RINGS AND FIELDS '07

RINGS AND FIELDS '07

Define ring, subrings, modules, and submodules.

Example 1. *Rings:*

(a) *We have the well-known rings;* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, *and* $\mathbb{C}$.
(b) *Inside* $\mathbb{C}$ *we find rings as follows; select an element* α *that is the root to some polynomial* $x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$ *where the* $a_j's$ *are integers, and set* $R = \mathbb{Z}[\alpha] = \{t \in \mathbb{C} \mid t = b_{n-1}\alpha^{n-1} + b_{n-2}\alpha^{n-2} + \cdots + b_0,$ *where each* $b_i \in \mathbb{Z}\}$.
(c) *Given any ring* R, *we can construct a ring from the collection of* $n \times n$ *matrices whose entries lie in* R;

$$S = Mat_n(R),$$

where multiplication and addition are the standard matrix operations.
(d) *The upper,* 2×2 *matrices over a commutative ring* R *with equal diagonal entries forms a commutative subring of* $Mat_2(R)$.

Example 2. *Modules Over a Ring* R:

(a) *For an index set* I, $\Pi_I R$ *and* $\oplus_I R$ *are modules over* R.
(b) *An* R*-module* F *is called free on a subset* X *if for every map* $f : X \to A$ *such that* $f(rx + sy) = rf(x) + sf(y)$ *for* $x, y \in X$ *and* $r, s \in R$, *where* A *is an* R*-module, there is a unique homomorphism* $h : M \to A$ *such that* $h|_X = f$.
(c) *An* R*-module* M *is called projective if, for every epimorphism* $f : A \to B$ *and homomorphism* $g : M \to B$, *there is a homomorphism*

Theorem 1. *An* R*-module* M *is free if and only if* $M \cong \oplus_I R$.

Theorem 2. *An* R*-module* M *is projective if and only if* $M \oplus N = F$ *for some free module* F.

Let us use the projective and free modules as a foundation for our course.

Theorem 3. *Every R-module is free if and only if R is a division ring.*

When is it true that every R-module is projective?

Artin-Wedderburn Theorem . *Every R-module is projective if and only if R is a finite direct product of matrix rings over division rings; i.e.,*

$$R = Mat_{n_1}(D_1) \times Mat_{n_2}(D_2) \times \cdots \times Mat_{n_k}(D_k),$$

for some natural numbers $n_1, n_2, \ldots, n_k$ and division rings $D_1, D_2, \ldots, D_k$.

Example 3. *Let $\mathbb{H}$ denote the (rational) Hamiltonian Quaternions;*

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{Q}\},$$

where addition is component-wise and multiplication extends linearly from $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$. Then, the left ideal of $R = Mat_2(\mathbb{H})$ consisting of the matrices with second column zero is a projective (left) ideal of R that is not free.

Example 4. *Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}$ and $I = (3, 1 + \sqrt{-5})$. We claim that I is projective but not free. First we will argue that $I \neq R$. Notice $3R \subseteq I$. Modulo $3R$, the general element of I can be represented as $(1+\sqrt{-5})\cdot(a+b\sqrt{-5}) = (a-5b)+(a+b)\sqrt{-5}$, which is congruent to $(a + b)[1 + \sqrt{-5}]$ mod $3R$. Therefore, $I/3R \cong \mathbb{Z}/3\mathbb{Z}$, and since $R/3R$ has order 9, I is properly contained in R.*

If I were free, then I would be principal; say $I = (a + b\sqrt{-5})$. Since I contains $3, 1+\sqrt{-5}$, by computing norms, a^2+5b^2 must divide 9 and 6. Hence $a^2 + 5b^2 = 1$ or 3. We rule out 1 since $I \neq R$. However, $a^2 + 5b^2 = 3$ is not possible. Therefore, I is not free.

Set

$$\alpha = \frac{2}{3}(1 + \sqrt{-5}), \text{ and } \beta = -1.$$

Note that $\alpha \cdot I \subseteq R$ and $\beta \cdot I \subseteq R$. Define the homomorphism $\theta : F = R \oplus R \to I$ by $\theta(r, s) = r3 + s(1 + \sqrt{-5})$. The epimorphism θ is split by the map $\delta : I \to F$ where $\delta(x) = (\beta x, \alpha x)$. (Check: $\theta(\delta(x)) = \theta((\beta x, \alpha x)) = 3\beta x + (1 + \sqrt{-5})\alpha x = x(-3 + \frac{2}{3}6) = x$. Therefore, I is projective.

Example 5. *The ring $R = \mathbb{Z}[\sqrt{-5}]$ of the last example has the property that every nonzero nonunit can be expressed as a product of irreducible elements (see homework), yet R is not a UFD (see the next example).*

Example 6. *Let d be a square-free integer $\neq 1$, and define*

$$R = \mathbb{Z}[\sqrt{d}] \text{ provided } d \equiv 2, 3 \pmod 4,$$

or

$$R = \mathbb{Z}[\frac{1+\sqrt{d}}{2}] \text{ when } d \equiv 1 (mod\ 4).$$

Then every ideal of R is projective. It is not known whether or not there are infinitely many $d's$ for which R is a PID. However, for such an R, R is a PID if and only if R is a UFD.

1. EXERCISE SET 1

In this homework set, R is an integral domain.

A nonzero, nonunit r of R is said to be *irreducible* provided $r = st$ for $s, t \in R$ can only happen when one of s or t is a unit. (Recall, $u \in R$ is a *unit* if $uv = 1$ for some $v \in R$). A nonzero, nonunit r of R is said to be *prime* if $r \mid ab$ for $a, b \in R$, implies $r \mid a$ or $r \mid b$.

R is said to have the *ascending chain condition on principal ideals*, if any increasing chain of ideals

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$$

stablizes (i.e., there is an index n such that $(a_m) = (a_n)$ for all $m \geq n$).

1. Show that if R has the ascending chain condition on principal ideals, then every nonzero nonunit r of R is a product of irreducible elements. Hint: To argue that r has an irreducible factor, either r is irreducible, or $r = r_1 s_1$ with r_1, s_1 nonzero nonunits. Note (r) is properly contained in (r_1) in this case. Repeat for r_1 and use the hypothesis to eventually obtain $r = s_1 t_1$ with s_1 irreducible. Now write $r = r_1 v_1 = r_1 r_2 v_2 = \ldots$ with $r_1, r_2, \ldots$ irreducible, and use the hypothesis to show that eventually some v_j is a unit.
2. Show that if R is a UFD then every irreducible element is prime and R has the ascending chain condition on principal ideals.
3. Show that if irreducible elements are prime in R and R has the ascending chain condition on principal ideals, then R is a UFD.
4. Show that R is a UFD if and only if every nonzero nonunit is a product of primes.
5. Show any PID is a UFD.

2. Integral Domains

Theorem 4. *Let R be an integral domain. Every submodule of $\oplus_n R$ for any n is free if and only if R is a PID.*

Proof. An ideal of R is a submodule of R. Hence if the condition is in force, R is necessarily a PID. Conversely, assume that R is a PID. We will show, by induction on n, that every submodule of $\oplus_n R$ is free. When $n = 1$, the nonzero submodules of R are ideals and are principal (hence isomorphic to R).

