Algebra Comprehensive Exam Notes

Revised: January 5, 2019

Topics Index

1 GROUP THEORY

1.1 Basics and definitions

Definition 1.1 (Groups)**.** A *group* is a set G which is closed under the group operation $*$ which satisfies the following properties:

(a) (*Associativity*) For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

(b) (*Identity*) There is an element $1 \in G$ such that $g * 1 = 1 * g = g$ for all $g \in G$.

(c) (*Inverses*) For all $g \in G$ there is an element $g^{-1} \in G$ such that $g^{-1} * g = g * g^{-1} = 1$.

An *abelian group* is a group whose group operation is commutative: $h * g = g * h$, or equivalently $ghg^{-1} = h$, for all $h, g \in G$. A *subgroup* H of G (written $H \leq G$) is a subset of G which is closed under the same group operation $*$. The *subgroup criterion* states that $H \leq G$ iff H is a non-empty subset of G closed under the group operation such that $xy^{-1} \in H$ for all $x, y \in H$.

Definition 1.2 (Normal subgroups)**.** The operation of *conjugation* can be performed by taking $H \leq G$ and any fixed $g \in G$ and then forming the set

$$K := gHg^{-1} = \left\{ghg^{-1} : h \in H\right\}.$$

The resulting set K is a *subgroup* of G ($K = gHg^{-1} \leq G$) for any $g \in G$. We note that *conjugate elements* and *conjugate subgroups* have the same order. Moreover, for any $K \leq G$ and any $g \in G$ we have that $K \cong gKg^{-1}$. A *normal subgroup* H of G (written $H \trianglelefteq G$) is a subgroup of G such that $gH = Hg$, or equivalently $gHg^{-1} = H$, for all $g \in G$. A *simple group* has no non-trivial normal subgroups of itself, i.e., other than $\{1\}$ and G itself. For p prime, $\mathbb{Z}/p\mathbb{Z}$ is simple (and these are the only *abelian* simple groups).

Example 1.3 (Fall 2014, #1)**.** Show that a group of order 80 cannot be simple.

Properties of normal subgroups. If a group of *generators* $\{g_1, g_2, \ldots, g_n\} \subset G$ for G is known, to check if $N \trianglelefteq G$ it suffices to check only that these generators *normalize* N: $g_i N g_i^{-1} \subseteq N$ for all $i = 1, 2, \ldots, n$. The conjugate subgroups formed by conjugation of the elements $h \in G$ by all other $g \in G$ (cf. the *conjugacy class* of an element of G) partition G. In fact, we have that *normal subgroups are precisely unions of conjugacy classes of* G in that if $H \trianglelefteq G$, then for every conjgugacy class C of G that either $C \subseteq H$ or $C \cap H = \varnothing$. Every subgroup of an *abelian* group is normal. Similarly, every subgroup of a *cyclic* group is cyclic and hence *normal*. *Quotient groups* of a *cyclic* group are also always themselves cyclic.

Example 1.4 (Fall 2014, #6)**.** Let G be a group of order 140 and H be a subgroup of index 4. Show that H is normal in G.

Proposition 1.5 (When a quotient is a group)**.** *If $H \trianglelefteq G$, then G/H is a group.*

Proposition 1.6 (Commutativity between non-intersecting normal subgroups)**.** *If $H, K \trianglelefteq G$ and $H \cap K = \{1\}$, then $hk = kh$ for all $h \in H$ and $k \in K$. In other words, the elements in two normal subgroups of G that only share the identity in common commute.*

Proof Sketch. Let $h \in H$ and $k \in K$ be arbitrary. We need to show that $hk = kh$, or equivalently that $hkh^{-1}k^{-1} = 1$. Since $H \cap K = \{1\}$, it suffices to show that $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$ and also that $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$. By the normality of H and K and the closure of subgroup elements under the group operation, this is clearly the case. □

Definition 1.7 (Centers, centralizers, and normalizers)**.** The *center of G* is defined as

$$Z(G) := \{z \in G : gz = zg,\ \forall g \in G\}.$$

The center $\mathbf{Z(G)}$ is *always* a normal subgroup of $\mathbf{G}$. Also, $H \leq Z(G) \leq G$ implies that $H \trianglelefteq G$. In somewhat more general analog, the *centralizer in G of a set S* is defined to be

$$C_G(S) := \{z \in G : sz = zs,\ \forall s \in S\}.$$

The centralizer $C_G(G) = Z(G)$ is a *subgroup* of G. Moreover, we can see by a simple computation that $Z(G) \trianglelefteq C_G(S)$ for any $S \subseteq G$. Even more generally, the *normalizer of S in G* is defined to be the subgroup

$$N_G(S) := \{z \in G : zS = Sz \iff zSz^{-1} = S\}.$$

Clearly, we have that $C_G(S) \leq N_G(S)$. When G is *abelian* we have the equivalences $Z(G) = C_G(A) = N_G(A)$ for any subset $A \subseteq G$. More generally, we have that $C_G(A) \leq N_G(A) \leq G$.

Example 1.8. Prove that $G/Z(G)$ cyclic $\implies$ G is abelian.

Proof. Since $G/Z(G)$ is cylic there exists a generator $g \in G$ such that $\forall h \in G$, $h \cdot Z(G) = g^n \cdot Z(G)$ $\leftrightarrow h^{-1}g^n \in Z(G)$ for some $n \in \mathbb{Z}$. Now let $h, k \in G$. We need to show that $hk = kh$. By the above argument, $\exists M, N \in \mathbb{Z}$ and $z_1, z_2 \in Z(G)$ such that $h = z_1 g^{-N}$ and $k = z_2 g^{-M}$. This implies that $hk = z_1 z_2 g^{-(M+N)} = kh = z_2 z_1 g{-}(M + N)$. □

Example 1.9. Prove that if G is a group such that $2 \mid |G|$, then $\#\{\text{elements of } G \text{ of order-2}\}$ is odd.

Proof. We first notice that for all $a \in G$, $|a| = |a^{-1}|$. We also have that we can selectively *pair inverses* as the disjoint union

$$H := G \setminus \{e\} = \bigcup_{\substack{g \in G \\ g \neq g^{-1}}} \{g, g^{-1}\}.$$

Now we know that $e \in G$ has order of $1 \neq 2$, so that $X := \{g \in G : g^2 = e, g \neq e\}$ satisfies that $|X|$ is even. Now we see that $X \subset H$ where $|H| = |G \setminus \{e\}|$ is even. □

Example 1.10 (Spring 2016, #4)**.** Let G be a finite group, and let H be a proper subgroup of G. Prove that the union of all conjugates of H is a proper subgroup of G. Show that the conclusion need not be true if G is infinite.

1.2 Some standard examples of groups

Example 1.11 (Dihedral groups)**.** The *dihedral group D_{2n}* corresponds to symmetries of rigid motions of a regular n-gon in the plane. These groups have the presentation

$$\begin{aligned} D_{2n} &= \left\langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \right\rangle \\ &= \left\langle r, s \mid r^n = s^2 = (rs)^2 = 1 \right\rangle. \end{aligned}$$

For fixed $n \geq 2$, in these groups we have that $1, r, r^2, \ldots, r^{n-1}$ are all distinct elements (rotations through multiples of $2\pi/n$ radians), $s \neq r^i$ for any i (reflections about the center point of symmetry), and the inversion identity that $r^i s = sr^{-i}$ for $i \in \mathbb{Z}$. Since $D_{2n} = \{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$, we see that each element of the order-$2n$ dihedral group can be written *uniquely* as $s^k r^i$ for some $k \in \{0, 1\}$ and $0 \leq i < n$.

Example 1.12 (Symmetric and alternating groups)**.** Given any set $\Omega \neq \varnothing$, we write S_Ω to denote the set of all bijections (or *permutations*) of the set Ω onto itself. In the special case where $\Omega := \{1, 2, 3, \ldots, n\}$ we commonly write S_n to denote the *symmetric group on n elements*. We see by a simple counting argument that $|S_n| = n!$. The group S_n is ***non-abelian*** for all $n \geq 3$. Within the symmetric group S_n, disjoint cycles commute, the order of a permutation is the *lcm* of the lengths of the cycles in a permutation's cycle decomposition, and inverses are easily expressed by cycle reversion (as shown in the following example in S_{13}):

$$\begin{aligned} \sigma &= (1\ 12\ 8\ 10\ 4)(1\ 13)(5\ 11\ 7)(69) \implies \\ \sigma^{-1} &= (4\ 10\ 8\ 12\ 1)(13\ 2)(7\ 11\ 5)(96) \\ [(1532)(46)]^{-1} &= (2351)(64). \end{aligned}$$

Also, there are the identities that give us the explicit expansions:

$$\begin{aligned} (a_1 a_2 \cdots a_m) &= (a_1 a_m)(a_1 a_{m-1}) \cdots (a_1 a_3)(a_1 a_2) \\ (ab)(ac) &= (acb) \\ (ab)(cd) &= (abc)(bcd) \\ (abc) &= (ab)(de)(de)(bc) \\ (ij) &= (1i)(1j)(1i). \end{aligned}$$

If $\sigma = (a_1 \cdots a_{k_1})(b_1 \cdots b_{k_2}) \cdots \in S_n$, then conjugation by any other element $\tau \in S_n$ corresponds to the cycle decomposition

$$\tau\sigma\tau^{-1} = (\tau(a_1) \cdots \tau(a_{k_1}))(\tau(b_1) \cdots \tau(b_{k_2})) \cdots .$$

Two elements of S_n are conjugate iff they have the same cycle type decomposition. Note that $S_2 \cong \mathbb{Z}/2\mathbb{Z}$ and $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ (and hence is cyclic).

Important subgroups: The *alternating group on n elements*, A_n, is the subgroup of S_n consisting of only the *even permutations* in S_n. Consequently, we see by the first isomorphism theorem (A_n is the kernel of the *sign function* $\varepsilon \to \{\pm 1\}$) that $|A_n| = \frac{1}{2} \cdot |S_n| = \frac{n!}{2}$. Key properties of the alternating subgroups include that $A_n \trianglelefteq S_n$ and that for $n \geq 5$, $\mathbf{A_n}$ **is a non-abelian simple group**.

Generators and presentations:

- $S_n = \langle (12), (123 \cdots\ n) \rangle$;
- $S_n = \langle (12), \ldots, (1n) \rangle$
- The 3–cycles generare A_n;

Example 1.13 (Spring 2018, #1)**.** Let H be the subgroup of S_6 generated by (16425) and (16)(25)(34). Let H act on S_6 by conjugation. Show that the set

$$\Sigma = \{(12)(35)(46), (13)(24)(56), (14)(25)(36), (15)(26)(34), (16)(23)(45)\},$$

is invariant under H, thereby defining a homomorphism $\phi : H \to S_5$. Show that ϕ is an isomorphism.

Example 1.14 (Good examples of small groups)**.** We also have the following isomorphisms of groups (good to know these to build up a knowledge base of small examples):

- $S_2 \cong \mathbb{Z}/2\mathbb{Z}$ and $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ (cyclic subgroup)
- $D_6 \cong S_3$;
- $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$;
- $S_3 \ncong \mathbb{Z}/6\mathbb{Z}$;
- $\mathrm{Aut}(Z_2 \times Z_2) \cong \mathrm{GL}_2(Z_2) \cong S_3$;
- $\mathrm{Aut}(Z_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, which has order $\phi(n)$;
- For p prime, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic;
- $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$ whenever q is prime, For any $n \in \mathbb{N}$, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \cong \mathbb{Z}/\phi(n)\mathbb{Z}$ where $\phi(p^k) = p^k - p^{k-1}$.
- If G has ***prime*** order, then $G \cong \mathbb{Z}/p\mathbb{Z}$.
- We have that $\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$ since both containments are of order 2 and hence normal, but $\langle s \rangle \not\trianglelefteq D_8$ as conjugation by r in D_8 sends $s \mapsto rsr^{-1} = r^2 s \notin \langle s \rangle$.
- $\mathbb{Q}^2$ is NOT a field: $(0,1) \cdot (1,0) = (0,0)$ (it has zero divisors)
- A field with exactly 2017 elements of order 2: $D_{2 \cdot 2017}$.

Example 1.15 (The Klein 4-group)**.** The *Klein 4-group* (*Vierergruppe*) is given by $V \cong Z_2 \times Z_2$. It also has the presentation

$$V = \left\langle a, b \mid a^2 = b^2 = (ab)^2 = 1 \right\rangle$$
$$V_4 = \left\langle a, b \mid a^2 = b^2 = 1, ab = ba \right\rangle.$$

The group has several representations by permutations in S_4. The most interesting of these is given by

$$V = \{e, (12)(34), (13)(24), (14)(23)\},$$

which happens to be *normal in* A_4 (also $V \trianglelefteq S_4$). In this particular permutation representation (the rest of such representations are not normal subgroups), we have written V as the kernel of a surjective group homomorphism from $S_4 \to S_3$.

Example 1.16 (Matrix groups)**.** Let the *general linear group of degree n* be defined by

$$\mathrm{GL}_n(F) := \{A : A\text{is a } n \times n \text{ matrix with entries in } F \text{ such that } \det(A) \neq 0\},$$

for some field F. The set $\mathrm{GL}_n(F)$ forms a (non-abelian) group under matrix multiplication. Typically we draw the coefficients of the matrices in GL_n from a finite field, $\mathbb{F}_{p^n}$. If $|F| = q < \infty$ is a finite field, then the order of the general linear group is given by

$$|\mathrm{GL}_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

A related normal subgroup that comes up in the definition of the kernel of the *determinant function* is the *special linear group* $\mathrm{SL}_n(F)$ consisting of the matrices with elements in the specified field whose determinant is one. The special case of $\mathrm{SL}_2(\mathbb{R})$ is related to Möbius transformations in the plane and their interpretations as 2×2 real matrices.

1.3 Fundamental theorems on groups

The *order* of a group is the number of elements of the group (either finite or infinite). Similarly, we can define the notion of the *order* of an *element* $g \in G$ as the smallest positive integer power $n \geq 1$ such that $g^n = 1$. If n is the order of some $g \in G$, then the subset $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ **is the *cyclic subgroup* of G generated by g**. For any element $x \in G$, the subgroup $\langle x \rangle$ is the *unique* (!) *minimal element* of the set of all subgroups of G containing x (ordered by inclusion). The *cyclic group of order* n, denoted Z_n or $\mathbb{Z}/n\mathbb{Z}$, can be regarded as equivalent to addition modulo n.

Theorem 1.17 (Lagrange)**.** *Let the order of G and/or $g \in G$ be respectively denoted by $|G| = \mathrm{ord}(G)$ and $|g| = \mathrm{ord}_G(g)$. Then the order of a subgroup (element of G) divides the order of G for any group G.*

Note that only a partial converse to this theorem is true. That is to say, that there is not necessarily a subgroup of order n for any divisor $n \mid |G|$. When the divisors of the order of a group G are prime, or even better powers of a prime, we have more to say about the existence of subgroups of these specified orders.

