ \hline 0 & i & 0 & 0 & 0 \\ \hline 0 & 0 & -i & 0 & 0 \\ \hline 0 & 0 & 0 & i & 1 \\ 0 & 0 & 0 & 0 & i \end{array}\right).$$

(b) Let $\mathbb{F}$ be a field of characteristic $p > 0$ and $p \neq 3$. If α is a root of the polynomial $f(x) = x^p - x + 3$, in an extension of the field $\mathbb{F}$, show that $f(x)$ has p distinct roots in the field $\mathbb{F}(\alpha)$.

Proof. TODO □

15. (January 2020 Q1) Let G be a finite group of order 100.

(a) Show that G is solvable. (Feel free to use that groups of order p^2 are abelian for p a prime number).

Proof. By Sylow 3, we have that $n_5(G) \equiv 1 \bmod 5$ and $n_5(G) \mid 4$. It follows that $n_5(G) = 1$, so there exists a unique subgroup $H \leq G$ of order 25, and by Sylow 2 H is normal in G. Then we get a subnormal sequence of subgroups

$$0 \trianglelefteq H \trianglelefteq G.$$

Since $|H| = 5^2$ and 5 is prime, we have that $H/0 \cong H$ is abelian, as desired. Moreover, the quotient G/H has order $|G|/|H| = 2^2$, and 2 is prime, so G/H is abelian as well. Thus we have directly shown G is simple. □

(b) Show, by giving a counterexample, that G need not be nilpotent.

Proof. Consider the group $G = D_{10} \times \mathbb{Z}/2 \times \mathbb{Z}/5$ (recall D_{10} has presentation $\langle r, s \mid r^5, s^2, rsrs\rangle$). The group G has order $10 \cdot 2 \cdot 5 = 100$. Note that $n_2(D_{10}) > 1$: s generates a subgroup of order 2 which is not normal: the relation $rsrs = 1$ implies $sr^{-1} = rs$, so that $rsr^{-1}s^{-1} = rrss^{-1} = r^2$, which is not the identity, so r does not commute with s, meaning $r\langle s\rangle r^{-1} \neq \langle s\rangle$. Then $K := \langle s\rangle \times \mathbb{Z}/2 \times \mathbb{Z}/5$ is a non-normal 2-Sylow subgroup of G, because

$$(r, e, e)K(r, e, e)^{-1} = r\langle s\rangle r^{-1} \times \mathbb{Z}/2 \times \{e\} \neq K.$$

Thus G is not nilpotent. □

16. (January 2020 Q2) Decide which of the following sets are ideals of the ring $\mathbb{Z}[x]$. Provide justification.

(a) The set of all polynomials whose coefficient of x^2 is a multiple of 3.

This is not an ideal.

Proof. Consider $f = 3x^2+x$, which clearly belongs to the collection S of polynomials in question. Then $xf(x) = 3x^3 + x^2 \notin S$, since $3 \nmid 1$. Hence $\mathbb{Z}[x]S \not\subseteq S$, so S is not an ideal. □

(b) $\mathbb{Z}[x^2]$, the set of all polynomials in which only even powers of x appear.

This is not an ideal

Proof. $x^2 \in S$, but $x \cdot x^2 = x^3 \notin S$, so $\mathbb{Z}[x]S \not\subseteq S$. □

(c) The set of polynomials whose coefficients sum to zero.

This is an ideal

Proof. Clearly if $f, g \in S$ then $-f, f+g \in S$, so S is an abelian group. Now we need to show $\mathbb{Z}[x]S \subseteq S$. To see this, let $f = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ and $g = \sum_{i=0}^{m} b_i x^i \in S$. Then we have

$$fg = \sum_{j=0}^{n}\sum_{i=0}^{m} a_j b_i x^{i+j},$$

so that the sum of the coefficients of fg is

$$\sum_{j=0}^{n}\sum_{i=0}^{m} a_j b_i = \sum_{j=0}^{n} a_j \left(\sum_{i=0}^{m} b_i\right) = \sum_{j=0}^{n} a_j \cdot 0 = 0,$$

where the middle equality follows because $g = \sum_{i=0}^{m} b_i x^i \in S$, so that $\sum_{i=0}^{m} b_i = 0$. □

17. (January 2020 Q3) Find the possible Jordan canonical forms of 7×7 matrices M with entries in $\mathbb{C}$ satisfying the following criteria:

- the characteristic polynomial of M is $(z-3)^4(z-5)^3$,
- the minimal polynomial of M is $(z-3)^2(z-5)^2$, and
- the $\mathbb{C}$-vector space dimension of the nullspace of $3 \cdot \mathrm{Id} - M$ is 2.

Solution. First we'd like to find the invariant factors $f_1, f_2, \ldots, f_k \in \mathbb{C}[x]$ of M. Recall the following facts about the invariant factors:

- f_j is nonconstant and monic for $j = 1, \ldots, k$.
- $f_j \mid f_{j+1}$ for $1 \leq j < k$.

- f_k is the minimal polynomial of A.
- $f_1 \cdots f_k$ is the characteristic polynomial of A.

Using the first two bullet points and these facts, we get that the the invariant divisors are either

- $f_1 = (z-3)^2(z-5)$, $f_2 = m := (z-3)^2(z-5)^2$, or
- $f_1 = z-3$, $f_2 = (z-3)(z-5)$, and $f_3 = m = (z-3)^2(z-5)^2$.

Hence the elementary divisors of M are either

- $(z-3)^2$, $z-5$, $(z-3)^2$, and $(z-5)^2$, or
- $z-3$, $z-3$, $z-5$, $(z-3)^2$, and $(z-5)^2$.

It is straightforward to see that given some $\alpha \in \mathbb{C}$, the dimension of $\ker(\alpha I - M)$ is the number of times some power of $z-\alpha$ appears as an elementary divisor of M. Hence since $\dim\ker(3I - M) = 2$, powers of $z-\alpha$ must appear as elementary divisors of M exactly twice. Thus the elementary divisors of M must be

$$(z-3)^2, \quad z-5, \quad (z-3)^2, \quad \text{and} \quad (z-5)^2.$$

Thus a matrix is a Jordan canonical form for M if it is block diagonal, with: two 3-Jordan blocks of size 2, a 5-Jordan block of size 1, and a 5-Jordan block of size 2. For example, the following matrix is a Jordan canonical form for M:

$$\left(\begin{array}{c|cc|cc|cc} 5 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 5 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{array}\right).$$

18. (January 2020 Q4) Determine if the following polynomials are irreducible over $\mathbb{Z}$.

(a) $x^3 - 5x - 1$.

The polynomial is irreducible

Proof. Since the polynomial $f = x^3 - 5x - 1$ is monic, by Gauss' Lemma it suffices to show that the polynomial is irreducible over $\mathbb{Q}$. By the rational root theorem, any rational root of the polynomial is an integer dividing -1, i.e., if $f(x) := x^3 - 5x - 1$ has a root in $\mathbb{Q}$ it is 1 or -1. Yet one can check that $f(1), f(-1) \neq 0$, so f has no roots. Thus f is a cubic over the field $\mathbb{Q}$ with no roots, so f is irreducible over $\mathbb{Q}$, as desired. $\square$

(b) $x^4 + 10x^2 + 5$.

This polynomial is irreducible.

Proof. This is Eisenstein's with $p = 5$. $\square$