Inductively, let L be a nonzero submodule of $F = \oplus_n R$. For $\pi_j : F \to R$ equal to the projection map onto the j^{th} coordinate, $I = \pi_j(L) \neq 0$ for some j. Since $I = aR$ for some $0 \neq a \in R$, we can define a splitting map $f : aR \to L$ by $f(ar) = rx$ where $x \in L$ is any element such that $\pi_j(x) = a$. By the standard argument,

$$L = Im\ f \oplus Ker\ \pi_j|_L \cong aR \oplus Ker\ \pi_j|_L.$$

Note that $Ker\ \pi_j|_L = \{y \in L \mid y \text{ has a zero } j^{th} \text{ component}\} \leq \oplus_{i \neq j} R$, where the index i runs over $1, 2, \ldots, j-1, j+1, \ldots, n$. By induction, $Ker\ \pi_j|_L \cong \oplus_m R$ is free, and therefore, $L \cong \oplus_{m+1} R$. □

Given an ideal $I \neq 0$ of R, define

$$I^{-1} = \{t \in Q \mid tIsubseteqR\}.$$

The ideal I is said to be *invertible*, if

$$I \cdot I^{-1} = R.$$

Analogously, we have

Theorem 5. *Let R be an integral domain. Every submodule of $\oplus_n R$ for any n is projective if and only if every ideal of R is invertible (projective).*

In order to see this we need a few observations.

Bear Injective Test Lemma . *The module U is injective if and only if U is injective relative to any sequence $0 \to I \to R$ where I is an ideal of R.*

Proof. Assume that U is injective with respect to any sequence $0 \to I \to R$, and suppose that $0 \to A \to B$ is exact and $f : A \to U$. Consider the set $\mathcal{C}$ of all 2-tuples (g, C) where $A \leq C \leq B$ and $g|_A = f$. There is a maximal element (g_0, C_0).

If $C_0 \neq B$ let $x \in B \setminus C_0$, and let $I = \{r \in R \mid rx \in C_0\}$. Set $C' = C_0 + \langle x \rangle$. If $I = 0$, then $\langle x \rangle \cap C_0 = 0$ and so $C' = C_0 \oplus \langle x \rangle \leq B$; we then have the over-module C' of C_0 and can define $g' : C' \to U$ by

$g'(c_0, rx) = g(c_0)$, contradicting the maximality of (g, C_0). Therefore $I \neq 0$.

By hypothesis, the map $h : I \to U$ given by $h(r) = g(rx)$ can be lifted to a map $h' : R \to U$. We then define $g' : C' \to U$ by $g'(c_0 + rx) = g(c_0) + h'(r)$. If $c_0 + rx = b_0 + sx$ with $c_0, b_0 \in C_0$ and $r, s \in R$, then $(r - s)x = b_0 - c_0 \in C_0$ and so $r - s \in I$. But then $g(b_0 - c_0) = g((r - s)x) = h(r - s) = h'(r - s) = h'(r) - h'(s)$ and so $g(b_0) - g(c_0) = h'(r) - h'(s)$ implying $g(b_0) + h'(s) = g(c_0) + h'(r)$ making g' well-defined. It is easy to check that g' is a homomorphism that extends g which contradicts the maximality of (g, C_0). Thus, $B = C_0$ as desired. □

Corollary 6. *The quotient field Q of R is injective.*

Proof. Let I be an ideal of R and $0 \neq a \in I$. If $0 \neq f : I \to Q$, define $h : R \to Q$ to be multiplication by $(1/a)f(a)$. If $b \in I$, then $h(b) = (1/a)f(a) \cdot b = (1/a)f(ab) = (1/a)af(b) = f(b)$. By Baer's Injective Test Lemma, Q is injective. □

Corollary 7. *If I, J are ideals of R, then $Hom(I, J)$ is naturally identifiable with $\{t \in Q \mid tI \subseteq J\}$.*

Proof. It is well-known that $Hom(I, Q)$ can be identified with Q via multiplication the elements of Q, and that $Hom(I, J)$ is naturally a submodule of $Hom(I, Q)$. The assertion follows. □

Lemma 8. *Let $I \neq 0$ be an ideal of R. Then I is invertible if and only if I is projective.*

Proof. Suppose $II^{-1} + R$. Then $1 = r_1s_1 + r_2s_2 + \ldots + r_ns_n$ with $r_j \in I$ and $s_j \in I^{-1}$ for each j by the definition of II^{-1}. The map $\theta : F = \oplus_n R \to I$ given by $\theta(x_1, x_2, \ldots, x_n) = \Sigma_j r_j x_j$ is split by the map $f : I \to F$ given by $f(a) = (as_1, as_2, \ldots, as_n) \in F$. Therefore, $I \oplus Ker\ \theta \cong F$ and I is projective.

Conversely, if I is projective, there is an epimorphism $\theta : F \to I$ that is split by some map $f : I \to F$. Let $\theta(e_i) = x_i \in I$ where e_i is the standard idempotent element of F having a 1 in the i^{th}-component and $0's$ elsewhere. Write $f = (f_1, f_2, \ldots, f_n)$ where $f_j : I \to R$. By the last corollary, regard $f_j \in Hom(I, R) = \{t \in Q \mid tI \subseteq R\} = I^{-1}$. It follows that $\Sigma_j x_j f_j a = a$ for every $a \in I$, and consequently that $\Sigma_j x_j f_j = 1$. That is, $I \cdot I^{-1} = R$.

□

The proof of the last theorem now follows easily from the proof at the beginning this section in light of the last lemma.

3. Dedekind Domains

A domain such that every nonzero ideal is invertible is called a *Dedekind domain*.

An R-submodule J of Q is called a *fractional ideal* of R if $rJ \subseteq R$ for some $0 \neq r \in R$.

The domain R is said to be *integrally closed* if the only over-ring of R inside Q that is fractional over R is R itself.

An ideal P of R is said to be *prime*, if $ab \in P$ implies $a \in P$ or $b \in P$ for any $a, b \in R$. Equivalently, P is prime if R/P is an integral domain.

Recall that a UFD is a domain such that every nonzero nonunit is a product of primes.

Theorem 9. *TFAE:*

(a) *R is Dedekind.*
(b) *Every nonzero ideal is $1\frac{1}{2}$-generated (i.e., can be generated by two nonzero elements with the first generator chosen arbitrarily).*
(c) *Every proper ideal of R is (uniquely) a product of prime ideals of R.*
(d) *R is integrally closed, each nonzero prime ideal is a maximal ideal, and every ideal of R is finitely generated.*
(e) *R is Noetherian and for every prime ideal P of R, R_P is is a PID.*

4. A Fundamental Theorem

A module is free if it is isomorphic to a direct sum of copies of R. The number of copies of R is called the *rank* of the free module. Note $\oplus_n R \cong \oplus_m R$ if and only if $n = m$. (One way to justify this is to note that $\oplus_n R$ has at most n linearly independent elements).

If M is a module over an integral domain, the *torsion* submodule T of M is

$$T = \{x \in M \mid rx = 0 \text{ for some } 0 \neq r \in R\}.$$

A module whose torsion submodule is zero is said to be *torsion-free*. For example, the torsion submodule of M/T is zero, and so M/T is torsion-free.

We can rephrase Theorem 4.