Theorem 1.18 (Cauchy)**.** *If p is prime and $p \mid |G|$ is a divisor of the order of G, then there is some subgroup $H \leq G$ such that $|H| = p$.*

Definition 1.19 (p-Subgroups and Sylow subgroups)**.** For prime p, a *Sylow subgroup* is a so-called maximal *p-subgroup* whose order is the power of the prime p, or equivalently by Lagrange's theorem, whose elements all have order of p^k for some $k \geq 1$. For example, consider the cyclic group $G := \{g, g^2, g^3, g^4 = 1\}$ of order p^2 when $p := 2$. Since the definition of the p-subgroup involved requires maximality, we see that G is itself a *Sylow subgroup*, but that the subgroup $H := \{1, g^2\}$ is not Sylow by a contradiction to maximality.

Theorem 1.20 (Sylow's three theorems)**.** *The following results are known as Sylow's theorems:*

I. If $|G| = p^a \cdot m$ for some prime p where $p \nmid m$, then there is a Sylow subgroup $H \leq G$ of order $|H| = p^a$.

*II. Let H, K both be Sylow p-subgroups as above, i.e., $|H| = |K| = p^a$. Then these two subgroups are conjugate: $\exists g \in G$ such that $gHg^{-1} = K$. If there is a **unique** Sylow p-subgroup H with $|H| = p^a$, then it is necessarily normal in G: $gHg^{-1} = H$ for all $g \in G$ (**Proof**: If $n_p = 1$, then $|gPg^{-1}| = |P| \implies gPg^{-1} \in \mathrm{Syl}_p(G)$).*

III. Let n_p denote the number of Sylow p-subgroups for p a prime divisor of the order of G. Then we have that (i) $n_p \mid m$; (ii) $n_p \equiv 1 \pmod{p}$; and (iii) for P any Sylow p-subgroup of G $n_p = [G : N_G(P)] = |G|/|N_G(P)|$, or equivalently, $|N_G(P)| = |G|/n_p$.

The intersection of any two distinct Sylow p-subgroups is 1. Also, if $H \in \mathrm{Syl}_p(G)$ and $K \in \mathrm{Syl}_q(G)$ for $p \neq q$ two distinct primes dividing the order of G, then all of the elements of H commute with all of the elements of K.

Exercise 1.21. Find all Sylow subgroups of the Dihedral group D_{12}.

Example 1.22 (Spring 2014, #1)**.** Suppose G is a group with $|G| = 60$ and that $|Z(G)|$ is divisible by 4. Show that G has normal subgroup of order 5.

Example 1.23 (Fall 2012, #2)**.** Let G be a group of order p^2q where p, q are distinct primes. Prove that G has a non-trivial normal subgroup.

Lemma 1.24. *If $N \trianglelefteq G$ and $P \in \mathrm{Syl}_p(G)$ and $P \trianglelefteq N$, then $P \trianglelefteq G$.*

Example 1.25 (All groups of order 45 are abelian)**.** If $|G| = pq$ for $p < q$ primes and $q \neq 1 \pmod{p}$, then G is cyclic.
Short Proof: Since p, q are primes dividing the order of the group, by Cauchy there are subgroups P and Q with these respective orders. Moreover, $P = \langle a \rangle$ and $Q = \langle b \rangle$ for some $a, b \in G$ since p and q are prime. Now $|ab| = \text{lcm}(|a|, |b|) = pq = |G| \implies G = \langle ab \rangle$.

Definition 1.26 (Group homomorphisms)**.** Given two groups G, H, a *group homomorphism*, $\phi : G \to H$ is a mapping between the groups which preserves the group structure: for all $g_1, g_2 \in G$ $\phi(g_1 g_2) = \phi(g_1) \cdot \phi(g_2)$ where the right-hand-side product corresponds to the group operation in the range space H. An *isomorphism* is a homomorphism which is bijective (the two groups are isomorphic, $G \cong H$, if an explicit isomorphism can be exhibited between the two groups). The *kernel* of a group homomorphism, $\text{Ker}(\phi)$, is defined as the **normal subgroup** of G given by

$$\text{Ker}(\phi) := \{g \in G : \phi(g) = 1\}.$$

A group homomorphism is *injective* iff $\boxed{\text{Ker}(\phi) = \{1\}}$. Other properties of homomorphisms include: *(1)* $\phi(g^{-1}) = \phi(g)^{-1}$; *(2)* $\phi(g^n) = \phi(g)^n$; and *(3)* $\phi(1_G) = 1_H$. The next isomorphism theorems provide key relations between the groups involved in the definition of a group homomorphism.

Theorem 1.27 (The first isomorphism theorem)**.** *If $\phi : G \to H$ is a group homomorphism, then $G/\text{Ker}(\phi) \cong \text{Im}(\phi)$. We also have that $\text{Ker}(\phi) \trianglelefteq G$ and $\text{Im}(\phi) \leq H$ are both subgroups.*

Example 1.28. There is *NO* injective homomorphism from $D_{12} \to S_4$. If there were such a map, then by the First Isomorphism Theorem, we would have that D_{12} is isomorphic to some subgroup of S_4. But D_{12} has an element r or order 6, and by considering the cycle decompositions of S_4 there is no such element in this group (in particular, there cannot be a 2-cycle, a 3-cycle, or a 6-cycle as there are not enough letters in the group to permute).

Example 1.29. For F a field, prove that $\text{GL}_n(F)/\text{SL}_n(F) \cong F^*$.

Proof. Since F is a field, we notice that this is equivalent to showing that $\text{GL}_n(F)/\text{SL}_n(F) \cong F \setminus \{0\}$. We exhibit the explicit homomorphism (NOTE: *Should show that this is a homomorphism.*) $\varphi : \text{GL}_n(F) \to F^*$ defined by $M \mapsto \det(M)$. Then

$$\text{Ker}(\varphi) = \{M \in \text{GL}_n(F) : \varphi(M) = 1\} = \text{SL}_n(F).$$

And by the First Isomorphism Theorem,

$$\text{GL}_n(F)/\text{Ker}(\varphi) \cong \text{Image}(\varphi) = F \setminus \{0\}. \qquad \square$$

Theorem 1.30 (The second isomorphism theorem)**.** *Let $S \leq G$ and $N \trianglelefteq G$. Then*

(1) $SN \leq G$;

(2) $S \cap N \trianglelefteq G$;

(3) $(SN)/N \cong S/(S \cap N)$.

Proposition 1.31 (The class equation)**.** *We denote representatives for the distinct conjugacy classes of the group G by x_i. Then we have that*

$$|G| = |Z(G)| + \sum_{i=k}^{n} [G : C_G(x_i)].$$

Consequences of the class equation. The following are consequences of the class equation:

- If p is prime and $|P| = p^\alpha$ for some $\alpha \geq 1$, then P has a non-trivial center: $Z(P) \neq 1$.
- If $|P| = p^2$ for some prime p, then P is abelian. More precisely, $P \cong Z_{p^2}$ or $P \cong Z_p \times Z_p$. **Proof Sketch:** $Z(P) \neq 1 \implies P/Z(G)$ is cyclic $\implies P$ is abelian.

A few representative problems from past comprehensive exams

Proof Technique: (*Subset containment*): To show two sets are equal ($A = B$) show that $A \subseteq B$ and $B \subseteq A$.
Another Typical Trick: Use that $[G : H] = [G : K] \cdot [K : H]$ when $H \leq K \leq G$ are subgroups.

Example 1.32 (Fall 2015, problem #2)**.** Let G be non-abelian and finite. Prove that $|Z(G)| \leq |G|/4$.

Proof Sketch. The statement of this problem is equivalent to showing that

$$|G/Z(G)| = [G : Z(G)] = |G|/|Z(G)| \geq 4.$$

If $|G|/|Z(G)| \in \{1, 2, 3\}$, in contrast, we show that G is abelian. If $|G|/|Z(G)| = 1$ then $Z(G) = G$ so that G is abelian. For the other two cases, we note that if $|H| = p$ for any group H where p is prime then H is cyclic. This fact follows from Lagrange's theorem which shows that for $g \in H$, $\text{ord}(g) = 1, p$ so that for $g \neq 1$, g is a generator for H. Considering the representative case where $|G/Z(G)| = 3$, we can see that the quotient satisfies the disjoint union representation $G = Z \cup Zg \cup Zg^2$ for some non-trivial $g \in G$. Then we perform a computation and rearrange terms with the normal center to see that this quotient is abelian. A similar argument holds for the order-2 case. □

Example 1.33 (Spring 2017, # 3)**.** Let G be a group of order 10. Which of the following is a possible class equation for G? (a) $1+1+1+2+5$; (b) $1+2+2+5$; (c) $1+2+3+4$; (d) $1+1+2+2+2+2$.

Proof. We show that (a) is not a valid class equation: if this were valid, then $|Z(G)| = 3$, and since $Z(G) \leq G$ by Lagrange $3 \mid 10$ ($\mathcal{X}$). Similarly, (c) is not a valid equation since each conjugacy class is a subgroup of G and hence its size must be a divisor of 10 ($\mathcal{X}$). We consider (d): Then $|Z(G)| = 2$ where $Z(G) \trianglelefteq G$ and hence $n_2 = 1$ ($Z(G)$ is the unique Sylow 2-subgroup of G). Now if we let H denote a Sylow 5-subgroup of G, then since $2, 5$ are both prime, $Z(G) \cong Z_2$ and $H \cong Z_5$ are both cyclic and hence abelian. We also know that all elements of $Z(G)$ commute with all elements of H since they are both Sylow subgroups for different primes. Then it follows that $G \cong Z(G) \times H$, which is abelian, and so can have no conjugacy classes of size $2 < 10 = |G|$. So (d) is not a possibility. We are left with showing that (b) is the class equation for the dihedral group D_{2n} when $n = 5$: $D_{10} = \langle r, s : r^5 = s^2 = (rs)^2 = 1\rangle$. Then we look at conjugacy classes in D_{10}: we have $\{1\}$, $\langle rs\rangle = \{a, b\}$, $\langle s\rangle = \{c, d\}$, and $\langle r\rangle = \{e_1, e_2, e_3, e_4, e_5\}$. □

Example 1.34 (Spring 2016, # 3)**.** Show that every group of order 35 is cyclic. In other words, up to isomorphism, there is only one unique group of order 35.

Approach 1 (Direct method). Note that $(5, 7) = 1$ (orders must be *coprime* for this attempt to work). $G \cong C_5 \times C_7$, which is cyclic (hence, abelian). Within $(a, b) \in C_5 \times C_7$, there is an element $(1, 1)$ of order 1, and element $(1, b)$ of order 7, an element $(a, 1)$ of order 5, and the remaining elements (a, b) of order 35. Then $(1, 1) = (a, b)^k = (a^k, b^k)$ which implies that $5 \mid k$ and $7 \mid k \implies 35 \mid k$. So this cyclic group is the whole group. □

Note that in the above we used the second isomorphism theorem to show that $HK = H \times K$ where H is the normal Sylow 5-subgroup and K denotes the normal Sylow 7-subgroup:

$$HK/K \cong H/(H \cap K) \cong H/\{1\} \cong H.$$

Example 1.35 (Fall 2017, # 1)**.** Let x and y be two elements of order 2 in a finite group G. Prove that $\langle x, y\rangle$ is eiether abelian or isomorphic to a dihedral group.

Proof. Let $H := \langle x, y\rangle$ and let $H' := \langle xy, y\rangle$. Now since $xy \in H$ and $x = xyy \in H'$, we can see that $H = H'$. Suppose that n is the order of xy in G. Then since $(xy)^n = y^2 = (xyy)^2 = 1$, we can construct a well-defined surjective group homomorphism from $D_{2n} = \langle r, s \mid r^n = s^2 = (rs)^2 = 1\rangle$ onto H by mapping $r \mapsto xy$ and $s \mapsto y$. To complete the proof, we need to argue that this homomorphism is injective – and hence bijective and so an isomorphism between these two groups. Let $r^k s^\ell$ denote a non-trivial element in the kernel of the homomorphism for some $k, \ell \in \mathbb{N}$ with $0 \leq k < n$ and $\ell \in \{0, 1\}$ and such that k is minimal – or as small as possible. Then by the mapping we have defined $(xy)^k y^\ell = 1$. Moreover, since $|xy| =: n$ and $|y| = 2$ WLOG we can assume that $k \geq 1$ and $\ell = 1$. If we have that $k = 1$, then $1 = xyy = x$, which contradicts the hypothesis that $|x| = 2$. So we may now assume that $k \geq 2$. Then by computational, or rather *algebraic*, trickery we can show that $1 = yxxy = yx[(xy)^k y]xy = yx[xy][(xy)^{k-2}][xy]yxy = (xy)^{k-2}y$, which again contradicts the minimality of k. Hence, $k = 0$ and we must have had that $\ell = 0$ as well for this element to be in the kernel. So the kernel of our homomorphism is $\{1\}$, which yields injectivity. We are done. □

1.4 Group actions

Definition 1.36 (Group actions)**.** Given a group G and any set X, a *group action* $\phi : G \times X \to X$ is a map defined by $g \cdot x \mapsto y$ which satisfies (1) $1 \cdot x = x$; and (2) $(gh) \cdot x = g \cdot (h \cdot x)$. Each element of G can be thought of a providing an individual mapping $\phi_{g_i} : X \to X$. The **kernel of a group action** is a *normal* subgroup of G:

$$\begin{aligned}\mathrm{Ker}(\varphi) &= \{g \in G : g \cdot x = x, \forall x \in X\} \\ &= \{g \in G : \varphi(g) = \mathrm{id}_X\}.\end{aligned}$$

The *orbit* of x is defined by $G \cdot x = \{gx : g \in G\} \leq X$. The *stabilizer of a in G*, denoted by G_a, is the subgroup of G defined by

$$G_a := \{g \in G : g \cdot a = a\} \leq G.$$

Clearly, $G_a \leq G$ for any fixed $a \in X$. The *orbit-stabilizer theorem* (see below) states that the mapping $hG_x \mapsto h \cdot x$ is a bijection: $|G| = |G \cdot x| \cdot |G_x|$ for any fixed $x \in X$.

Example 1.37 (Groups act on themselves by conjugation)**.** If G is a group and $G \circlearrowleft G$ by conjugation, then $\mathrm{Ker}(\text{action}) = C_G(G) = Z(G)$.

Theorem 1.38 (The orbit-stabilizer theorem)**.** *Let the equivalence relation $\sim$ on A be defined by $a \sim b$ if and only if $a = g \cdot b$ for some $g \in G$. The number of elements in the equivalence class containing some $a \in A$ (or the orbit of G containing a) is given by $[G : G_a]$: the index of the stabilizer of a in G. Alternately, $|\operatorname{Orb}(x)| = [G : \operatorname{Stab}(x)] = |G|/|\operatorname{Stab}(x)|$.*

Example 1.39 (Spring 2015, # 5)**.** Let G be a finite group, $H \leq G$, and set $[G : H] = p$ for p prime. Let n_H be the number of subgroups of G *conjugate* to H where K is conjugate to H if $\exists g \in G$ such that $gKg^{-1} = H$. Prove that $n_H = 1$ if H is normal and that $n_H = p$ otherwise.

Proof. First, by the definition of normal if H is normal then $gHg^{-1} = H$ for all $g \in G$. Thus $n_H = 1$ in this case. Now suppose that H is not normal. Let $X := \{\text{set of subgroups of } G\}$. We form the group action $G \times X \to X$ by conjugation which maps subgroups to subgroups (well-defined): $(g, H) \mapsto gHg^{-1}$. Next, we look at the orbit of H under the action: $G \cdot H = \{gHg^{-1} : g \in G\}$. So we see that $|\operatorname{orbit}(H)| = n_H = |G \cdot H|$, which is the quantity we are looking for. By the orbit-stabilizer theorem, we have that

$$n_H = |G \cdot H| = \frac{|G|}{|G_H|} = \frac{|G|}{|\{g \in G : gHg^{-1} = H\}|} = \frac{|G|}{|N_G(H)|}.$$

From this we establish two possible cases. In case I, we consider that $H = N_G(H)$ so that $n_H = |G|/|H| = [G : H] = p$ and we are done. In case II, we must consider the possibility that $H \neq N_G(H)$ where $H \leq N_G(H) \leq G$ so that $p = [G : H] = [G : N_G(H)] \cdot [N_G(H) : H]$. Then by assumption and since p is prime we have that $[G : N_G(H)] = 1$, which implies that H is normal – a contradiction to our assumption. So in this case we have that $n_H = p$, as required. □

Example 1.40 (Fall 2013, #1)**.** Let G be a group, and let H be a subgroup of G. If every prime p dividing $n := |H|$ is at least $[G : H]$, prove that H is a normal subgroup of G.

Example 1.41 (Spring 2011, #2)**.** Prove that if G is a finite group containing no subgroup of index 2, then any subgroup of index 3 is normal in G.

Lemma 1.42 (Burnside's lemma)**.** *Suppose that a finite group G acts on a finite set X. Define a function $f : G \to \mathbb{N}$ by letting $f(g)$ be the number of points of X fixed by g: $f(g) = |\{x \in X : g \cdot x = x\}|$. Then the number of orbits of this action is equal to*

$$\#(orbits) = |X/G| = \frac{1}{|G|} \sum_{g \in G} f(g).$$

In other words, the number of orbits is the average number of points fixed by the elements of G.

Exercise 1.43. Let G be a group acting on a set X. Show that if $x_1, x_2 \in X$ lie in the same orbit, then their stabilizers are conjugate subgroups of G.

1.5 Fundamental theorem of finitely generated abelian groups

Proposition 1.44 (Inveriant factor decomposition)**.** *If G is a finitely generated abelian group, then there is a unique (!) expression of $G \cong \mathbb{Z}^r \times Z_{n_1} \times \cdots \times Z_{n_s}$ where $r \geq 0$, $n_j \geq 2$, and $n_{i+1} \mid n_i$ for $1 \leq i < s$. Here r is called the free rank and the n_i are called the invariant factors. We see that G is finite $\iff$ $r = 0$, that $|G| = n_1 \cdots n_s$, and that if p is a prime factor of $|G|$ then $p|n_1$.*

Proposition 1.45 (Primary decomposition for finite abelian groups)**.** *Let $|G| = n < \infty$ and suppose that the prime factorization is $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Then $G \cong A_1 \times \cdots A_k$ where $|A_i| = p_i^{\alpha_i}$. Moreover, for each A_i, $A_i \cong Z_{p_i^{\beta_1}} \times \cdots \times Z_{p_i^{\beta_t}}$ where $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t \geq 1$ and $\beta_1 + \cdots + \beta_t = \alpha_i$. The prime powers $p_i^{\beta_j}$ are the elementary divisors of G.*

Corollaries of the previous proposition include the following:

- $Z_m \times Z_n \cong Z_{mn}$ <u>iff</u> $\gcd(m, n) = 1$;
- If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then $Z_n \cong Z_{p_1^{\alpha_1}} \times \cdots \times Z_{p_k^{\alpha_k}}$.
- Let G be a finite group and let $p_1, \cdots, p_s$ be the distinct primes dividing its order with $P_i \in \mathrm{Syl}_{p_i}(G)$. Then TFAE: *(i)* $P_i \trianglelefteq G$ for all $1 \leq i \leq s$; and *(ii)* $G \cong P_1 \times P_2 \times \cdots \times P_s$.

Particular examples of these decompositions include the following:

- $G = Z_6 \times Z_{15}$. Then $G \cong Z_2 \times Z_3 \times Z_3 \times Z_5$ and the elementary divisors of G are $2, 3, 3, 5$;
- $G = Z_{10} \times Z_9$ has elementary divisors $2, 5, 9$ and $G \cong Z_2 \times Z_5 \times Z_9$.
- Also, note that $Z_6 \times Z_{15}$ has no element of order 9 whereas $Z_{10} \times Z_9$ does.

Example 1.46 (Spring 2013, #2)**.** Write down a complete list of abelian groups of order 270.

1.6 Misc results on groups

Proposition 1.47 (Normal-indexed subgroups)**.** *If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of index p is necessarily normal. Note that such a subgroup of minimal prime order need not exist. In particular, any index-2 subgroup $H \leq G$ such that $[G : H] = 2$ is normal in G: in fact, $H \trianglelefteq G$.*

Example 1.48 (Properties of left cosets)**.** For fixed choices of $g \in H$, the *cosets* of the group H are defined by $gH = \{gh : h \in H\}$. Given a normal $N \trianglelefteq G$, the set of *left cosets* of N in G forms a partition of G:

$$G = \bigcup_{g \in G} gN.$$

We have that two cosets are equal, $uN = vN$, for some $u, v \in G$ iff $v^{-1}u \in N$. ***All cosets have the same size.***

Example 1.49 (Properties of cyclic subgroups)**.** If $|x| = n < \infty$ for some element $x \in G$, then the order of the a^{th} power element is given by $|x^a| = n/\gcd(n, a)$. In particular, if $H = \langle x \rangle$ then this cyclic subgroup is also generated as $H = \langle x^a \rangle$ iff $\gcd(a, n) = 1$. Every subgroup of a cyclic subgroup is also itself cyclic. In the cyclic group case, we have a complete converse to Lagrange's theorem. Namely, if $H = \langle x \rangle$ with $|x| = |H| = n < \infty$, then for each distinct $a \mid n$ there are *unique* (!) cyclic subgroups of H of order a: $S = \langle x^d \rangle$ where $d = n/a$ has order $|S| = a$.

Example 1.50 (Products of groups)**.** For any two $H, K \leq G$, we have that

$$HK := \{hk : h \in H, k \in K\}.$$

The order of such indirect product groups satisfies the following formula: $|HK| = |H| \cdot |K|/|H \cap K|$. This product group is itself not necessarily a subgroup of G. However, whenever $K \trianglelefteq G$ (with $H \leq G$), then $HK \leq G$. Alternately, if $H, K \leq G$ and $H \leq N_G(K)$, then $HK \leq G$.

Fact: The number of conjugates of a subset $S \subseteq G$ is the index of the normalizer of S, $[G : N_G(S)]$, where $N_G(S) = \{g \in G : gSg^{-1} = S\}$.

Some classifications

(1) $|G| = p$ leads to a cyclic group;

(2) $|G| = p^2$ leads to an abelian group, isomorphic to one of $Z_p \times Z_p$ or Z_{p^2};

(3) $|G| = pq$: *(i)* if $p \nmid q - 1$, then G is cyclic; and *(ii)* if $p \mid q - 1$ we have one cyclic and one non-abelian case;

(4) $|G| = p^3$, with $p \neq 2$: all lead to abelian cases: one of Z_{p^3}, $Z_{p^2} \times Z_p$, or $(Z_p)^3$.

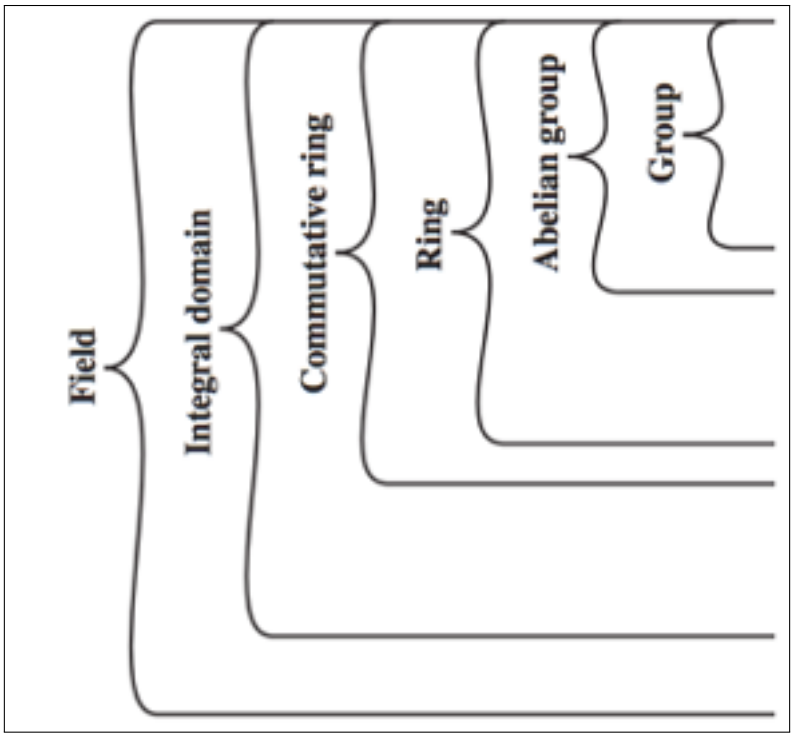
2 RING THEORY

2.1 Basics

Definition 2.1. A *ring* $R(+,\cdot)$ is a set together with two binary operations such that *(i)* $R(+)$ is an *abelian* group with additive identity $a+0=0+a=a$; *(ii)* $R(\cdot)$ is a *monoid* satisfying $a(bc)=(ab)c$ with multiplicative identity $1a=a1=a$; and *(iii)* the distributive laws relating the two operations hold: $a(b+c)=ab+ac$ and $(a+b)c=ac+bc$. Note that we do not require multiplicative inverses nor that multiplication is commutative. We have the following general containment structure:

$$\text{group} \supset \text{ring} \supset \text{commutative ring} \supset \text{domains}.$$

In a field, we add in inverses with respect to $\cdot$ and require that $\cdot$ is commutative.



Misc definitions.

- $R^\times$ is the set of units of R which forms a group under $*$ (hence, the *group of units*).
- An example of a *zero divisor* in Z_6 is $2\cdot 3=0$.
- In a *commutative ring* the operation $\cdot$ becomes abelian.
- An (*integral*) *domain* is a **commutative ring** with identity $1\neq 0$ with no zero divisors: $ab=0 \iff a=0$ or $b=0$. **Any *finite integral domain* is a field.**

- A *unit* is an element in the ring with a multiplicative inverse, i.e., $a \in R$ such that $a^{-1} \in R$ exists. The product of two units is a unit. Units may not commute under multiplication.
- A *nilpotent* element $a \in R$ is an element such that there is a $n \geq 1$ such that $a^n = 0$. For example, in $8\mathbb{Z}$, or equivalently mod 8, 2 is nilpotent since $2^3 = 0$.
- A polynomial $p(x) \in R[x]$ is *reducible* if $\exists q(x), r(x) \in R[x]$ (not units) such that $p(x) = q(x)r(x)$.

To show that $S \subseteq R$ is a *subring* it must be *non-empty* and closed under $(-)$ and $(*)$. The relation "*is a subring*" is transitive.

Example 2.2 (Spring 2013, #6)**.** Let p be a prime number, and let $\mathbb{F}_p$ be the finite field with p elements. How many elements of $\mathbb{F}_p$ have cube roots?

Definition 2.3 (Ideals)**.** The motivation for defining *ideals* is similar to that behind defining normal subgroups of a group G. We seek that if $I + a, I + b \in R/I$ are cosets that $(I + a) + (I + b) = I + a + b$ and $(I + a)(I + b) = I + ab$. Now a *left ideal* is a set $I \subseteq R$ such that for all $x, y \in I$ and for all $r \in R$: $x + y \in I$ and $rx \in I$. We see that all elements of an ideal are of the form $r_1x_1 + \cdots + r_nx_n \in I$. Also, $0 \in I$ (always since $\pm a \in I$) and the multiplicative identity $\boxed{1 \in I \text{ iff } I = R}$.
Variants. We define the *left ideal*

$$RI = \{r_1x_1 + \cdots + r_nx_n : n \in \mathbb{N}, r_i \in R, x_i \in I\},$$

and do similarly for the corresponding *right ideals*, IR. We can also define sets like Rx and of course RxR to be the *principal ideal generated by* x defined by $RxR = \{r_ixr_j : r_i, r_j \in R\}$.
Properties. $I+J$ is the smalest ideal of R containing both I and J. Additionally, $IJ = \{a_1b_1+\cdots+a_nb_n : a_i \in I, b_i \in J\}$ is an ideal contained in $I \cap J$ (but it may be smaller). It is also the smallest ideal containing the set $\{ab : a \in I, b \in J\}$. In particular, it is immediate that $IJ \subseteq I \cap J$.

To prove that $I \subseteq R$ is an ideal, we need to check that I is non-empty, that it is closed under $(+)$, and that it is closed under $(*)$ by *all* elements of R.

For any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ (and these are the only ideals of $\mathbb{Z}$). The *natural projection* $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is called *reduction modulo* n.

Example 2.4 (Fall 2013, #4)**.** Let R be a commutative ring with identity.

a. Let I, J be ideals of R, and let P be a prime ideal of R. If $IJ \subset P$, prove that either $I \subset P$ or $J \subset P$;

b. Let A, B, I all be ideals of R. If $I \subset A \cup B$, prove that either $I \subset A$ or $I \subset B$.

Definition 2.5 (Ring homomorphisms)**.** A *ring homomorphism* $\phi : R \to S$, satisfies the following:

(i) $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$;

(ii) $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$;

(iii) $\phi(0_R) = 0_S$;

(iv) If ϕ is surjective or S is an ID, then $\phi(1_R) = 1_S$

If ϕ is a ring homomorphism, then $\boxed{\text{Ker}(\phi) = \{x : \phi(x) = 0\} \text{ is } \textbf{\textit{always}} \textbf{ an ideal}}$. If I is any ideal, then the map $R \to R/I$ defined by $r \mapsto r + I$ is a **surjective** ring homomorphism with **kernel I**.

Theorem 2.6 (The isomorphism theorems for rings)**.** *The first isomorphism theorem for rings states that if $\phi : R \to S$ is a ring homomorphism then:*

(1) $\mathrm{Ker}(\phi)$ *is an ideal of* R*;*

(2) $\mathrm{Im}(\phi)$ *is a subring of* S*;*

(3) $\mathrm{Im}(\phi) \cong R/\mathrm{Ker}(\phi)$*.*

Similarly, the second isomorphism theorem for rings states that if R is a ring, $S \subseteq R$ is a subring, and I is an ideal of R that:

(1) $S + I$ *is a subring of* R*;*

(2) $S \cap I$ *is an ideal of* S*;*

(3) $(S + I)/I \cong S/(S \cap I)$*.*

Theorem 2.7 (Chinese remainder theorem)**.** *If $A, B \subseteq R$ are ideals we call them coprime if $A+B = R$, which is the same as $\exists a \in A, b \in B$ such that $a + b = 1$. The Chinese remainder theorem states that if I_1, I_2, ..., I_k are pairwise coprime ideals of R and if $I = I_1 \cap \cdots \cap I_k$, then*

$$R/I \cong R/I_1 \times \cdots \times R/I_k,$$

under the isomorphism $I + a \mapsto (I_1 + a) \times \cdots \times (I_k + a)$. If R is commutative, then $I = I_1 \cdots I_k$.