Proposition 10. *If R is an integral domain, then any finitely generated torsion-free module is isomorphic of a submodule of $\oplus_n R$ for some n.*

Proof. Let C be finitely generated with generating set $\{x_1, x_2, \ldots, x_n\}$ of nonzero elements. Select x_1; if x_2 is independent of x_1, select x_2; otherwise reject x_2. Having selected a subset S of $\{x_1, x_2, \ldots, x_m\}$ in this fashion, select x_{m+1} if $S \cup \{x_{m+1}\}$ is an independent set; otherwise reject x_{m+1}. In this way we find a linearly independent subset U of $\{x_1, x_2, \ldots, x_n\}$ such that for any $x_i \notin U$, $U \cup \{x_i\}$ is linearly dependent.

Define $F = \oplus_{x \in U} \langle x \rangle$, a free module contained in C. Given any index j, there is a nonzero ring element r_j such that $r_j x_j \in F$ (this is because U is a linearly independent set but $U \cup \{x_j\}$ is linearly dependent. Thus, if $c = \Sigma_j a_i x_i \in C$ with $a_i \in R$, multiply by $r = \Pi_j r_j \neq 0$ to obtain $rc = \Sigma_j a_i r x_i \in F$. Therefore, $C \cong rC \leq F$ and C is isomorphic to a submodule of the free module F (the isomorphism sends $c \mapsto rc$ which is $1 - 1$ since C is torsion-free). □

A domain is said to be *noetherian* if each ideal of R is finitely generated.

Theorem 11. *The following are equivalent for an integral domain R:*

(a) *R is noetherian.*
(b) *The finitely generated torsion-free modules are precisely the modules that are isomorphic to a submodule of $\oplus_n R$ for some n.*
(c) *If M is a finitely generated module, then any submodule of M is finitely generated.*
(d) *If K is a finitely generated module and $K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots$ are submodules of K, then there is an index m such that $K_n = K_m$ for all $n \geq m$.*

Proof. $(a) \to (b)$. Clearly the submodules of $\oplus_n R$ are torsion-free. Induction on n shows that the submodules are finitely generated as well. Conversely, the case $n = 1$ shows that

$(b) \to (c)$. Let N be a submodule of M. As M is finitely generated, there is a free module $F = \oplus_n R$ and an epimorphism $\phi : F \to M \to 0$. By the Correspondence Theorem, $\phi^{-1}(N) = K$ is a submodule of F and by (b) is finitely generated. Therefore $N = \phi(\phi^{-1}(N))$ is finitely generated.

$(c) \to (d)$. Set $N = \cup_n K_n$. Since K is a submodule of M, K is finitely generated; generated by $x_1, x_2, \ldots, x_m$ say. For each i, there is an index n_i such that $x_i \in K_{n_i}$. With $m = max\{n_1, n_2, \ldots, x_n\}$, each $x_i \in K_m$ and so $N \subseteq K_m \subseteq N$.

$(d) \to (a)$. Given an ideal I of R, let $x_1 \in I$ and $I_1 = Rx_1$. If $I \neq I_1$, there is an $x_2 \in I \setminus I_1$. Set $I_2 = Rx_1 + Rx_2$. If $I \neq I_2$ there is an $x_3 \in I \setminus I_2$. Set $I_3 = \Sigma Rx_i$. Continuing in this manner, by (d), some I_k must coincide with I. □

Furthermore we have a fundamental splitting result:

Corollary 12. *If M is a finitely generated module over a PID, then $M = T \oplus N$ where T is the torsion submodule of M, and N is free, of finite rank.*

Proof. The map $M \to M/T$ splits because M/T is finitely generated, torsion-free (hence free) by the last theorem. □

Finitely Generated Modules Over a PID . *If R is a PID and M is a finitely generated module, then M is a (finite) direct sum of cyclic modules.*

Proof. It remains to show that any finitely generated torsion module T is a direct sum of cyclic modules. Given a prime $p \in R$, let $T_p = \{t \in T \mid p^k t = 0 \text{ for some } k \geq 1\}$. The submodule T_p is called the p-primary submodule of T. We claim that $T = \oplus_{p\, prime} T_p$ where the index includes exactly one p from each associate class of a given prime. (Note that $T_p = T_q$ when p and q are associated primes.) This reduces the problem to finitely generated primary modules (i.e., a finitely generated module K such that for some prime p, every element in K can be annihilated by a power of p).

Let $0 \neq t \in T$. Then $rt = 0$ for some $0 \neq r \in R$. Express r as $r = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$ with $p_1, p_2, \ldots, p_m$ non-associate primes. Set $r_j = r/p_j^{e_j}$ and note that the greatest common divisor of $r_1, r_2, \ldots, r_m$ is 1. This is because, any prime dividing r_j must divide $r_j p_j^{e_j} = r$ and some must be one of the p_i's; but p_i does not divide r_i.

In general, it is easy to see that the gcd of $a_1, a_2, \ldots, a_n$ is a where $aR = a_1R + a_2R + \cdots + a_mR$. Write $b_1r_1 + b_2r_2 + \cdots + b_mr_m = 1$ for some $b_1, b_2, \ldots, b_m \in R$. Then $t = (b_1r_1t) + (b_2r_2t) + \cdots + (b_mr_mt)$ and with $t_j = b_jr_jt$, $p_j^{e_j}t_j = 0$ so $t_j \in T_{p_j}$. Thus $t \in \Sigma_j T_{p_j}$.

If $x \in T_{p_1} \cap \Sigma_{j=2}^n T_{p_j}$ with $p_1, p_2, \ldots, p_m$ non-associate primes, then $p_1^{f_1}x = 0$ and $x = x_2 + x_3 + \cdots + x_n$ with $p_j^{f_j}x_j = 0$ for $j \geq 2$. The elements $p_1^{f_1}$ and $p_2^{f_2} \cdot p_3^{f_3} \cdots p_n^{f_n}$ are relatively prime (i.e., have gcd 1) and so $ap_1^{f_1} + bp_2^{f_2} \cdot p_3^{f_3} \cdots p_n^{f_n} = 1$ for some $a, b \in R$. Then $x = (ap_1^{f_1} + bp_2^{f_2} \cdot p_3^{f_3} \cdots p_n^{f_n})x = ap_1^{f_1}x + bp_2^{f_2} \cdot p_3^{f_3} \cdots p_n^{f_n}x = 0$.

From the next home set, we obtain that any finitely generated nonzero primary module M has a factorization

$$M = \langle x \rangle \oplus K,$$

where $x \neq 0$. Since K is either 0 or can be likewise factored

$$K = \langle x_2 \rangle \oplus K_2,$$

we obtain progressive decompositions

$$M = \langle x \rangle \oplus \langle x_2 \rangle \oplus \cdots \langle x_j \rangle \oplus K_j,$$

which must stabilize since the chain of submodules $\langle x \rangle \leq \langle x \rangle \oplus \langle x_2 \rangle \leq \langle x \rangle \oplus \langle x_2 \rangle \oplus \cdots \langle x_j \rangle$ stabilizes (i.e., terminates with some $K_j = 0$). Therefore, M is a direct sum of cyclics and the proof is complete. □

Analogously, we have

Finitely Generated Modules Over a Dedekind Domain . *If R is Dedekind and M is a finitely generated module, then $M = P \oplus C$ where P is a projective module and C is a finite direct sum of cyclic modules.*

5. EXERCISE SET 2

In this set R is a PID. A module M is said to be *p-primary* where p is a prime element of R, if for every $x \in M$ there exists a natural number k such that $p^k x = 0$.