2.2 Representative questions from past comprehensive exams

Example 2.8 (Fall 2015, #3)**.** Which of the following are isomorphic?

(a) $R_1 = \mathbb{Q}[x]/(x^2 - 1)$;

(b) $R_2 = \mathbb{Q}[x]/(x^2 - 2)$;

(c) $R_3 = \mathbb{Q}[x]/(x^2 - 3)$;

(d) $R_4 = \mathbb{Q}[x]/(x^2 - 4)$.

Proof. Recall that $\boxed{A := F[x]/(p(x)) \text{ is a field } \underline{\text{iff}}\ p(x) \text{ is irreducible over } F}$. Thus R_2 and R_3 are fields by Eisenstein where the other two choices are not since they split into linear factors over $\mathbb{Q}$. And we know that we cannot have an isomorphism between a field and a non-field. To show that $R_2 \ncong R_3$ we need to find a contradiction in the properties of the elements of each respective field. Namely, by splitting field theory properties we have that $R_2 \cong \mathbb{Q}(\sqrt{2})$ and $R_3 \cong \mathbb{Q}(\sqrt{3})$, but for example, 3 is not a square in R_2: $(a + b\sqrt{2})^2 = 3 \implies a^2 + 2b^2 = 3$ and $2ab\sqrt{2} = 0 \implies a = 0 \vee b = 0$, but $a^2 = 3$ nor $2b^2 = 3$ have rational solutions. Now since $\frac{1}{2}(x+1) - \frac{1}{2}(x-1) = \frac{1}{4}(x+2) - \frac{1}{4}(x-2) = 1$, we have that $(x+1), (x-1)$ are coprime, as are $(x+2), (x-2)$. So by the Chinese remainder theorem we see that $R_1 \cong \mathbb{Q}[x]/(x-1) \times \mathbb{Q}[x]/(x+1) \cong \mathbb{Q} \times \mathbb{Q}$ and similarly for R_4. Hence $R_1 \cong R_4$. Noting also that $\mathbb{Q}^2$ is not a field since $(0, 1) \cdot (1, 0) = 0$. □

Example 2.9 (Spring 2015, #2)**.** Which of the following are isomorphic? $R_1 = \mathbb{Z}[i]/(5)$, $R_2 = \mathbb{F}_5[x]/(x^2 - 1)$, and $R_3 = \mathbb{F}_5[x]/(x^2 + 1)$?

Proof. Here we may write $\mathbb{F}_5 = \{0,1,2,3,4\}$. Factorizing over this finite field shows that $x^2+1 = (x+a)(x+b) = (x-a)(x+a) = x^2-a^2 \mapsto (x-2)(x+2) = x^2-4$. So both polynomials x^2-1 and x^2+1 split into linear factors in $\mathbb{F}_5[x]$. Now we see that in each case the ideals formed by these linear factors are coprime: $3(x+1)+2(x-1) = 1 = (x-2)-(x+2) = -4 = 1$. Then by the CRT, we obtain that $R_3 \cong \mathbb{F}_5[x]/(x+4) \times \mathbb{F}_5[x]/(x+1) \cong \mathbb{F}_5 \times \mathbb{F}_5$, and similarly, $R_2 \cong (\mathbb{F}_5)^2$ so that $R_2 \cong R_3$. It remains to show that also $R_1 \cong R_2, R_3$.

Since $5 = (2+\imath)(2-\imath)$ is reducible in $\mathbb{Z}[\imath]$ with the ideals $(2\pm\imath)$ again coprime to one another, by the CRT we find that $R_1 \cong Z[\imath]/(2+\imath) \times Z[\imath]/(2-\imath)$. Consider an arbitrary non-identity element $a+b\imath$ in the ring $\mathbb{Z}[\imath]$. We consider the behavior of adding multiples of this element (first modulo $2+\imath$): $a+b\imath \pmod{2+\imath}, \ldots, 5(a+b\imath) = (2+\imath)(2-\imath)(a+b\imath) = 0 \pmod{2+\imath}$. Hence $1 < \mathrm{ord}(a+b\imath) \leq 5$ (since we assumed that this element was not the identity). So by order considerations we have obtained that $R_1 \cong Z_5 \times Z_5 \cong (\mathbb{F}_5)^2$ since 5 prime implies that Z_5 is in fact a finite field. Then all three rings are isomorphic to one another. □

Example 2.10 (Fall 2015, #8 and Spring 2017 #8)**.** Let B be a commutative ring and let $f = \sum_{i=0}^{n} b_i x^i$ for $b_i \in B$. Prove that f is nilpotent iff the b_i are nilpotent.

Proof. In the reverse direction, we first claim that the sum of any two nilpotent $a, b \in B$ is also nilpotent. Indeed, for if $a^n = b^m = 0$, then $(a+b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^j$, where $i+j = n+m$ which implies that we always have at least one of $i \geq n$ or $j \geq m$. By extension (and/or the multinomial theorem) we can see that the sum of a collection of nilpotent $a_i \in B$ is also nilpotent, i.e., if $a_1^{m_1} = \cdots = a_n^{m_n} = 0$, then $(a_1 + \cdots + a_n)^{m_1+\cdots+m_n} = 0$. This then implies necessarily that if the b_i are nilpotent for all $0 \leq i \leq n$ then there is some power m such that $f(x)^m = \left(\sum_i b_i x^i\right)^m = 0$. So f is nilpotent too.

In the forward direction, let $m \geq 1$ be such that $f(x)^m = 0$. Then $\deg(f(x)^m) = nm$ and

$$0 = \left(\sum_{i=0}^{n} b_i x^i\right) = a_{nm}x^{nm} + \cdots + a_1 x + b_0^m,$$

where the coefficients $a_i \in B$ are uniquely determined by the b_i and the power m. Surely the equation above must hold when we specialize the indeterminate $x \mapsto 0$:

$$f(x)^m\Big|_{x=0} = b_0^m = 0,$$

and so we have determined that b_0 is nilpotent. This shows also that $-b_0$ is nilpotent, and so $f(x) - b_0 = x(b_n x^{n-1} + \cdots + b_1)$ must be nilpotent. Then we repeat the same argument used for b_0 to show that b_1 is nilpotent, and so on by induction, to obtain that b_i is nilpotent for all $0 \leq i \leq n$. And we are done. □

Example 2.11 (Fall 2012, #5)**.** Let R be a commutative ring and set $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ a zero divisor in the polynomial ring $R[x]$. Show that there is a non-zero element $b \in R$ such that $ba_0 = ba_1 = \cdots = ba_n = 0$.

Example 2.12 (Spring 2015, #6)**.** Let I be a non-zero ideal of $\mathbb{Z}[x]$ and suppose that the lowest degree of a polynomial in I is n and that I contains a monic polynomial of degree n. Prove that I is a principal ideal.

Proof. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ denote this magical stated monic polynomial of degree n which we are given to exist. We surmise that we must prove that $I = (f)$, i.e., I is principal with generator f. To show this we can use subset containment. Namely, we must show both that (i) $(f) \subseteq I$; and that (ii) $I \subseteq (f)$ so that $I = (f)$. For (i) it is easy enough to see that if $m \in I$ is any fixed element then clearly $(m) \subseteq I$ since $rm \in I$ for all $r \in R$. Now to show (ii) we let $g \in I$ and use the monic property of f to write $g = f \cdot q + r$ where $\deg(r) < \deg(f)$. Since $q \cdot f \in I$ and $g \in I$, we must then have that $r = g - q \cdot f \in I$. But we have by hypothesis that the degree of f is minimal in I. Hence, $r = 0$ which shows that $g \in (f)$. □

2.3 Other topics on rings

An ideal generated by a single element is called a *principal ideal*. A domain in which all ideals are principal is called a *PID*. As an example, $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ where $d = \gcd(m, n)$. Also, since for $b \in R$, $b \in (a) \iff b = ra$ (a divides b in R, or equivalently, $(a) \subseteq (b)$), we have that $n\mathbb{Z} \subseteq m\mathbb{Z} \iff m \mid n$. An ideal M of R is called *maximal* if $M \neq R$ and the only ideals of R containing M are M and R itself. *Every non-zero ideal in a PID is maximal.*

Example 2.13 (Spring 2017, #7)**.** Let R be a commutative ring with 1, and let M be a principal maximal ideal. Prove each of the following:

1. Show that there is no ideal I such that $M^2 \subsetneq I \subsetneq M$;
2. Give an example of a ring R and a maximal ideal M to show that this statement is false if M is not assumed to be principal.

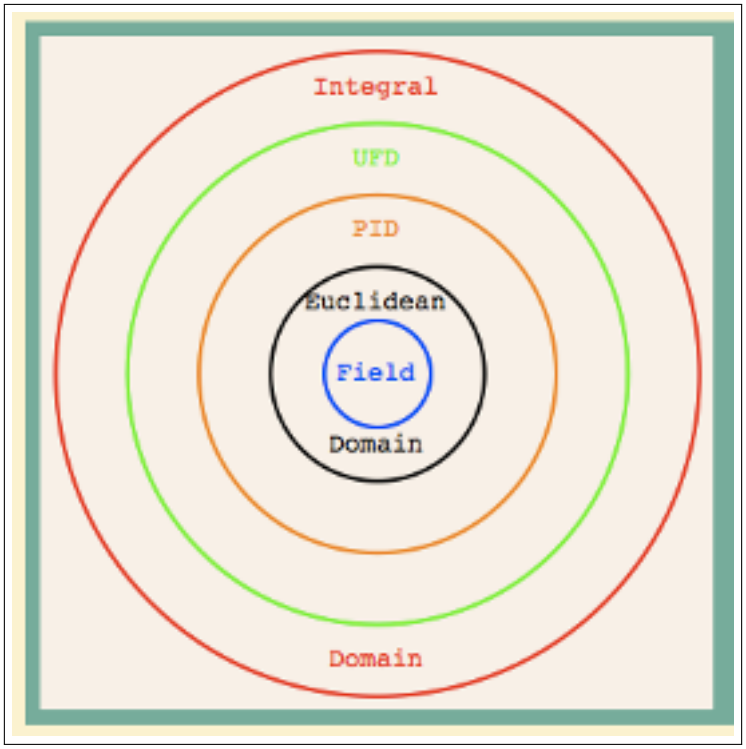
Proposition 2.14 (Irreducibility in PIDs)**.** *In a PID, a non-zero element is prime iff it is irreducible.*

Proposition 2.15 (UFDs)**.** *An UFD is an integral domain in which every element has a unique (!) factorization into irreducibles. In a UFD a non-zero element is prime iff it is irreducible.*
Every PID is a UFD. In particular, every ED is a UFD.

Proposition 2.16 (Facts)**.** *We'll recall that:*

- *PID $\implies$ UFD;*
- *R a UFD $\implies$ $R[x]$ is a UFD;*
- *ED $\implies$ PID, but not every PID is an ED. Euclidean domains possess a division algorithm. Every ED is a UFD.*
- *If F is a field, then $F[x], F[[x]]$ is an ED, and hence a PID (where a PID is a commutative ring).*
- *R an ID $\implies$ $R[x], R[[x]]$ both IDs.*

Let R be a commutative ring. Then **M *is a maximal ideal iff* R/M *is a field.*** *Also, $R[x]/(I) \cong (R/I)[x]$ – and in particular, I prime implies that (I) is prime in $R[x]$. However, it is NOT true that if I is maximal in R then I is maximal in $R[x]$. Finally, if R is a commutative ring, then $R[x]$ is a PID $\iff$ R is a field. If R is commutative, then R is a field iff the only ideals of R are 0 and R itself.*



For $r \in R$, $r \neq 0$ and r not a unit, r is *irreducible* if whenever $r = ab$ with $a, b \in R$ then one of a, b is a unit. A non-zero element $p \in R$ is *prime* if (p) is a prime ideal $\iff$ $p|ab$ implies that $p|a$ or $p|b$. An irreducible element is not necessarily prime: Take $3 \in \mathbb{Z}[\sqrt{-5}]$ and observe that $3 \mid (2+\sqrt{-5})(2-\sqrt{-5}) = 3^2$, but neither of $2 \pm \sqrt{-5}$ is divisible by 3 in R.

Definition 2.17 (Prime ideals)**.** An ideal P is prime if $P \neq R$ and $ab \in P$ implies that $a \in P$ or $b \in P$. **If R is commutative, then P is a prime ideal iff R/P is an integral domain.** *Maximal ideals are prime in commutative rings, though the converse is false.* In general, prime $\implies$ irreducible. In a PID, we have that prime $\iff$ irreducible. Similarly, in a UFD we have that prime $\iff$ irreducible. In $\mathbb{Z}$, maximal ideals are the same as prime ideals. *Every maximal ideal is prime.*

Fact: In a quotient ring, $x_1 + I = x_2 + I$ implies that $x_1 - x_2 \in I$.

Example 2.18 (Fall 2016, #2)**.** Let R be an integral domain containing a field F. Show that if R has finite dimension as a vector space over F, then R is a field.

Example 2.19 (Spring 2014, #4)**.** Let R be a principal ideal domain. Show that if $P \neq \langle 0 \rangle$ is a prime ideal, then P is maximal.

Example 2.20 (Fall 2013, #3)**.** Let I be the ideal (n, x^3+2x+2) in $\mathbb{Z}[x]$. For which n with $1 \leq n \leq 7$ is I a maximal ideal?

Example 2.21 (Notable cases and facts)**.** Collected from various sources:

- The ideal $I := (2, x)$ is *NOT* principal in $\mathbb{Z}[x]$ since $x \notin I$:

$$\begin{aligned}(2, x) &= \{2p(x) + x \cdot q(x) : p, q \in \mathbb{Z}[x]\} \\ &= \{\text{polynomials in } \mathbb{Z}[x] \text{ with even constant term}\}.\end{aligned}$$

  Thus we conclude that $\mathbb{Z}[x]$ is not a Euclidean domain. However, $\mathbb{Q}[x]$ *IS* an ED.

- If the ideal $(a, b) = (d)$ is principal then we can show that $d = \gcd(a, b)$.

- $\mathbb{Z}[\sqrt{-5}]$ is *NOT* a UFD, and hence is *NOT* a PID: $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

- $N(\alpha)$ prime implies that α is irreducible. (**Proof strategy:** Try taking $N(a\imath + b) = a^2 + b^2$, which is a norm an looking for prime factors.)
- $(\mathbb{Z}/p\mathbb{Z})[x]$ is a PID for p prime. However, $\mathbb{Z}[x]/(p)$ is a PID, where $\mathbb{Z}[x]$ is *NOT* a PID.
- $x^2 + 1$ is *NOT* a perfect square in $\mathbb{Z}[x]$, but it is in $\mathbb{Z}/2\mathbb{Z}[x]$.
- If R is an integral domain then $\deg(pq) = \deg(p) + \deg(q)$.
- If R is an integral domain, then the units of $R[x]$ are precisely the units in R.
- R an integral domain $\implies$ $R[x]$ is an integral domain.
- $R[x]$ has zero divisors $\iff$ R has zero divisors.
- $x^2 + 4 \in I^2 = I \cdot I$, but $x^2 + 4$ *cannot* be written as a single product $q(x)p(x)$ in $\mathbb{Z}[x]$.
- $R[x]/(x) \cong R$.
- $\mathbb{Z}[2\imath]$ is an integral domain, but *NOT* a UFD.