1. Let M be a finitely generated p-primary module. Show there exists a natural number n such that $p^n M = 0$ (i.e., for every $x \in M$, $p^n x = 0$).
2. Let M be a finitely generated p-primary module. Argue that chains of submodules $K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \subseteq \cdots$ must stablize (i.e., there exists an m such that for all $n \geq m$, $K_n = K_m$).
3. Let M be a finitely generated p-primary module.
   (a) The *order of an element* $0 \neq y \in M$ is the least positive integer ℓ such that $p^\ell y = 0$ (this is justified by Problem 1). Use Problem 1 to show there is an element $x \in M$ that has maximal order k (i.e., $p^k x = 0$, while $p^{k-1} x \neq 0$ and if $0 \neq y \in M$, then $p^k y = 0$).
   (b) With the x in part (a), show there is a submodule K of M that is maximal with respect to $\langle x \rangle \cap K = 0$. (Hint: Use Problem 2)
4. Let M be a finitely generated p-primary module. This problem shows that for x and K from Problem 3, $M = \langle x \rangle \oplus K$. Let $X = \langle x \rangle$.
   (a) Given $r \in R$ a nonzero, nonunit, write $r = p^i s$ such that $i \geq 0$ and p does not divide s (R is a UFD). Show that $ry \in X \oplus K$ if and only if $p^i y \in X \oplus K$. Hint: For one direction, p^n, s relatively prime, where $p^n y = 0$, implies $ap^n + bs = 1$ for some $a, b \in R$. Multiply by p^i.
   (b) To show that $M = \langle x \rangle \oplus K$, it suffices to show that $py \in X \oplus K$ implies $y \in X \oplus K$, for every $y \in M$, using induction and part (a).
   (c) We will now assume that $py \in X \oplus K$ and show that $y \in X \oplus K$. Show there is an index $j < k$ (where k is given in Problem 1) such that $p^j py = 0$. (Take $j = 0$ if $py = 0$ and otherwise compare the orders of y and x).
   (d) Write $py = rx + z$ with $r \in R$ and $z \in K$. Using the j from part (c), conclude that $p \mid r$. Write $r = ps$.
   (e) With $K' = K + \langle y - sx \rangle$, either $K = K'$ or $X \cap K' \neq 0$. In the latter case, write $0 \neq tx = z' + a(y - sx)$ for some $t, a \in R$ and $z' \in K$. Argue that p does not divide a since otherwise, $tx \in K$.

(f) Continuing part (e), write $up + va = 1$, and conclude that $y = upy + vay \in X \oplus K$.

6. EXERCISE SET 3

In this set, R is an integral domain.

1. Show that if F is a field, then $R = F[x]$ is a PID. Hint: use the degree function $deg : F[x] \to \mathbb{N}$ and the division algorithm in $F[x]$ to show that if $f(x) \neq 0$ is a polynomial of smallest degree in an ideal $I \neq 0$, then $I = (f(x))$.
2. Show that $\mathbb{Z}[x]$ is not a PID. (Hint: Show that $I = (2, x)$ is not principal.)
3. Let R be a UFD with quotient field Q, and let $f(x) \in R[x]$.
   (a) Show that there is an element $r \in R$ and a polynomial $g(x) \in R[x]$, such that $f(x) = rg(x)$ and the gcd of the coefficients of $g(x)$ is 1. (r is called the *content of* f and we write $c(f) = r$).
   (b) Show that if $f(x) = g(x)h(x)$ with $g(x), h(x) \in Q[x]$, then there exists polynomials $g_1(x), h_1(x) \in R[x]$ each having content 1, and elements $0 \neq a, a_1, b, b_1 \in R$ such that a, a_1 and b, b_1 are coprime pairs, and $ag(x) = a_1 g_1(x)$ and $bh(x) = b_1 h_1(x)$. Thus, $abf(x) = a_1 b_1 g_1(x) h_1(x)$.
   (c) Reduce ab and $a_1 b_1$ in part (b) as necessary to obtain $df(x) = eg_1(x)h_1(x)$ with the $gcd(d, e) = 1$. Show that if $c(f) = 1$, then d and e are units.
   (d) Conclude that $f(x) \in R[x]$ is irreducible in $R[x]$ if and only if $f(x)$ is irreducible in $Q[x]$.
4. Let R be a UFD. Using Problem 1 and Problem 3 (d), show that $R[x]$ is a UFD. Conclude that $\mathbb{Z}[x]$ is a UFD that is not a PID.
5. The *Hilbert Basis Theorem* asserts that if R is noetherian, then so is $R[x]$. Assuming R is a noetherian domain, show that $R[x]$ is noetherian. Hint: If J is an ideal in $R[x]$, let I_n be the ideal of elements that occur as coefficients of x^n in some polynomial of degree n in J. Observe that $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$. Use this to pick generators for J.

7. Primary Decompositions

In this section R is a commutative noetherian ring (it need not be a domain, but the issue never arises). Since we are not restricting ourselves to domains, the symbol Q is in play and will be used here to denote a special type of ideal.

Recall that an ideal $P \neq R$ is called a *prime* ideal, if $ab \in P$ implies $a \in P$ or $b \in P$. If one wishes, we can define the term I *divides* J when I and J are ideals, to be the condition $J \subseteq I$. It is an easy exercise

to show that $P \neq R$ is prime if and only if P divides $I \cdot J$ implies P divides I or P divides J, for ideals I and J.

We say that an ideal $Q \neq R$ is *primary*, if for any $a, b \in R$, $ab \in Q$ and $a \notin Q$, implies $b^n \in Q$ for some natural number n. While primary integers are just the powers of primes, this is not the case for ideals in general rings of our type.

The *radical* of an ideal I, $rad(I)$, is defined to be

$$rad(I) = \{r \in R \mid r^n \in I \text{ for some } n \geq 1\}.$$

Proposition 13. (1) *For any ideal I, there exists an $n \geq 1$ such that $rad(I)^n \subseteq I$.*
(2) *If Q is primary, then $rad(Q)$ is prime.*

Proof. (1) It is easy to see that $rad(I)$ is an ideal, and since $R$is noetherian, there exists $a_1, a_2, \ldots, a_m \in rad(I)$ such that $rad(I) = \langle a_1, a_2, \ldots, a_m \rangle$. For each j there exists an positive integer k_i for which $a_i^{k_i} \in I$. Take $n = k_1 + k_2 + \cdots + k_m$. Then, the general element $r_1a_1 + r_2a_2 + \cdots + r_ma_m$ of $rad(I)$ satisfies $(r_1a_1 + r_2a_2 + \cdots + r_ma_m)^n = \Sigma \frac{n!}{i_1!i_2!\cdots i_m!}(r_1a_1)^{i_1}(r_2a_2)^{i_2}\cdots(r_ma_m)^{i_m}$ where the sum is over all non-negative integers $i_1, i_2, \ldots, i_m$ that sum to n (Multinomial Theorem). In any monomial $(r_1a_1)^{i_1}(r_2a_2)^{i_2}\cdots(r_ma_m)^{i_m}$, one of the i_j's must be greater than k_j and so that monomial lies in I. Therefore, $rad(I)^n \subseteq I$.

(2) Let $P = rad(Q)$ and suppose $ab \in P$ with $a \notin P$. By definition $(ab)^n \in Q$ for some n. Since $a \notin P$, $a^n \notin Q$ and since Q is primary, $(b^n)^m \in Q$ for some m. Then $b^{nm} \in Q$ and $b \in P$. □

A proper ideal I is called *irreducible*, if

$$I = J_1 \cap J_3 \implies I = J_1 \text{ or } I = J_2,$$

for ideals J_1, J_2.