Example 2.22 (Characterizations of units and nilpotent elements)**.** Let R be an integral domain and let $f := \sum_{i=0}^{n} a_i x^i \in R[x]$. Then f is *nilpotent* precisely when all of the a_i's are nilpotent, and f is a *unit* precisely when $a_1, a_2, \ldots, a_n$ are nilpotent and a_0 is a unit in R. Let $g := \sum_{i \geq 0} b_i x^i \in R[[x]]$. Then g is *nilpotent* precisely when all of the b_i are nilpotent, and g is a unit whenever a_0 is a unit.

Example 2.23 (Spring 2012, #4)**.** Let R be a commutative ring with identity and let $R^\times$ be the group of invertible elements of R. Prove that $R \setminus R^\times$ is an ideal if and only if R has a unique maximal ideal.

3 IRREDUCIBLE POLYNOMIALS

3.1 Irreducibility criteria

Theorem 3.1 (Gauss' lemma)**.** *Let R be a UFD with field of fractions F, and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then it is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some non-constant $A, B \in F[x]$, then there are non-zero $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ and $p(x) = a(x)b(x)$ in $R[x]$. The contrapositive of Gauss' lemma is also often useful.*

An example gives that $7x$ is reducible in $\mathbb{Z}[x]$ but not in $\mathbb{Q}[x]$ since 7 is a unit in $\mathbb{Q}$.

Proposition 3.2 (Roots and irreducibility)**.** *We have the following two characterizations of reducible polynomials of small degree:*

(1) Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree-1 iff $p(x)$ has a root in F, i.e., $\exists \alpha \in F$ such that $p(\alpha) = 0$.

(2) A polynomial of degree 2 or 3 over a field is reducible iff it has a root in F.

Proposition 3.3 (Rational roots theorem)**.** *Let $p(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial of degree n with integer coefficients. If $r/s \in \mathbb{Q}$ is in lowest terms, and r/s is a root of $p(x)$, then we must have that $r|a_0$ and $s|a_n$, i.e., we have the more useful characterization that if the linear factor $ax + b|p(x)$ for integers a, b, then $a|a_n$ and $b|a_0$. In particular, if $p(x)$ is monic in $\mathbb{Z}[x]$ and $p(d) \neq 0$ for all $d|a_0$, then $p(x)$ has no roots in $\mathbb{Q}$.*

Example 3.4 (Fall 2017, #2)**.** Find a factorization of

$$f(x) = 6x^4 - 4x^3 + 24x^2 - 4x - 8,$$

into prime elements of $\mathbb{Z}[x]$.

Example 3.5 (Spring 2012, #5)**.** Prove from first principles that the polynomial $p(x) = 2x^3 + x + 2$ is irreducible over $\mathbb{Q}[x]$.

Proposition 3.6. *Let I be a proper ideal in the integral domain R, and let $p(x)$ be non-constant and monic in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.*

Theorem 3.7 (Eisenstein for PIDs)**.** *Let P be a prime ideal of the integral domain R, and let $f(x) = x^n + \cdots + a_0$ be a polynomial in $R[x]$ for some $n \geq 1$. Suppose $a_{n-1}, \ldots, a_1, a_0$ are all elements of P and suppose that $a_0 \notin P^2$. Then $f(x)$ is irreducible in $R[x]$.*

Theorem 3.8 (Eisenstein for $\mathbb{Z}$)**.** *Let $p \in \mathbb{Z}$ be prime and let $f(x) = x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Suppose that $p|a_i$ for all $i = 0, 1, \ldots, n-1$, but that $p^2 \nmid a_0$. Then $f(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ (by Gauss' lemma). This is the same as the previous theorem for the prime ideals (p) (p prime) of the integral domain $\mathbb{Z}$.*

Example 3.9. Consider the following:

(a) Prove that $x^7 + 48x - 24$ is irreducible in $\mathbb{Q}[x]$.

(b) Show that $f(x, y) = x^4 + x^3y^2 + x^2y^3 + y$ is irreducible in $\mathbb{Q}[x, y]$.

Proof of (a). By Eisenstein for the polynomial ring $\mathbb{Z}[x]$ with the prime ideal (3), we find that the polynomial is irreducible over $\mathbb{Z}[x]$: the polynomial is monic with $3|48$, $3|(-24)$, and $3^2 \nmid (-24)$. By the contrapositive to Gauss' lemma, the polynomial is also irreducible over $\mathbb{Q}[x]$. □

Proof of (b). We apply Eisenstien to $\mathbb{Q}[x, y] = \mathbb{Q}[y][x]$ for the prime ideal $(y) \in \mathbb{Q}[y]$, Indeed, (y) is a prime ideal as $\mathbb{Q}[y]/(y) \cong \mathbb{Q}$ is a field and hence an integral domain. Moreover, f is clearly monic with all non-leading terms divisible by y, and with constant term not divisible by y^2. □

Example 3.10. Another example which implicitly uses Eisenstein's criterion in the integer polynomial case shows that the following polynomial is irreducible whenever p is a prime integer:

$$\frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2} + \cdots + \frac{p(p-1)}{2}x + p \in \mathbb{Z}[x].$$

Example 3.11 (Fall 2018, #7)**.** Prove that $f(x) = x^4 + 1$ is reducible modulo every prime p, but irreducible in $\mathbb{Q}[x]$.

3.2 Towards field theory

Proposition 3.12. *The maximal ideals in $F[x]$ for F a field are the ideals $(f(x))$ generated by irreducible polynomials in F.*

Proposition 3.13. *Let $g(x)$ be a non-constant monic element of $F[x]$ and let $g(x) = f_1(x)^{n_1} \cdots f_k(x)^{n_k}$ be its factorization into distinct irreducibles. Then*

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times \cdots \times F[x]/(f_k(x)^{n_k}).$$

Notice that for F a field, $F[x]/\langle x \rangle \cong F[[x]]/\langle x \rangle \cong F$.

Example 3.14. We have that $\mathbb{C} \cong \mathbb{R}/(x^2 + 1)$ and that $K := \mathbb{Q}/(x^2 + 1) \cong \mathbb{Q}(\imath)$.

Example 3.15 (Fall 2014, #5)**.** Let $f(X) = (X^7 - 1)/(X - 1) = X^6 + X^5 + \cdots + 1$. Prove that f is irreducible over $\mathbb{F}_3$, but not over $\mathbb{F}_7$.

4 FIELD THEORY

4.1 Basics and definitions

The *characteristic* of a field F is either zero (no such integer exists for many infinite fields) or some prime p: $\text{ch}(F) = 0, p$. For finite fields, the order of the field $\mathbb{F}$ is always some power of a prime p^n. If $\phi : F \to F'$ is a homomorphism *of fields*, then either $\phi \equiv 0$ is the trivial homomorphism, or ϕ is necessarily injective. The ideal $(p(x))$ is **maximal** when $p(x)$ is irreducible over F. Let $F \subseteq K \subseteq L$ be fields. Then $[L : F] = [L : K] \cdot [K : F]$.

Example 4.1 (Spring 2016, #8)**.** Let p be prime and set $q = p^n$ for some positive integer n. Show that the map $x \mapsto x^p$ is an automorphism on $\mathbb{F}_q$ to itself. Describe all automorphisms on $\mathbb{F}_q$.

Example 4.2 (Fall 2014, #3)**.** Let R, S be commutative rings with 1, and let $f : R \to S$ be a ring homomorphism. Prove that if R is a field, then either f is injective of $S = 0$.

Definition 4.3 (Field extensions)**.** If the field K is an extension of the field F, written K/F for K a *field extension* of F, then we write $[K : F] = \dim_F(K)$ as the dimension of K as a vector space over F. The extension $K := F(\alpha)$ is *simple* and the element α is a *primitive element* for the extension. The element $\alpha \in K$ is said to be *algebraic over* F is α is the root of a non-zero polynomial $f(x) \in F[x]$ with coefficients in F. Suppose that $K_1, K_2 \subseteq K$ are subfields. Then the *composite field*, K_1K_2, is the smallest subfield of K containing both K_1 and K_2. In such a case, we have that $[K_1K_2 : K] \leq [K_1 : K] \cdot [K_2 : K]$.

If α, β are both algebraic over F, then so are $\alpha \pm \beta$, $\alpha\beta$, α/β (for $\beta \neq 0$), and α^{-1} (for $\alpha \neq 0$).

Theorem 4.4 (Important Characterizations When Adjoining Primitive Elements)**.** *Let F be a field and $p(x) \in F[x]$ be irreducible. Suppose that K is an extension of F containing a root α of $p(x)$ and let $F(\alpha)$ denote the subfield of K generated by α over F. Then*

$$F(\alpha) \cong F[x]/(p(x)).$$

A corollary of this result is that if $\deg(p(x)) = n$*, then*

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in F\} \subseteq K.$$

The roots of an irreducible polynomial $p(x)$ over F are algebraically indistinguishable in that the fields obtained by adjoining any one root of the polynomial to F are all isomorphic.

Definition 4.5 (Minimal polynomials)**.** A polynomial $f(x) \in F[x]$ has α as a root iff $m_{F,\alpha}(x) \mid f(x)$ in $F[x]$. A *monic* polynomial over F with α as a root is the *minimal polynomial* for α over F iff it is irreducible over F. Let $m_\alpha(x)$ denote the minimal polynomial of α over F. Then $F(\alpha) \cong F[x]/(m_\alpha(x))$ and in particular, $\boxed{[F(\alpha) : F] = \deg(m_\alpha(x)) = \deg_F(\alpha)}$.

Example 4.6 (Fall 2016, #5)**.** An *algebraic integer* is the solution to a monic polynomial with coefficients in $\mathbb{Z}$.

(a) Show that α is an algebraic integer if and only if $\{1, \alpha, \alpha^2, \ldots\}$ generates a finite rank $\mathbb{Z}$-module.

(b) Let α be an algebraic integer and let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a monic polynomial with coefficients in $\mathbb{Z}$ which has α as a root and which is irreducible in $\mathbb{Z}[x]$. Let $R := \mathbb{Z}[\alpha]$. Prove that α is a unit in R if and only if $a_0 = \pm 1$. (HINT: Consider $1/p(x)$.)

Example 4.7 (Spring 2012, #6)**.** Let L/K be a finite extension of fields and suppose $a, b \in L$ are elements such that $[K(a) : K] = 3$ and $[K(b) : K] = 2$. What are the possibilities for $[K(a + b) : K]$? Prove that your answer is correct.

Example 4.8 (Fall 2012, #8)**.** Let $\alpha := \sqrt{5}$ and $\beta := \sqrt[3]{2}$.

(a) Prove that the degree of the field extension $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ is 6;

(b) Prove that the degree of the field extension $\mathbb{Q}(\alpha + \beta)/\mathbb{Q}$ is 6;

(c) Find the minimal polynomial of $\alpha + \beta$ over $\mathbb{Q}$.

Example 4.9. Let $K := \mathbb{F}_2 \cong \mathbb{Z}/2\mathbb{Z}$ and set $g(x) = x^2 + x + 1$, which is irreducible in $\mathbb{F}_2(x)$. Let $L := \mathbb{F}_2[x]/(g(x))$. Then L/K has degree 2 and $L = \{a + b\theta : a, b \in \mathbb{F}_2\}$ where $\theta^2 = \theta + 1$.

Definition 4.10 (Frobenius map)**.** If K is a field of characteristic p, then the map $\varphi(x) \mapsto x^p$ is an injective (surjective) map from $K \to K$.

Example 4.11 (Spring 2017, #2)**.** Consider the polynomial

$$f(x) = \frac{x^{23} - 1}{x - 1} = \sum_{n=0}^{22} x^n.$$

Determine the number of irreducible factors of $f(x)$ over (1) $\mathbb{Q}$; (2) $\mathbb{F}_2$; and (3) $\mathbb{F}_{2048}$.

Example 4.12 (Spring 2015, #1)**.** Complete each of the following subproblems:

(a) Prove that the polynomial $f(X) = X^6 + X^3 + 1 = (X^9 - 1)/(X^3 - 1)$ is irreducible over $\mathbb{Q}$;

(b) Find the factorization of $f(X)$ over $\mathbb{F}_{19}$.

4.2 Splitting fields of polynomials

Definition 4.13. The extension field K/F is a *splitting field* for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors in $K[x]$ and does not split completely into linear factors over any subfield of K containing F. By a key theorem, we know that if $f(x) \in F[x]$ then there exists an extension field K/F which is the splitting field for $f(x)$. A splitting field of a polynomial of degree n over F is of degree ***at most*** **n!** over F.

Example 4.14 (Splitting fields of special polynomials)**.** First, the splitting field for $f(x) = (x^2 - 2)(x^2 - 3)$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and is hence of degree 4 over $\mathbb{Q}$. Subfields of degree 2 over $\mathbb{Q}$ are given by: $\mathbb{Q}(\alpha)$ for $\alpha \in \{\sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Second, since

$$x^4 + 4 = (x^2 + 2)^2 - 4x^2 = (x^2 + 2x + 2)(x^2 - 2x + 2),$$

the splitting field of this polynomial over $\mathbb{Q}$ is $\mathbb{Q}(\imath)$ which satisfies only $[\mathbb{Q}(\imath) : \mathbb{Q}] = 2$, despite being a polynomial of degree 4. Additionally, the polynomial splits as $x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2})$, so its splitting field is $\mathbb{Q}(\sqrt[3]{2}, \omega)$, which is a degree-6 extension over $\mathbb{Q}$.

Example 4.15 (Spring 2014, #3)**.** Find the degree of the splitting field of the polynomial $f(x) = x^6 - 7$ over each of the following fields:

(a) $\mathbb{Q}$;

(b) $\mathbb{Q}(\zeta_3)$, where ζ_3 is a primitive 3^{rd} root of unity;

(c) $\mathbb{F}_3$ (the finite field with 3 elements).

Example 4.16 (Spring 2012, #7)**.** What is the cardinality of the splitting field of $f(x) = x^3 - 1$ over $\mathbb{F}_{11}$? Same question over $\mathbb{F}_{49}$.

Example 4.17 (Cyclotomic fields and splitting fields of $x^n - 1$)**.** First, we require some notation and definitions for the *n^{th} roots of unity* when $n \geq 2$. A generator for the *cyclic* group of all n^{th} roots of unity is a *primitive n^{th} root of unity*. Writing $\zeta_n := e^{2\pi\imath/n}$ there are exactly $\phi(n)$ primitive roots and these are of the form ζ_n^a for $1 \leq a < n$ where $\gcd(a, n) = 1$. We define $\mathbb{Q}(\zeta_n)$ to be the *cyclotomic field of the n^{th} roots of unity*. It follows that $\mathbb{Q}(\zeta_n)$ is the splitting field of $f(x) = x^n - 1$ over $\mathbb{Q}$. For p prime ζ_p is a root of the irreducible polynomial

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

which then in turn implies that $\Phi_p(x)$ is the minimal polynomial of ζ_p over $\mathbb{Q}$. Then we see that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. More generally, $\boxed{[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)}$.

Example 4.18 (The spliting field of $x^p - 2$ for p prime)**.** See also page 541. The splitting field of $x^p - 2$ is $\mathbb{Q}(\zeta_p, \sqrt[p]{2})$, which is a degree $p(p-1)$ extension over $\mathbb{Q}$.

Definition 4.19 (Separability of polynomials)**.** A polynomial $f(x) \in F[x]$ is called $\boxed{\textbf{\textit{separable}}}$ **(over F) if it has no multiple roots in F.** Otherwise the polynomial is *inseparable*. For example, the polynomial $f(x) = x^2 - t$ is irreducible over $\mathbb{F}_2$, but is inseparable over $\mathbb{F}_2(t)$ since its two roots $\pm\sqrt{t}$ are indistinguishable in this field. Also, this polynomial is inseparable since $D_x[f] = 0$ in $\mathbb{F}_2$ and $\sqrt{t}$ is algebraic over $\mathbb{F}_2$.

Proposition 4.20 (Characterizations of separability by the derivative)**.** *A polynomial $f(x)$ has a multiple root α iff α is also a root of $D_x[f(x)]$, i.e., $f(x)$ and $D_x[f(x)]$ are both divisible by the minimal polynomial for α. In particular, $f(x)$ is separable iff it is relatively prime to its derivative:* $\gcd(f, D_x[f]) = 1$.

Example 4.21 (Fall 2012, #6)**.** Let $f(x) \in \mathbb{Q}[x]$ be a rational polynomial irreducible over $\mathbb{Q}$. Prove that $f(x)$ has no multiple (repeated) roots in $\mathbb{C}$.

Corollary 4.22 (Irreducibility and separability)**.** ***Every $\boxed{\textbf{\textit{irreducible}}}$ polynomial over a field of characteristic 0 (for example, $\mathbb{Q}$) is separable.*** *A polynomial over such a field is separable iff it is the product of distinct irreducible polynomials over F. We also can prove that every irreducible polynomial over a finite field is separable. A polynomial in $\mathbb{F}[x]$ is separable iff it is the product of distinct irreducible polynomials in $\mathbb{F}[x]$.*

If F is a field of characteristic p, then for any $a, b \in F$ we have that *(i)* $(a + b)^p = a^p + b^p$; and *(ii)* $(ab)^p = a^p b^p$. One corollary of this fact is that if $\mathbb{F}$ is a finite field of characteristic p then every element of $\mathbb{F}$ is a p^{th} power (notationally: $\mathbb{F} = \mathbb{F}^p$).

4.3 More on cyclotomic polynomials and their extensions

Definition 4.23. Let μ_n denote the group of n^{th} roots of unity over $\mathbb{Q}$. Then we have that $\boxed{\mu_n \cong \mathbb{Z}/n\mathbb{Z}}$ where the group operations are $*$ in both, i.e., μ_n is a *multiplicative group*. The *cyclotomic polynomials* are defined as the first sequence:

$$\begin{aligned}\Phi_n(x) &= \prod_{\substack{1\le a<n\\(a,n)=1}} (x-\zeta_n^a),\ \deg(\Phi_n(x)) = \phi(n)\\ &= \prod_{d|n}(1-x^{n/d})^{\mu(d)}\\ x^n-1 &= \prod_{\zeta^n=1}(x-\zeta) = \prod_{d|n}\Phi_d(x).\end{aligned}$$

For example, $\Phi_6(x) = x^2 - x + 1$, $\Phi_p(x) = x^{p-1} + \cdots + x + 1$, and we have that $\Phi_{2p}(x) = \Phi_p(-x)$ for prime p. The cyclotomic polynomial $\Phi_n(x)$ is seen to be an irreducible monic polynomial in $\mathbb{Z}[x]$ of degree $\phi(n)$. Then as a corollary of this fact, we have that both $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, and $\Phi_n(x)$ must be the minimal polynomial of any n^{th} root of unity.

As an example (following from the preceeding section), we find that $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\imath, \sqrt{2})$ since $\zeta_8 + \zeta_8^7 = \sqrt{2}$ (see page 555). Note that in general, we have that $\zeta_p + \zeta_p^{p-1} = 2 \cdot \cos(2\pi/p)$. Also, $\zeta_8^2 = \frac{\sqrt{2}}{2}(1 + \imath)$.

5 GALOIS THEORY

Definition 5.1. We have some new uses of previous notation:

(1) An isomorphism $\sigma : K \to K$ is an *automorphism* of K. The collection of automorphisms of K is the group $\mathrm{Aut}(K)$ which is a group under composition of functions and $\mathrm{Aut}(K/F)$ (see below) is an important subgroup.

(2) The element $\sigma \in \mathrm{Aut}(K)$ *fixes* $\alpha \in K$ if $\sigma\alpha = \alpha$. If $F \subseteq K$ is a subfield and σ fixes all $\beta \in F$, then we say that σ *fixes* the field F.

(3) Let $\mathrm{Aut}(K/F)$ denote the collection of $\sigma \in \mathrm{Aut}(K)$ which fix F.

(4) If $H \leq \mathrm{Aut}(K)$, then the subfield of K fixed by all of the elements of H is called the *fixed field of* H.

Proposition 5.2. *Let K/F be a field extension and suppose that $\alpha \in K$ is algebraic over F. Then for any $\sigma \in \mathrm{Aut}(K/F)$, $\sigma\alpha$ is a root of the minimal polynomial of α over F, i.e., $\mathrm{Aut}(K/F)$ only permutes the roots of irreducible polynomials in $F[x]$.*

Proposition 5.3. *Let E be the splitting field of $f(x) \in F[x]$ over F. Then $|\mathrm{Aut}(E/F)| \leq [E : F]$ with equality only if $f(x)$ is separable over F.*

Definition 5.4 (Galois groups and Galois extensions)**.** We say that K is *Galois over* F, and write that K/F is a *Galois extension*, if $|\mathrm{Aut}(K/F)| = [K : F]$. If K/F is Galois, then $\mathrm{Aut}(K/F)$ is the *Galois group* of K/F, also denoted by $\mathrm{Gal}(K/F)$. *If K is the splitting field over F of a separable polynomial $f(x) \in F[x]$, then K/F is Galois.* Moreover, if $f(x) \in F[x]$ is separable, then the *Galois group of $f(x)$ over F* is the Galois group of the splitting field of $f(x)$ over F.

Alternately: A *Galois extension* H/K is an algebraic extension that is both *normal* and *separable*. In a normal extension H/K, every polynomial that is irreducible over K is either irreducible over H or splits into linear factors over H. A polynomial f is again separable in H if it has only distinct roots in H iff its formal derivative $D_x[f]$ does not have any roots in H.

5.1 Some preliminary and motivating examples

Example 5.5. The field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is Galois over $\mathbb{Q}$ since it is the splitting field of $f(x) = (x^2 - 2)(x^2 - 3)$. Any automorphisms $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ are completely determined by their actions on the generators $\sqrt{2}$ and $\sqrt{3}$: $\sqrt{2} \to \pm\sqrt{2}$ and $\sqrt{3} \to \pm\sqrt{3}$. In particular, we define

$$\sigma : \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{3} \to \sqrt{3} \end{cases}$$

$$\tau : \begin{cases} \sqrt{2} \to \sqrt{2} \\ \sqrt{3} \to -\sqrt{3}, \end{cases}$$

or stated more explicitly as the mappings

$$\sigma : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$
$$\tau : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}.$$

Then as we can easily compute,

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}.$$

Moreover, there is a distinctive pattern to the subgroups of this Galois group and their corresponding fixed fields shown for illustration below:

Subgroup	**Fixed field**
$\{1\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\{1, \sigma\}$	$\mathbb{Q}(\sqrt{3})$
$\{1, \sigma\tau\}$	$\mathbb{Q}(\sqrt{6})$
$\{1, \tau\}$	$\mathbb{Q}(\sqrt{2})$
$\{1, \sigma, \tau, \sigma\tau\}$	$\mathbb{Q}$

Example 5.6. The splitting field of $x^3 - 2$ over $\mathbb{Q}$ is of degree 6 since

$$x^3 - 2 = 0 \implies x = \sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}, \quad \text{for } \rho \equiv \zeta_3 = \frac{-1 + \sqrt{-3}}{2}.$$

Hence, the splitting field of this polynomial is $\mathbb{Q}(\sqrt[3]{2}, \rho \cdot \sqrt[3]{2})$. Notice that there are technically *nine* possbilities for automorphisms permuting these roots, but not all of these turn out to be automorphisms of the full field. To simplify our considerations, we can use our notation for the generators $\sqrt[3]{2}$ and ρ. Then any σ in the Galois group maps $\sqrt[3]{2} \to \{\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}\}$ and/or $\rho \to \{\rho, \rho^2 = -(1 + \rho)\}$ (i.e., $\rho^2 + \rho + 1 = 0$). In particular, we define

$$\sigma : \begin{cases} \sqrt[3]{2} \to \rho\sqrt[3]{2} \\ \rho \to \rho \end{cases}$$
$$\tau : \begin{cases} \sqrt[3]{2} \to \rho\sqrt[3]{2} \\ \rho \to \rho^2 = -(1 + \rho) \end{cases}.$$

Then as we can compute, $\boxed{\sigma^3 = \tau^2 = 1}$, which implies together with the observation that $\sigma\tau = \tau\sigma^2$, that

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong S_3.$$

Example 5.7 (Non-Galois extensions)**.** First, we see that $\mathbb{Q}(\sqrt[4]{2})$ is ***NOT*** Galois over $\mathbb{Q}$ since σ sends $\sqrt[4]{2} \to \{\pm\sqrt[4]{2}, \pm\imath \cdot \sqrt[4]{2}\}$ – and only two of these possibilities are actually elements of the field itself. We do however note that this degree-4 extension corresponds to the composition of the two degree-2 extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. In these two sub-cases, *both* of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ *are* in fact Galois extensions since they are **quadratic extensions** (**splitting fields of some** $x^2 - D$). Secondly, we note that the inseparable extension $\mathbb{F}_2(x)/\mathbb{F}_2(t)$ corresponding to the splitting field of the polynomial $f(x) = x^2 - t$ is *NOT* Galois since this extension can only possibly have the trivial automorphism.

Example 5.8 (**Important**)**.** The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois since $\mathbb{F}_{p^n}$ is the splitting field over $\mathbb{F}_p$ of the separable polynomial $x^{p^n} - x$. In this case, the automorphism $\sigma_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $\alpha \mapsto \alpha^p$ is surjective. We can also deduce that $\sigma_p^n = 1$, so that $\boxed{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \text{ is cyclic}}$ of order n and hence isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Example 5.9 (Simplifiying Observations by Hamed and Daniel, Fall 2018)**.** We have the following isomorphism properties of special Galois groups:

- $\text{Gal}(\mathbb{Q}(\sqrt[4]{2}, \imath)/\mathbb{Q}) \cong \mathbb{Z}_4 \times \mathbb{Z}_2$;
- $\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

5.2 The fundamental theorem of Galois theory

Theorem 5.10 (Key Result)**.** *Let $G := \{1 = \sigma_1, \ldots, \sigma_n\}$ be the subgroup $G \leq \text{Aut}(K)$ with fixed field F. Then $[K : F] = n = |G|$. An important corollary of this result is that* ***the extension*** $\mathbf{K/F}$ ***is Galois iff it is the splitting field of some separable polynomial over*** $\mathbf{F}$***.***

Theorem 5.11. *Let K/F be a Galois extension and set $G := \text{Gal}(K/F)$. The fundamental theorem of Galois theory states that there is a bijective correspondence between the subfields E of K containing F $(K - E - F)$ and the subgroups $H \leq G$ $(1 - H - G)$. This bijection is given by the correspondences $E \to \{$The elements of G fixing $E\}$ and $\{$The fixed field of $H\} \leftarrow H$. The exact statement of this theorem is reproduced from Dummit and Foote (page 574) below.*

Theorem 14. *(Fundamental Theorem of Galois Theory)* Let K/F be a Galois extension and set $G = \text{Gal}(K/F)$. Then there is a bijection

$$\left\{ \begin{array}{c} \text{subfields } E \\ \text{of } K \\ \text{containing } F \end{array} \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subgroups } H \\ \text{of } G \end{array} \begin{array}{c} 1 \\ | \\ H \\ | \\ G \end{array} \right\}$$

given by the correspondences

$$E \longrightarrow \left\{ \begin{array}{c} \text{the elements of } G \\ \text{fixing } E \end{array} \right\}$$

$$\left\{ \begin{array}{c} \text{the fixed field} \\ \text{of } H \end{array} \right\} \longleftarrow H$$

which are inverse to each other. Under this correspondence,

(1) (inclusion reversing) If E_1, E_2 correspond to H_1, H_2, respectively, then $E_1 \subseteq E_2$ if and only if $H_2 \leq H_1$

(2) $[K : E] = |H|$ and $[E : F] = |G : H|$, the index of H in G:

$$\begin{array}{ll} K & \\ | & \} \quad |H| \\ E & \\ | & \} \quad |G : H| \\ F & \end{array}$$

Example 5.12. We have now two good ways to see that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. The first way is to look at conjugates of the roots of $\alpha = \sqrt{2} + \sqrt{3}$ and deduce that its minimal polynomial is $f(x) = x^4 - 10x^2 + 1$. This minimal polynomial is irreducible where $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ is clearly a subfield of the Galois extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Thus by order considerations these two fields must be equal. The second way is a consequence of the fundamental theorem. Namely, only the automorphism $1 \in \{1, \sigma, \tau, \sigma\tau\}$ fixes $\sqrt{2} + \sqrt{3}$, so it must be the case that the fixing group for this field is the same as that for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

5.3 Finite fields

We have some basic facts about finite fields and their Galois groups and extensions:

- If $[\mathbb{F} : \mathbb{F}_p] = n$, then $|\mathbb{F}| = p^n$ and $\mathbb{F}$ is isomorphic to the splitting field of the polynomial $f(x) = x^{p^n} - x$.
- We have that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle \cong \mathbb{Z}/n\mathbb{Z}$. Moreover, since the Galois group here is abelian, every subgroup of it is normal, which then implies that each of the subfields $\mathbb{F}_{p^d}$ for $d \mid n$ are Galois over $\mathbb{F}_p$.

Proposition 5.13 (Distinct irreducibles over finite fields)**.** *The polynomial $x^{p^n} - x$ is precisely the product of all the distinct irreducible polynomials in $\mathbb{F}_p[x]$ of degree d where d runs through all the divisors of n. We then have the following consequences of this observation:*

- *The irreducible quadratics over $\mathbb{F}_2$ are the divisors of $(x^4 - x)/(x(x-1)) = x^2 + x + 1$.*
- *The irreducible cubics over $\mathbb{F}_2$ are divisors of $(x^8 - x)/(x(x-1)) = x^6 + x^5 + \cdots + x + 1 = (x^3 + x + 1)(x^3 + x^2 + 1)$.*
- *We have that $\boxed{\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/(f(x)) \text{ for } f(x) \text{ irreducible}}$ of degree n. For example, $\mathbb{F}_2[x]/(x^4 + x + 1) \cong \mathbb{F}_2[x]/(x^4 + x^3 + 1) \cong \mathbb{F}_{16}$.*

5.4 Special Galois groups

Regarding cyclotomic extensions and abelian extensions over $\mathbb{Q}$, we first have that $\boxed{\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times}$, where we have the correspondence $a \pmod n \mapsto \sigma_a$ for $\sigma_a(\zeta_n) := \zeta_n^a$. An interesting case gives us the first example so far of an abelian extension of degree-4: $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ has the *cyclic* Galois group $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$.