Proposition 14. *Any irreducible ideal is primary.*

Proof. Let I be irreducible and suppose that I is not primary. There exists $a, b \in R$, such that $ab \in I$, $a \notin I$ and $b^n \notin I$ for every $n \geq 1$.

Let $I_n = \{r \in R \mid rb^n \in I\}$; $rb^n \in I$ implies $rb^{n+1} \in I$ and so $I_n \subseteq I_{n+1}$ for all n. Since R is noetherian, there is an index m such that $I_n = I_m$ for all $n \geq m$. Let $I' = \{rb^m + c \mid r \in R,\ c \in I\}$.

CLAIM: $I' \cap I_m = I$.

If $s \in I_m \cap I'$, then $s = rb^m + c$ and $sb^m \in I$. Then $rb^{2m} = cb^m - sb^m \in I$ and so $r \in I_{2m} = I_m$. Therefore, $s = rb^m + c \in I$. Clearly, $I \subseteq I' \cap I_m$, and the claim is supported. But neither I' nor I_m equal I, resulting in a contradiction. □

Primary Decompositions of Ideals Exist . Any proper ideal I of R can be expressed as

$$I = I_1 \cap I_2 \cap \cdots \cap I_m,$$

with I_j primary ideals of R.

Proof. If there are ideals that do not possess primary decompositions, let I be maximal with respect to not having a primary decomposition. By the previous proposition, I is not irreducible, and so $I = J_1 \cap J_2$ with J_1, J_2 different (i.e., larger than) I. Hence J_1, J_2 have primary decompositions, and therefore so does I; a contradiction. □

There are serious problems with the uniqueness issue. However, a general context under which there is uniqueness, is for noetherian domains such that every nonzero prime ideal is maximal, once the primary decomposition has been adequately aligned.

Proposition 15. *If I and J are primary ideals with radical P, then $I \cap J$ is a primary ideal with radical P.*

Hence, when considering a primary decomposition

$$I_1 \oplus I_2 \oplus \cdots \oplus I_n,$$

we can select the distinct primes among $rad(I_j)$, $j = 1, 2, \ldots, n$; call then $P_1, \ldots, P_k$, and set

$$J_i = \cap\{I_j \mid rad(I_j) = P_i\}.$$

We then have $I_1 \oplus I_2 \oplus \cdots \oplus I_n = J_1 \oplus J_2 \oplus \cdots \oplus J_k$, with the J_i's primary with distinct radicals. We now only consider primary decompositions of the latter type, in seeking to show uniqueness.

Lemma 16. *If $I_1, I_2, \ldots, I_m$ are relatively prime (i.e., $I_i + I_j = R$ for all $i \neq j$), then*

$$I_1 \cap I_2 \cap \cdots \cap I_m = I_1 I_2 \cdots I_m.$$

Proof. For two, $I_1 + I_2 = R$ implies $I_1 \cap I_2 = (I_1 \cap I_2)(I_1 + I_2) = (I_1 \cap I_2)I_1 + (I_1 \cap I_2)I_2 \subseteq I_1 I_2$. The other containment is obvious. The inductive step is left as Exercise 4.4. □

Theorem 17. *Let R be a noetherian domain such that every nonzero prime ideal is maximal. If $I_1, I_2, \ldots, I_m$ and $J_1, J_2, \ldots, J_n$ are collections of primary ideals with distinct radicals, such that*

$$I = I_1 \cap I_2 \cap \cdots \cap I_m = J_1 \cap J_2 \cap \cdots \cap J_n,$$

then $n = m$ and after reindexing, $I_j = J_j$ for all j.

Proof. Each primary ideal mentioned in the statement contains a power of its radical by Proposition 13. Let P_i be the radical of I_i, so that $P_i^{k_i} \subseteq I_i$ for each i. Since $P_i^{k_i} + P_j^{k_j} = R$ for $i \neq j$ (Exercise 4.2), it follows that $I_i + I_j = R$ for all $i \neq j$. Therefore, by the previous lemma,

$$I = I_1 I_2 \cdots I_m = J_1 J_2 \cdots J_n.$$

With $k = max\{k_1, \ldots, k_m\}$, $P_1^k \cdots P_m^k \subseteq I$. Likewise, if Q_j is the radical of J_j, then $Q_1^\ell \cdots Q_n^\ell \subseteq I$. For the sake of later discussions, let us assume that $k \geq \ell$ (else, replace k by ℓ). We now have, for any i,

$$Q_1^k \cdots Q_n^k \subseteq I \subseteq I_i \subseteq P_i = rad(I_i).$$

Since P_i is maximal (hence prime), each P_i contains and is therefore equal to some Q_j. Conversely, each Q_j coincides with some P_i, and since $P_1, P_2, \ldots, P_m$ are distinct and $Q_1, Q_2, \ldots, Q_m$ are distinct, we conclude that $n = m$ and after reindexing, $P_i = Q_i$.

We will now show that $I_1 = J_1$; the proof for the others follows from the indexing being arbitrary. By Exercise 4.3, there exists a $t \in (P_2 \cdots P_m)^k \setminus P_1$. It follows that $t \in I_2 \cdots I_m$ and that $ta \in I$ for every $a \in I_1$, yet $t \notin I_1$ because $t \notin P_1$. Moreover, $t^j \notin I_1$ for any j, because P_1 is prime. Likewise, $tr \in I$ for every $r \in J_1$, yet $t \notin J_1$.

Suppose $r \in J_1$, so that $tr \in I$. Since $tr \in I_1$ and I_1 is primary, either $r \in I_1$ or $t^j \in I_1$ for some j. We've already observed that $t^j \in P_1$ is impossible, so therefore, $r \in I_1$. Similarly, $I_1 \subseteq J_1$, and the proof is complete. □

8. EXERCISE SET 4

1. Prove Proposition 15.
2. If I, J are comaximal ideals (i.e., $I+J = R$), show that $I^k+J^\ell = R$ for any integers k, ℓ.
3. Assume that $I_1, I_2, \ldots, I_m$ are pairwise comaximal ideals of R. If k is a positive integer, show that
$$I_1 + (I_2 \cdots I_m)^k = R.$$
4. Finish the proof of Lemma 16: If $I_1, I_2, \ldots, I_m$ are pairwise comaximal, then
$$I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n.$$
5. Let $R = \mathbb{Z}[x]$. Show that the ideal $I = (x^2, 2x)$ has the following primary decompositions with mutually distinct radicals:
$$I = (x) \cap (x^2, 2) = (x) \cap (x^2, 2 + x) = (x) \cap (x^2, 2x, 4).$$
6. Let $I \neq R$ be an ideal that contains a power of a maximal ideal. Then I is primary. Therefore, if R is a domain such that every nonzero prime ideal is maximal, the the primary ideals are precisely the ideals that contain a power of a maximal ideal.
7. Show that $I = (x^2, 2x)$ in $R = \mathbb{Z}[x]$ is not primary yet I contains $(x)^2$. This shows the assumption in Exercise 4.6 that I contain a power of a maximal ideal cannot be weakened to a power of a prime.

9. Nakayama's Lemma

In this section R is still a commutative ring.

Proposition 18. *If I is an ideal in a commutative ring R, and $I \neq R$, then I is contained in a maximal ideal of R.*

As a consequence, and element $0 \neq r \in R$ is contained in some maximal ideal if and only if r is not a unit.

The (Jacobson) *radical* of R is defined to be

$$J(R) = \cap\{\ M \mid M \text{ is a maximal ideal of } R\ \}.$$

Nakayama's Lemma . If K is a finitely generated module over a commutative ring R such that $J(R)K = K$, then $K = 0$.

Proof. Suppose $r \in J(R)$. If $1 - r$ is not a unit of R, then by the last proposition, $1 - r \in M$ for some maximal ideal M. But then $1 = 1 - r + r \in M$, a contradiction. Thus, $1 - r$ is a unit.

Let $x_1, x_2, \ldots, x_n$ be a minimal generating set for K. By hypothesis, we can write

$$x_1 = \Sigma_j r_j x_j$$

with $r_j \in J(R)$ for all j. Therefore, $x_1 = (1-r_1)^{-1}\Sigma_{j=2}^{n} r_j x_j$, contradicting the minimality of the generating set, unless $n = 1$ and $x_1 = 0$. □

A ring R is called *quasi-local*, if R has a unique maximal ideal M. In this case $J(R) = M$.

Kaplansky . If R is a quasi-local ring, then any projective R-module is free.

Proof. We will only include the proof that finitely generated projective modules are free. Let W be a finitely generated projective module, and let $x_1, x_2, \ldots, x_n$ be a minimal generating set for W. There is a free module F of rank n and a natural epimorphism $f : F \to W$ given by $f(e_i) = x_i$ where $e_1, e_2, \ldots, e_n$ is the standard basis for F.

Let $K = Ker\ f$. Since W is projective, there is a monomorphism $g : W \to F$ such that $F = K \oplus Im\ g$. Observe that $K \subseteq MF$, because if $f(r_1, r_2, \ldots, r_n) = \Sigma_j r_j x_j = 0$, and r_1 (say) is not in M, then r_1 is a unit, allowing a reduction in the size of the generating set; a contradiction. Thus, $K \subseteq MF$ and since $K = \pi(F)$ where $\pi : F \to K$ is the coordinate projection map, it follows that $MK = K$. By Nakayama's Lemma, $K = 0$. □

10. Subrings of Quadratic Number Fields

Let us look to the classical examples of Dedekind to illustrate some of the discussions thus far. Call an element $\alpha \in \mathbb{C}$ *integral* over $\mathbb{Z}$ if there is a monic polynomial $0 \neq f(x) \in \mathbb{Z}[x]$ that has α as a root. If $f(x)$ has degree n, then

$$R = \mathbb{Z}[\alpha] = \{b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} \mid b_j \in \mathbb{Z}\},$$

is an integral domain that is generated by $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ over $\mathbb{Z}$. It turns out, α is integral if and only if α belongs to a subring R of $\mathbb{C}$ that is finitely generated as a $\mathbb{Z}$-module.

We say that α is *algebraic* (over $\mathbb{Q}$) if α is a root to some polynomial $0 \neq f(x) \in \mathbb{Z}[x]$. Integral elements are algebraic but not conversely. The number $\frac{1}{\sqrt{2}}$ is not integral, being a root to the irreducible polynomial $2x^2 - 1$, which is not monic.

Given an algebraic element α, there is an irreducible polynomial in $\mathbb{Z}[x]$ having alpha as a root. Denote this polynomial by $irr_{\mathbb{Z}}(\alpha)$. It is easy to check that a complex number α is integral if and only if it is algebraic and $irr_{\mathbb{Z}}(\alpha)$ is monic.

The elements of the form $\sqrt[n]{m}$ where m, n are integers and $n > 0$ are integral. For our examples here we will consider the case $n = 2$ and m is square-free. The field

$$\mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}$$

is called a *quadratic number field*.

A subring R of a quadratic number field $\mathbb{Q}[\sqrt{m}]$ is said to be *full*, if R contains at least one nonrational number. In this case, R is called *integrally closed* if each $\alpha \in \mathbb{Q}[\sqrt{m}]$ that is integral actually belongs in R.

Example 7. *A full subring R of $\mathbb{Q}[\sqrt{m}]$ that is finitely generated over $\mathbb{Z}$ is integrally closed if and only if*

$$R = \mathbb{Z}[\sqrt{m}] \text{ when } m \equiv 2 \text{ or } 3 \ (mod\ 4), \text{ and}$$

$$R = \mathbb{Z}[\tfrac{1+\sqrt{m}}{2}] \text{ when } m \equiv 1 \ (mod\ 4).$$

It then turns out that a full subring S of $\mathbb{Q}[\sqrt{m}]$ is integrally closed if and only if

$$S = \cap_{P \in \mathcal{P}} R_P$$

where R is one of the rings of the previous example, and $\mathcal{P}$ is a set of maximal ideals of R. By the theory of localizations, the ideals of S are IS where I is an ideal of R. Hence S is noetherian if R is noetherian. Since R is finitely generated as a $\mathbb{Z}$-module, any ideal is

finitely generated as a $\mathbb{Z}$-module and therefore as an R-module. Hence R and S are noetherian.

If P is a nonzero prime ideal of R, and $0 \neq \beta \in P$, then $n\beta^{-1} \in R$ for some n (since $\mathbb{Q}[\sqrt{m}]$ is a field), and therefore $n\beta^{-1}\beta = n \in P$. Consequently, since R is an image of $\mathbb{Z} \oplus \mathbb{Z}$, R/P is an image of $\mathbb{Z} \oplus \mathbb{Z}/n(\mathbb{Z}\oplus\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}$. Therefore R/P is a finite integral domain, implying that R/P is a field. I.e., P is maximal.

To recap, an integrally closed full subring of $\mathbb{Q}[\sqrt{m}]$ is

(i) integrally closed,
(ii) noetherian, and
(iii) every nonzero prime ideal is maximal.

Such rings are called *Dedekind* domains, after the person to first formally study these rings, and the initiator of formal commutative ring theory.

Theorem 19. *A full subring R of $\mathbb{Q}[\sqrt{m}]$ is a Dedekind domain if and only if every ideal I is a product prime ideals. Furthermore, these conditions are equivalent to the property that for any ideal $I \neq 0$ of R, $I^{-1} = \{t \in \mathbb{Q}[\sqrt{m}] \mid tI \subseteq R\}$ satisfies $I^{-1}I = R$.*

The proof of this is within the scope of our course, but as time is of the essence, will be omitted. *Class Number Theory* and *Algebraic Number Theory* study the field $\mathbb{Q}[\sqrt{m}]$ by considering the group of isomorphism classes of ideals of R (as in Example 7) where $[I] \cdot [J] = [IJ]$; here, $[I]^{-1} = [I^{-1}]$.

Corollary 20. *Let R be a full subring of $\mathbb{Q}[\sqrt{m}]$. Then every primary ideal is a power of a prime ideal if and only if R is Dedekind.*

Proof. Since R is noetherian such that nonzero prime ideals are maximal, any proper ideal I of R can be expressed as

$$I = I_1 I_2 \cdots I_m,$$

where $I_1, I_2, \ldots, I_m$ are primary ideals with distinct radicals. If for each I, every I_j is a power of a prime, then I is a product of prime ideals and R is Dedekind by the theorem. Conversely, if R is Dedekind, then a primary ideal J must also be a product of prime ideals. Since J contains a power of its radical $P = rad(J)$, $P^k \subseteq J = P_1 P_2 \cdots P_\ell \subseteq P_j$, implies $P = P_i$ for any i. I.e., J is a power of a prime ideal. □

Corollary 21. *Let R be a full subring of $\mathbb{Q}[\sqrt{m}]$. Then R is a UFD if and only if R is a PID. In this case, R is Dedekind.*

Proof. Assume that R is a UFD and let r be a prime in R. Then (r) is a prime ideal, and because R is a full subring of $\mathbb{Q}[\sqrt{m}]$, (r) is maximal.