Corollary 5.14. *Suppose that we have K_1, K_2 both Galois extensions of F with $K_1 \cap K_2 = F$. Then*

$$\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

Let $n = p_1^{a_1} \cdots p_k^{a_k}$ denote the factorization of n into distinct prime powers. Then the cyclotomic fields $\mathbb{Q}(\zeta_{p_i^{a_i}})$ intersect only in the field $\mathbb{Q}$ for $i = 1, 2, \ldots, k$, and their composite field is precisely the cyclotimic field $\mathbb{Q}(\zeta_n)$. Hence, we obtain that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k^{a_k}})/\mathbb{Q}).$$

Equivalently, we obtain our previous result from the Chinese remainder theorem which states that

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times.$$

5.5 Galois groups of polynomials

Theorem 5.15 (Symmetric Galois groups and general polynomials)**.** *For indeterminates $x_1, x_2, \ldots, x_n$, the general polynomial*

$$f(x) = (x - x_1) \cdots (x - x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n,$$

over the field $F(s_1, s_2, \ldots, s_n)$ is separable with Galois group of S_n.

Definition 5.16 (Discriminants of polynomials)**.** The *discriminant* of the roots x_i of $f(x)$ is the square product:

$$D := \prod_{i<j} (x_i - x_j)^2, \ \sqrt{D} = \prod_{i<j} (x_i - x_j).$$

Properties of discriminants.

- We have that $D = 0$ iff $f(x)$ is *NOT* separable, i.e., when the roots $x_1, x_2, \ldots, x_n$ are not distinct.
- D is symmetric in the roots of $f(x)$ and is hence fixed by all of the automorphisms in the Galois group of $f(x)$.
- Since $D \in F$ and $\sqrt{D} = \prod_{i<j}(x_i - x_j)$, $\sqrt{D}$ is *always* contained in the splitting field for $f(x)$.

Proposition 5.17. *The Galois group of $f(x) \in F[x]$ is a subgroup of A_n iff the discriminant $D \in F$ is the square of an element of F.*

Polynomials of degree 2

Here, by renormalization if necessary, we have that $f(x) = x^2 + bx + c$ and $\boxed{D = b^2 - 4c}$.

- The polynomial f is separable iff $b^2 - 4c \neq 0$ (i.e., no repeated roots in this case).
- The Galois group of f is a subgroup of $S_2 \cong \mathbb{Z}/2\mathbb{Z}$, the cyclic group of order 2. This Galois group is trivial ($\cong A_2$) iff $b^2 - 4c$ is a rational square.
- If the polynomial f is irreducible, the the Galois group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ since the splitting field is the quadratic extension $F(\sqrt{D})$.

Polynomials of degree 3

Here, we consider the polynomial $f(x) = x^3 + ax^2 + bx + c$ under the change of variable $x \mapsto y - a/3$ to obtain the polynomial $g(y) = y^3 + py + q$. Under this substitution, the splitting fields of both f and g are the same and these two polynomials have the same discriminant $D = -(4p^3 + 27q^2)$.

(a) If g is reducible: *(i)* $1, 1, 1$ leads to the trivial Galois group; and *(ii)* 1, irreducible of degree 2 leads to a Galois group of degree 2.

(b) If g is irreducible:

- A root of $f(x)$ generates an extension of degree-3 over F so that the degree of the splitting field over F is divisible by 3.
- The Galois group is a subgroup of S_3 (either A_3 or all of S_3 itself).
- The Galois group is $\boxed{A_3 \cong \mathbb{Z}/3\mathbb{Z}}$ iff D is square in F.
- If $D = h^2$ for some $h \in F$, then the splitting field is obtained by adjoining any single root of f to F. The resulting field is Galois over F of degree 3 with a cyclic group of order 3 as its Galois group.
- If D is not square in F, then the splitting field of $f(x)$ is of degree 6 over F, and hence $\boxed{F(\vartheta, \sqrt{D})}$ for any single root ϑ of $f(x)$. The resulting extension is Galois over F with Galois group S_3.

Polynomials of degree 4

Here we have $f(x) = x^4 + ax^3 + bx^2 + cx + d$ and then $g(y) = y^4 + py^2 + qy + r$ under the change of variable $x \mapsto y - a/4$. Let the roots of $g(y)$ be $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, and let G denote the Galois group for the splitting field of $g(y)$. We are primarily concerned with the case where $g(y)$ is reducible:

- Case degree $1, 3$ split: Then G is the Galois group of the cubic from above.

- Case degree 2, 2 split (both irreducible): Then the splitting field is the extension $F(\sqrt{D_1}, \sqrt{D_2})$ where D_1, D_2 are the two discriminants of the irreducible quadratics.
- In the last case, if $D_1 = h^2 \cdot D_2$ for some $h \in F$, then this extension is quadratic and $G \cong \mathbb{Z}/2\mathbb{Z}$.

5.6 Practice problems

Example 5.18 (Spring 2018, #5)**.** Compute the Galois group of $x^4 - x^2 - 6$ over $\mathbb{Q}$.

Example 5.19 (Fall 2017, #4)**.** Find all primitive elements in the field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Justify your answer.

Example 5.20 (Fall 2017, #8)**.** Show that $f(x) = x^3 - 3x - 1$ is an irreducible element of $\mathbb{Z}[x]$. Compute the Galois group of the splitting field of f over $\mathbb{Q}$ and over $\mathbb{R}$.

Example 5.21 (Spring 2017, #6)**.** Find the Galois group of the splitting field of the polynomial $f(x) = x^3 - x + 1$ over each of the following fields:

1. $\mathbb{F}_2$;
2. $\mathbb{R}$; and
3. $\mathbb{Q}$.

Example 5.22 (Spring 2016, #1)**.** Let $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. List all intermediate fields K such that $\mathbb{Q} \subset K \subset F$, and find all elements $\alpha \in F$ such that $F = \mathbb{Q}(\alpha)$.

Example 5.23 (Spring 2015, #3)**.** Let K be the splitting field over $\mathbb{Q}$ for an *irreducible* polynomial of degree 3. What are the possibilities for $[K : \mathbb{Q}]$? Give an example to show that each possibility does occur.

Example 5.24 (New Algebra Comp Exam Problems, #4)**.** Find the Galois group of the splitting field for $f(x) = x^3 - 7$ over $K = \mathbb{Q}(\sqrt{-3})$.

6 SOLUTIONS TO OTHER ASSIGNED PROBLEMS

Example 6.1 (Spring 2016, # 5)**.** Is the ring $\mathbb{Z}[2\imath]$, where $(2\imath)^2 = -4$, a PID? If not, give an example of a non-principal ideal.

Proof. Let $R := \mathbb{Z}[2\imath]$ be the base ring and let the ideal $I := (2, 2\imath)$ of R. We show that this ideal is not principal. Notice that $2, 2\imath$ do not divide each other in R. Suppose that $(2, 2\imath) = (f)$ for some $f \in R$. Then $2, 2\imath \in R$ implies that $2 = af$ and $2\imath = bf$ for some $a, b \in R$. Consider the non-negative, multiplicative norm $\phi : R \to \mathbb{R}_{\geq 0}$ defined by $\phi(a + b\imath) := a^2 + b^2$. Then we can compute that

$$\begin{aligned} 4 &= \phi(2) = \phi(a)\phi(f) \\ 4 &= \phi(2\imath) = \phi(b)\phi(f), \end{aligned}$$

which implies that $\phi(f) \mid 4$, or that $\phi(f) \in \{1, 2, 4\}$, i.e., $f \in \{\pm 1, \pm 2, \pm 2\imath\}$. To simplify cases, we will symmetrically assume (WLOG) that $f \in \{1, 2, 4\}$. We consider the following cases:

- If $\phi(f) = 1$, then $(2, 2\imath) = R$, which is a contradiction because, for example, $1 \notin (2, 2\imath)$.
- If $\phi(f) = 2$, we arrive at a contradiction because there are no elements in R of norm 2.
- If $\phi(f) = 4$, then $f = \pm 2, \pm 2\imath$ (where we will assume that $f = 2$ or $f = 2\imath$ for simplicity of exposition).

Let's suppose that $(2, 2\imath) = (2)$. Then $2\imath = 2g$ for some $g \in R$ which implies that $g = \imath$, a contradiction since $\imath \notin R$. If on the other hand, $(2, 2\imath) = (2\imath)$, then for some $h \in R$ $2 = 2\imath \cdot h$, which is the same as $h = -\imath \notin R$, another contradiction. Hence R is not a PID. □

Example 6.2 (Spring 2016, # 7)**.** Let R be an integral domain. Show that every automorphism of $R[x]$ that is identity on R is given by $x \mapsto ax + b$ where $a, b \in R$ and a is a unit.

Proof. Let $\sigma \in \mathrm{Aut}(R[x])$ be such that $\sigma(x) = a_n x^n + \cdots + a_1 x + a_0$ for $a_n \neq 0$. Then for any degree-m element $g(x) := b_m x^m + \cdots + b_1 x + b_0$ with $m \geq 1$ we have that $\sigma(g(x)) = a_n b_m^n x^{mn} +$(lower order terms), which is itself a polynomial of degree $mn \geq n$ with non-zero leading coefficient $a_n b_m^n$. The leading coefficient is again non-zero since R is an integral domain. For the polynomial x to be in the image of σ (which it must be since σ is an automorphism of $R[x]$), we are going to need to require that $n = 1$ and that a_1 is a unit. □

Example 6.3 (Fall 2016, # 3)**.** Let R be an integral domain. Suppose that r is a non-zero, non-unit, irreducible element of R, and let $\langle r \rangle$ denote the ideal generated by r.

(a) If R is a UFD, is $R/\langle r \rangle$ also a UFD?

(b) If R is a PID, is $R/\langle r \rangle$ also a PID?

Proof. For (a): *NO.* As a counter example, let $R := \mathbb{C}[x, y, z]$ and let $r := xy - z^2$. Then R is an integral domain since $\mathbb{C}$ is a field and r is irreducible since otherwise $xy - z^2$ would factor as a homogeneous polynomial of degree-1. By our inspection this is not possible. It follows that $x \cdot y = z \cdot z$ has two different factorizations in the quotient since $z^2 + \langle r \rangle = z^2 + xy - z^2 + \langle r \rangle = xy + \langle r \rangle$. For (b): *YES.* In a PID, an irreducible element generates a prime ideal, and prime ideals in this context a maximal. Hence the quotient is a field. □

Example 6.4 (Spring 2017, # 4)**.** Prove or disprove: The following rings are isomorphic? $R_1 := \mathbb{F}_5[x]/(x^4 + x^2 + 1)$ and $R_2 := \mathbb{F}_5/(x^4 - x^3 + x^2 - 1)$.

Proof. First we handle R_2: We can factor $x^4 - x^3 + x^2 - 1 = (x - 1)(x^3 + x + 1)$. Moreover, if we plug in $x = 0, 1, 2, 3, -1$ we can see that $x^3 + x + 1$ does not have any roots in $\mathbb{F}_5$. Then by the Chinese remainder theorem (CRT), we have that

$$R_2 \cong \mathbb{F}_5 \times \mathbb{F}_5[x]/(x^3 + x + 1).$$

In this case, taking a composition if necessary, we can define a ring homomorphism from $R_2 \to \mathbb{F}_5$.

On the other hand, suppose that there were a corresponding ring homomorphism $\phi : R_1 \to \mathbb{F}_5$. Any such homomorphism takes the form $\phi(f) = f(i)$ for some $i \in \mathbb{F}_5$. But since $x^4 + x^2 + 1$ should be zero in the quotient, and since $x^4 + x^2 + 1 \neq 0$ upon substitution of $x = 0, 1, 2, 3, 4$, we have a contradiction. Thus the two rings cannot be isomorphic. □

Example 6.5 (Spring 2018, # 3)**.** Let R be a commutative ring with 1. Suppose an ideal I in R is such that $xy \in I$ implies that either $x \in I$ or $y^n \in I$. Let

$$\sqrt{I} := \{r \in R : r^n \in I \text{ for some integer } n \geq 1\}.$$

Show that $\sqrt{I}$ is the smallest prime ideal containing I. (Here, "*smallest*" means that any other prime ideal containing I, contains $\sqrt{I}$. Hint: remember to prove that $\sqrt{I}$ is an ideal, which is also prime.)

Proof. *Show that $\sqrt{I}$ is an ideal.* Since $0 = 0^1 \in I$ we know that $\sqrt{I}$ is non-empty. Now suppose that $x, y \in \sqrt{I}$. We need to show that $x + y \in \sqrt{I}$. By the definition of $\sqrt{I}$, we have that there are $n, m \geq 1$ such that $x^n, y^m \in I$. By applying the binomial theorem,

$$(x + y)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} x^i y^{n+m-i}.$$

For any $0 \leq i \leq n + m$, either $i \geq n$ or $n + m - i \geq m$. So it follows that $x^i y^{n+m-i} \in I$, which implies that $x + y \in \sqrt{I}$. Then because I is an ideal, for any $a \in R$, $(ax)^n = a^n x^n \in I$. So $ax \in \sqrt{I}$ and hence we have proved that $\sqrt{I}$ is an ideal.
Show that $\sqrt{I}$ is prime. Suppose that $x, y \in R$ and that $xy \in \sqrt{I}$. Then by definition there is a positive natural number $n \geq 1$ such that $(xy)^n = x^n y^n$ (by commutativity) is in I. By the construction of I, we know that either $x^n \in I$ or $(y^n)^m = y^{nm} \in I$ for some $m \geq 1$. In the first case, $x \in \sqrt{I}$, and in the second case $y \in \sqrt{I}$. Thus we have shown that $\sqrt{I}$ is a prime ideal.
Show that if P is prime and $I \subseteq P$, then $\sqrt{I} \subseteq P$. Suppose that P is a prime ideal containing I and suppose that $x \in \sqrt{I}$. We need to show that $x \in P$. Now since $x \in \sqrt{I}$ we must have that $x^n \in I \subseteq P$ for some $n \geq 1$. Since P is itself prime, either x or x^{n-1} is in P. In the first case we are done. In the second case, we have that $x^{n-1} = x(x^{n-2}) \in P$, so we can repeat the same argument inductively to show that x or x^{n-2} is in P. Since n is a finite natural number, we can eventually see that we must have that $x \in P$. Hence we have shown that $\sqrt{I}$ is the *smallest* such prime ideal containing I. □

Example 6.6 (Spring 2018, # 4)**.** Suppose that R is a commutative ring with 1 such that for every $x \in R$, there is some natural number $n > 1$ such that $x^n = x$. Show that every prime ideal of R is maximal.