Conversely, if M is maximal then $M = (r)$ for some prime r (that is, if $p_1 p_2 \cdots p_n \in M$, then some $p_j \in M$ and therefore $M = (p_j)$).

Because the maximal ideals of R are of the form (p) for some prime p, if $b \in R$ is not a multiple of p, then

$$Rb + Rp = R.$$

Therefore, $sb + tp = 1$ for some $s, t \in R$.

If I is a primary ideal, then $(p^n) \subseteq I \subseteq (p)$ for some prime p. Let k be the smallest index such that $(p^k) \subseteq I$, so that $p^{k-1} \notin I$. Suppose there exists $a \in I \setminus (p^k)$. Since R is a UFD we can write $a = p^j b$ with p, b relatively prime. Note $j < k$ since $a \notin (p^k)$.

Since b, p are coprime, there exists $s, t \in R$ such that

$$sb + tp = 1.$$

Thus,

$$p^{k-1} = sp^{k-1}b + tp^k = sp^{k-1-j}p^j b + tp^k \in I,$$

contrary to the choice of k. Therefore, $I = (p^k)$ and every primary ideal is a power of a prime (maximal) ideal. □

There are only finitely many known PID's of the form of Example 7. Here are some interesting heavy-duty algebraic number theoretic results: Let R be as in Example 7:

(a) There are infinitely many integral primes p such that pR is prime.

(b) There are infinitely many integral primes p such that $pR = P_1 P_2$ for distinct maximal ideals P_1, P_2.

(c) There are only finitely many p's for which $pR = P^2$; these are the prime divisors of m with the possible exception of $p = 2$.

Some research problems suggested by the topics that came up in this regard:

1. Which full subrings S of $\mathbb{Q}[\sqrt{m}]$ have every ideal generated by an integer? This pertains to a problem of P. Hill which I answered in the 1990's.

2. If $R \subseteq S \subseteq Q$ with R a domain, when is it the case that ideals of S are extendable from R; i.e., every ideal J of S is of the form IS where I is an ideal of R (i.e., $I = J \cap R$)? I answered this to a degree in the late 90's.

3. If R is noetherian, when is every overring of R inside Q of the form $\cap_{P\in\mathcal{P}} R_P$? These turn out to be the Dedekind domains.

4. If R is a noetherian domains such that every nonzero prime ideal is maximal, under what conditions does the Krull-Schmidt Theorem hold relative to finitely generated, torsion-free modules? I.e., when is it the case that whenever

$$A_1 \oplus A_2 \oplus \cdots \oplus A_n \cong B_1 \oplus B_2 \oplus \cdots \oplus B_n,$$

with A_i, B_j indecomposable, torsion-free finitely generated R-modules, then

$$m = n \text{ and after reindexing } A_i \cong B_i \ \forall\ i?$$

11. Semi-Simple Rings

Let R be a ring (not necessarily commutative). In this section, we will consider **right** R-modules and and right ideals. A module refers to a right R-module. The case for left modules can be made independently and analogously. A module is called *simple* if is had no proper submodules. A module M is called *semi-simple* if it is a sum of simple submodules;

$$M = \Sigma_i N_i,$$

where each N_i is simple.

Schur's Lemma . If I and J are simple modules and $f \in Hom(I, J)$, then either $f = 0$ or f is an isomorphism. In particular, $End_R(I) = \{f \mid f : I \to I \text{ is a module homomorphism } \}$ is a division ring.

Proof. Let $0 \neq f : I \to J$. Since $Ker\ f$, $Im\ f$ are submodules of I and J respectively, and since I, J are simple,$Im\ f = I$ and $Ker\ f = 0$. In particular, any $g : I \to I$ is an automorphism. Thus, $g^{-1} : I \to I$ is a well-defined homomorphism, implying that $End_R(I)$ is a division ring. □

The *Jacobson Radical* of R, $J(R)$, is defined to be

$$J(R) = \cap\{M \mid M \text{ is a maximal right ideal}\}.$$

The ring R is called *(Jacobson) semi-simple* if $J(R) = 0$. R is called *right artinian* if R has the descending chain condition on right ideals: i.e., if

$$I_1 \supseteq I_2 \supseteq \cdots,$$

are right ideals, then for some index m, $I_n = I_m$ for all $n \geq m$.

Chinese Remainder Theorem . If $P_1, P_2, \ldots, P_k$ be parwise comaximal ideals of R, then

$$R/\cap_j P_j \cong R/P_1 \times R/P_2 \times \cdots \times R/P_k$$

as rings.

Proof. Define a map $\theta : R \to R/P_1 \oplus R/P_2 \oplus \cdots \oplus R/P_k$ by $\theta(r) = (r + P_1, r + P_2, \ldots, r + P_k)$. Clearly $Ker\ \theta = \cap_j P_j$ so it remains to show that θ is an epimorphism.

We have $P_1 + P_2 = R$, implying that $P_1P_3 + P_2P_3 = P_3$, from which it follows that $P_1 + P_2P_3 = P_1 + P_1P_3 + P_2P_3 = P_1 + P_3 = R$. Continuing in this way, $P_1 + \Pi_{j\geq 2}P_j = R$. Now let $\hat{P}_j = \Pi_{i\neq j}P_i$ (with the P_i's appearing with increasing index moving from left to right). We can induct on k to show that $\hat{P}_1 + \hat{P}_2 + \cdots + \hat{P}_k = R$. The case $k = 2$ is obvious. Inductively, for $n \geq 3$, let

$$Q_j = \Pi_{i\neq j}^{n-1} P_i.$$

By induction $Q_1 + Q_2 + \cdots + Q_{n-1} = R$. Note $\hat{P}_j = Q_jP_n$ if $j < n$. Thus $Q_1P_n + Q_2P_n + \cdots + Q_{n-1}P_n = P_n$, and therefore

$$\hat{P}_1 + \hat{P}_2 + \cdots + \hat{P}_{n-1} + \hat{P}_n = P_n + \hat{P}_n = R,$$

as claimed.

Write $1 = x_1 + x_2 + \cdots + x_k$ where $x_j \in \hat{P}_j$. Let $r_1, r_2, \ldots, r_k \in R$ be given, and take $r = r_1x_1 + r_2x_2 + \cdots r_kx_k$. Modulo P_j,

$$r \ \equiv\ r_jx_j \ \equiv\ (r_jx_1 + \cdots + r_jx_n) \ \equiv\ r_j.$$

Therefore, the map from $R \to R/P_1 \oplus R/P_2 \oplus \cdots \oplus R/P_k$ is an epimorphism which is clearly an R-module map.