Proof. An ideal M is maximal *iff* R/M is a field. Let P be a prime ideal. We already know that R/P is an integral domain since P is prime, so it suffices for us to show that each non-zero element of R/P has a multiplicative inverse. We will use the bar notation to denote reduction modulo P when considering any non-zero $\bar{x} \in R/P$ corresponding to $x \in R$. For convenience in notation, for this fixed x let $y := \bar{x}$. Suppose that $n \geq 2$ is the guaranteed natural number such that $x^n = x$. Then we can see that $\bar{x^n} = y^n = \bar{x} = y$, or equivalently that $y(y^{n-1} - 1) = 0$. But since R/P is an integral domain and we have assumed that $y \neq 0$, we know that $y^{n-1} = y \cdot y^{n-2} = 1$. Thus y^{n-2} is our desired inverse for y. □

Example 6.7 (Fall 2015, # 1)**.** Let F be a finite field and let M be an invertible $n \times n$ matrix with entries in F. Prove that $M^m - I_n$ is not invertible for some integer $m \geq 1$.

Proof. Select any $n \times 1$ vector $v \neq 0$ with coefficients in F. Because F is finite there are only finitely-many choices for the vectors in the sequence $v, Mv, M^2v, \ldots$. By the pidgeonhole principle we must have that $M^iv = M^jv$ for some $i \neq j$. Letting $u := M^iv$, we see that $M^{j-i}u = u$, or that $(M^{j-i} - I_n)u = M^{j-i}u - I_nu = u - u = 0$. So we can conclude that either $M^{j-i} - I_n$ is not invertible (in which case we are done), or that it is invertible which would imply that $u = 0$. But we can always select a u such that $u \neq 0$ since if we could not pick such a u (i.e., if we had that $M^iv = 0\ \forall v$) then this would imply that $M \equiv 0$. And that would be a contradiction to our hypothesis on the invertibility of M. □

Example 6.8 (Fall 2015, # 7)**.** Show that for any field F and any integer $d \geq 1$, there exists at most one finite multiplicative subgroup $G \subset F \setminus \{0\}$ of order d.

Proof. We know that any polynomial of degree n over F has at most n roots since F is a field. For $d \geq 1$, consider the polynomial $p(x) \in F[x]$ defined by $p(x) := x^d - 1$. Now if a subgroup G of order d exists, then $\forall e \in G$, e is a root of $p(x)$. But if there were another distinct subgroup H with $|H| = d$ and where $\exists f \in H$ such that $f \notin G$, then we would have found $d + 1$ distinct roots of $p(x)$, a contradiction. □

Example 6.9 (Fall 2015, # 4)**.** Justify the following completely:

(a) Give an example of a degree-6 Galois extension $F/\mathbb{Q}$ with a non-abelian Galois group.

(b) Give an example of a degree-6 Galois extension $K/\mathbb{Q}$ with an abelian Galois group.

Proof. For (a): Let F be the splitting field of $f(x) = x^3 - 2$. Since f is irreducible (by Eisenstein, for example) the extension $F/\mathbb{Q}$ is Galois and has degree at most $3 \cdot 2 = 6$ over $\mathbb{Q}$. Letting $\alpha := \sqrt[3]{2}$ denote the real cube root of 2, we see that $\mathbb{Q}(\alpha) \subset F$, but that this inclusion is not an equality because $\mathbb{Q}(\alpha) \subset \mathbb{R}$ where $F \nsubseteq \mathbb{R}$. Hence we must have that $[F : \mathbb{Q}] = 6$. We also know that since $\deg(f) = 3$, the Galois group at hand is a subgroup of S_3, so it must in fact be isomorphic to all of S_3, which is not abelian.

For (b): We consider the cyclotomic field $K = \mathbb{Q}(\zeta_7)$ where $\zeta_7 := e^{2\pi\imath/7}$ is a primitive 7^{th} root of unity. Then $K/\mathbb{Q}$ is a cyclotomic extension which is Galois with cyclic Galois group $(\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$. Cyclic groups are abelian so we have produced the desired example. □

Example 6.10 (Spring 2016, # 1)**.** Let $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. List all intermediate fields K such that $\mathbb{Q} \subset K \subset F$, and find all elements $\alpha \in F$ such that $F = \mathbb{Q}(\alpha)$.

Proof. The field $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(x^2 - 2)(x^2 - 3)$ and so is a Galois extension over $\mathbb{Q}$. Let $G := \mathrm{Gal}(F/\mathbb{Q})$ and notice that the automorphisms $\hat{\sigma} \in G$ are determined by their actions permuting the leading sign of the generators $\sqrt{2} \to \pm\sqrt{2}$ and $\sqrt{3} \to \pm\sqrt{3}$. Let $\sigma, \tau \in G$ be defined by $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\tau(\sqrt{3}) = -\sqrt{3}$, i.e., so that $\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) \mapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$ and $\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) \mapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$. Then we can see that $\sigma\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) \mapsto$

$a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$, so that $\sigma\tau \neq \sigma, \tau$, but where $\sigma^2 = \tau^2 = (\sigma\tau)^2 = 1$. So $G = \{1, \sigma, \tau, \sigma\tau\} \cong Z_2 \times Z_2$ is the Klein 4-group. By the fundamental theorem of Galois theory, the subfields K such that $\mathbb{Q} \subset K \subset F$ are in bijective correspondence with the fixed fields of the distinct subgroups of G. For the sake of completion we can list them. In summary, these K are given by $\mathbb{Q}(\beta)$ for $\beta = \sqrt{2}, \sqrt{3}, \sqrt{6}$.

Now for the second part of the question. A basis for F over $\mathbb{Q}$ is given by $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ so that every element of F is of the form $\alpha := a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ for some $a, b, c, d \in \mathbb{Q}$. By order considerations on the degrees of the minimal polynomials of the elements α of these forms, we have that $F = \mathbb{Q}(\alpha)$ precisely when α is not strictly contained in any of the subfields K from above. This happens when at least two of the b, c, d coefficients are non-zero. □

Example 6.11 (Fall 2016, # 2)**.** Let R be an integral domain containing a field F. Show that if R has finite dimension as a vector space over F, then R is a field.

Proof. Since R is an integral domain, we just need to show that every non-zero $r \in R$ has a multiplicative inverse. Fix this $r \neq 0$ and consider the ring homomorphism $\phi : F[x] \to R$ that is the identity on F and maps $x \mapsto r$. Since $[R : F] = n < \infty$ is finite dimensional, it follows that $\mathrm{Ker}(\phi) \neq \{1\}$ has a non-trivial kernel. We also know that $\mathrm{Ker}(\phi)$ is a prime ideal in $F[x]$. Then F a field $\implies$ $F[x]$ is a PID, so that $F[x]/\mathrm{Ker}(\phi)$ is a field. This implies that x has an inverse in this quotient field. By the first isomorphism theorem for rings, $\mathrm{Im}(\phi) \cong F[x]/\mathrm{Ker}(\phi)$, therefore r has an inverse in R. □

Example 6.12 (Fall 2016, # 4)**.** Let K/F be a Galois extension whose Galois group is the symmetric group S_3. Is it true that K is the splitting field of an irreducible cubic polynomial over F?

Proof. The answer is *YES*. We now need to be more rigorous and prove our claim. Suppose that L is the fixed field of the transposition $(12) \in S_3$. Then $[L : F] = 3$, and since L is a subfield of a separable extension, L is a separable extension of F. It follows that there is a primitive $\alpha \in L$ such that $L = F(\alpha)$. Let $g(x)$ denote the minimal polynomial of α. We claim that K is the splitting field for g over F.

To see this, notice that since K/F is a Galois extension, the conjugates of α are contained in K. So if S is the splitting field for g over F, then $S \subseteq K$. Now by construction, $S \supseteq L$. Then since $[L : F] = 3$ and $[K : F] = 6$ and the dimension of any sub-extension of K divides 6, it must be the case that S is a degree-3 extension or a degree-6 extension, In the former case, $S = L$ and in the latter case $S = K$. We pull a clever observation out of the solutions to notice that $(13)L$ is the fixed field of the permutation $(13)(12)(13)^{-1} = (32)$. So by the fundamental theorem of Galois theory, $(13)L \neq L$ – and hence L cannot be a Galois extension of F. Then L is not the splitting field of g over F which leaves us with $S = K$. □

7 MORE PRACTICE PROBLEMS FROM PAST EXAMS

7.1 Problems specific to modules

An introduction to modules is given in Chapter 10 of Dummit and Foote.

Definition. Let R be a ring (not necessarily commutative nor with 1). A *left R-module* or a *left module over R* is a set M together with

(1) a binary operation $+$ on M under which M is an abelian group, and

(2) an action of R on M (that is, a map $R \times M \to M$) denoted by rm, for all $r \in R$ and for all $m \in M$ which satisfies

(a) $(r+s)m = rm + sm$, for all $r, s \in R, m \in M$,

(b) $(rs)m = r(sm)$, for all $r, s \in R, m \in M$, and

(c) $r(m+n) = rm + rn$, for all $r \in R, m, n \in M$.

If the ring R has a 1 we impose the additional axiom:

(d) $1m = m$, for all $m \in M$.

We see importantly that $\mathbb{Z}$-modules are essentially the same as abelian groups. Note that we have an analogous *sub-module criterion*: N is a submodule if $x + ry \in N$ for all $r \in R$ and $x, y \in N$. Representative problems from past comprehensive exams include the following samples:

Example 7.1 (Spring 2018, #8)**.** A R-module M is called *irreducible* of $M \neq 0$ and the only submodules of M are 0 and M. Now suppose that R is a commutative ring with 1 and that M is a left R-module. Show that M is irreducible if and only if M is isomorphic to R/I for a maximal ideal I of R.

Example 7.2 (Spring 2017, #5)**.** Give an example of a module M over $\mathbb{Z}[x]$ which is torsionfree (for all $f \in \mathbb{Z}[x]$ and $m \in M$, $f \cdot m = 0$ implies $f = 0$ or $m = 0$), but not free.

Example 7.3 (Spring 2016, #6)**.** A R-module M is called *faithful* if $rM = 0$ for $r \in R$ implies $r = 0$. Let M be a finitely generated faithful R-module and let J be an ideal of R such that $JM = M$. Prove that $J = R$. (HINT: $\mathrm{Adj}(A) \cdot A = \det(A) \cdot I$.)

Example 7.4 (Fall 2015, #8)**.** Let R be a commutative ring and let $f(X) = \sum_{i=0}^{d} c_i X^i$ be a *nilpotent* univariate polynomial with coefficients $c_i \in R$. Show that the coefficients c_i are also nilpotent.

Example 7.5 (Fall 2016, #3)**.** Let R be an integral domain. Suppose r is a non-zero, non-unit, irreducible element of R, and let $\langle r \rangle$ denote the ideal generated by r.

(a) If R is a UFD, is $R/\langle r \rangle$ also a UFD?

(b) If R is a PID, is $R/\langle r \rangle$ also a PID?

Example 7.6 (Spring 2016, #5)**.** Is the ring $\mathbb{Z}[2\imath]$, where $(2\imath)^2 = -4$, a principal ideal domain? If not, give an example of a non-principal ideal.

Example 7.7 (Fall 2017, #7)**.** Let $R := \mathbb{Q}[x, y]$. Is R an Euclidean domain? Is R a unique factorization domain?

Example 7.8 (Spring 2011, #5)**.** Suppose L/K is an algebraic field extension, and that R is a subring of L containing K. Prove that R is a field.

7.2 Fall 2017 exam problems

(2) Find a factorization of $f(x) = 6x^4 - 4x^3 + 24x^2 - 4x - 8$ into prime elements of $\mathbb{Z}[x]$.

(3) Let A and B be finitely generated abelian groups such that $A \times A \cong B \times B$. Prove that $A \cong B$.

(4) Find all primitive elements in the field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Justify the answers.

(6) Let p be prime and let G be any p-subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$. Prove that there is a non-zero vector $v \in \mathbb{F}_p^n$ such that $gv = v$ for all $g \in G$ with respect to the natural action of $\mathrm{GL}_n(\mathbb{F}_p)$ on $\mathbb{F}_p^n$. (*Group actions question*).

(8) Show that $f(x) = x^3 - 3x - 1$ is an irreducible element of $\mathbb{Z}[x]$. Compute the Galois group of the splitting field of f over $\mathbb{Q}$ and over $\mathbb{R}$.

7.3 Spring 2017 exam problems

(2) Consider the polynomial $f(x) = \frac{x^{23}-1}{x-1} = \sum_{n=0}^{22} x^n$, Determine the number of irreducible factors of $f(x)$ over each of the following fields: (a) $\mathbb{Q}$; (b) $\mathbb{F}_2$; and (c) $\mathbb{F}_{2048}$.

(6) Find the Galois group of the splitting field of the polynomial $f(x) = x^3 - x + 1$ over each of the following fields: (a) $\mathbb{F}_2$; (b) $\mathbb{R}$; (c) $\mathbb{Q}$.

7.4 Spring 2016 exam problems

(2) Show that two commuting complex square matrices share an eigenvector, without using the result that they are simultaneously triangularizable.

(4) Let G be a finite group and let $H \leq G$ be a proper subgroup. Prove that the union of all conjugates of H is a proper subset of G. Show that the conclusion need not be true if G is infinite. (*Group actions problem*)

7.5 Spring 2015 exam problems

(1) (a) Prove that the polynomial $f(x) = x^6 + x^3 + 1 = (x^9 - 1)/(x^3 - 1)$ is irreducible over $\mathbb{Q}$; (b) Find the factorization of $f(x)$ over $\mathbb{F}_{19}$.

(3) Let K be the splitting field over $\mathbb{Q}$ for an irreducible polynomial of degree 3. What are the possibilities for $[K : \mathbb{Q}]$? Give an example to show that each possibility does occur.

(7) (a) If n is prime and $F(x)$ is an irreducible polynomial over $\mathbb{Q}$ of degree n, prove that the Galois group of F over $\mathbb{Q}$ contains an n-cycle. (b) If n is not prime, show that the Galois group in part (a) need not contain an n-cycle. [HINT: Consider the cyclotomic polynomial $\Phi_8(x)$]

7.6 Problems from other previous exams

Example 7.9 (Fall 2014, #4)**.** Let V be a finite-dimensional complex vector space. A linear operator $T : V \to V$ is called *nilpotent* if $T^m = 0$ for some $m \in \mathbb{Z}^+$. Show that if T is nilpotent, then $T^n = 0$, where n is the dimension of V.

Example 7.10 (Spring 2014, #2)**.** Let $\mathrm{GL}_n(\mathbb{Q})$ denote the group of invertible matrices with entries in the rational numbers. Let p be a prime satisfying $p > n + 1$. Show that if $A \in \mathrm{GL}_n(\mathbb{Q})$ satisfies $A^p = I$, then $A = I$.

Example 7.11 (Fall 2012, #1)**.** Over a field of characteristic 0, prove that you cannot find two matrices A, B such that $AB - BA = I$. Show that the statement is false in a field of characteristic 2.

Example 7.12 (Spring 2011, #4)**.** Let R be a *local ring*, i.e., a commutative ring with identity having a unique maximal ideal M. Let A be a 2×2 matrix with coefficients in M. Show that the matrix $B = A + I$ is invertible over R.