Note $1^2 = 1 = \Sigma_{i,j}x_ix_j$ which maps to $(x_1^2+P_1, x_2^2+P_2, \ldots, x_k^2+P_k) = (x_1+P_1, x_2+P_2, \ldots, x_k+P_k)$. Multiplying $1 = x_1+x_2+\cdots+x_k$ through by r and s respectively, we obtain

$$r = rx_1 + rx_2 + \cdots + rx_k$$

and

$$s = sx_1 + sx_2 + \cdots + sx_k.$$

So, rs maps to $(rsx_1^2+P_1, rsx_2^2+P_2, \ldots, rsx_k^2+P_k) = (rsx_1+P_1, rsx_2+P_2, \ldots, rsx_k+P_k)$. The former term $(rsx_1^2 + P_1, rsx_2^2 + P_2, \ldots, rsx_k^2 + P_k)$ is equal to $(rx_1 + P_1, rx_2 + P_2, \ldots, rx_k + P_k) \cdot (rsx_1 + P_1, rsx_2 + P_2, \ldots, sx_k + P_k)$

□

Artin-Wedderburn Theorem . The following are equivalent for a ring R:

1. R is semi-simple as a module.
2. R is semi-simple artinian as a ring.
3. There exists natural numbers $n_1, n_2, \ldots, n_k$ and division rings $D_1, D_2, \ldots, D_k$ such that

$$R \cong Mat_{n_1}(D_1) \times Mat_{n_2}(D_2) \times \cdots \times Mat_{n_k}(D_k).$$

Proof. (1) $\rightarrow$ (3): If R is semi-simple as a right module, write $R = \Sigma_j I_j$, and in particular, $1 = x_{j_1} + x_{j_2} + \cdots + x_{j_m}$ with $x_{j_i} \in I_{j_i}$. If $r \in R$, then $r = x_{j_1}r + x_{j_2}r + \cdots + x_{j_m}r$. Furthermore, $r = ra_{k_1} + \cdots + ra_{k_m} \in \Sigma_{i=1}^{m} I_{k_i}$ for any $r \in R$, and after relabeling I_{k_i} as I_i, we obtain

$$R = I_1 + I_2 + \cdots + I_m,$$

a finite sum.

Reorder the I_j's so that $I_1, I_2, \ldots, I_k$ are pairwise non-isomorphic and if $j \geq k$, then $I_j \cong I_i$ for some $i \leq k$. We have that

$$R \cong I_1^{n_1} \oplus I_2^{n_2} \oplus \cdots \oplus I_k^{n_k},$$

with $Hom_R(I_i, I_j) = 0$ for all $i \neq j$ by Schur's Lemma.

We now have the isomorphisms

$$R \cong End_R(R) \cong Hom_R(I_1^{n_1} \oplus I_2^{n_2} \oplus \cdots \oplus I_k^{n_k}, I_1^{n_1} \oplus I_2^{n_2} \oplus \cdots \oplus I_k^{n_k})$$

$$\cong Hom_R(I_1^{n_1}, I_1^{n_1}) \times Hom_R(I_2^{n_2}, I_1^{n_2}) \times \cdots \times Hom_R(I_k^{n_k}, I_k^{n_k}),$$

and in turn this last ring is isomorphic to

$$Mat_{n_1}(D_1) \times Mat_{n_2}(D_2) \times \cdots \times Mat_{n_k}(D_k).$$

The first isomorphism is called the *left regular representation of* R and sends $r \in R$ to $\lambda_r \in End_R(R)$ where $\lambda_r(a) = ra$ (note, this is a right module map). If $f \in End_R(R)$, then $f(a) = f(1)a$ and so $f = \lambda_{f(1)}$. The rest of the details concerning this isomorphism are easy to check.

The second isomorphism is an application of the obvious fact that if $A \cong B$ as modules, then $End_R(A) \cong End_R(B)$ as rings. Specifically, if $\theta : A \rightarrow B$ is a right module isomorphism, then the map $\delta \mapsto \theta\delta\theta^{-1}$ is an isomorphism from $End_R(A)$ onto $End_R(B)$.

The third isomorphism employs the principal that if $Hom(A, B) = 0$, then

$$Hom(\oplus_{i=1}^{n} A_i, \oplus_{i=1}^{n} B_i) = \begin{pmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{21} & f_{22} & \cdots & f_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ f_{n1} & f_{n2} & \cdots & f_{nn} \end{pmatrix},$$

where $f_{ij} : A_i \to B_j$. Such a matrix sends $(a_1, a_2, \dots, a_n) \in \oplus_j A_j$ to $(\Sigma_j f_{1j}(a_j), \Sigma_j f_{2j}(a_j), \dots, \Sigma_j f_{nj}(a_j)) \in \oplus_j B_j$ (via left multiplication by the matrix on $(a_1, a_2, \dots, a_n)$).

The final isomorphism follows from Schur's Lemma and properties of Hom. Let I be a simple right ideal of R, and $D = End_R(I)$. Then

$$End_R(I^m) \cong Mat_m(D),$$

as rings. To examine this we will distinguish between different copies of I; let X_i be the copy of I generating the i^{th} component. Then $\alpha \in End_R(I^m)$ can be identified with the $m \times m$ matrix whose i, j^{th} entry is $\pi_j \alpha|_{X_i}$ where $\pi_j : \oplus_\ell X_\ell \to X_j$ is projection onto the j^{th} coordinate. Conversely, a matrix A in $Mat_m(D)$ represents an endomorphism of $\oplus_i X_i$ via left multiplication by A on the m-tuples inside $X_1 \oplus X_2 \oplus \cdots \oplus X_m$. In this way we identify elements of $End_R(I^m)$ with the corresponding elements of $Mat_m(D)$.

(3) $\to$ (2): Follows from Exercise 5.5.

(3) $\to$ (1): Follows from Exercise 5.4.

(2) $\to$ (3): According to the Chinese Remainder Theorem, it is sufficient to find comaximal two-sided ideals $P_1, P_2, \dots, P_n$ whose intersection is zero such that R/P_i is a matrix ring over a division ring for each i.

Let P be the right annihilator of a simple right R-module A. Then

$$A(rP) \subseteq (Ar)P = 0,$$

implying that P is a two-sided ideal. Certainly $P \neq R$. To the end of showing that R/P is a matrix ring over a division ring, we embed R/P into $End_D(A)$ where $D = End_R(A)$ (is a division ring), via right multiplication (i.e., $r \in R$ maps to right multiplication by r in $End_D(A)$).

We will establish a lemma below which will aide us. Assuming this for now, suppose A is not finite dimensional over D; say $x_1, x_2, \dots$ are independent over D. Set I_j equal to the right annihilator of $\{x_1, x_2, \dots, x_j\}$. Then

$$I_1 \supseteq I_2 \supseteq \cdots,$$

is a chain of right ideals of R. By the lemma below, for each j, there exists $r \in I_j$ such that $x_{j+1} r \neq 0$, implying $I_j \neq I_{j+1}$. This contradicts R being right artinian. Hence A is finite dimensional. By Exercise 5.1, $End_D(A)$ is the matrix ring $Mat_n(D)$ where $n = dim_D\ A$.

We have the embedding of R/P into $End_D(A)$. It remains to show that this map is onto. Let $x_1, x_2, \dots, x_n$ be a basis for A over D and let $y_1, y_2, \dots, y_n \in A$. Set B_j equal to the D-subspace of A generated by $\{x_1, x_2, \dots, x_n\} \setminus \{x_j\}$ and let $I_j = ann_R\ (B_j)_R$. By the lemma below, $x_j I_j \neq 0$ and since A is right simple over R, $x_j I_j = A$ for all j.

Write $y_j = x_j t_j$ for $t_j \in I_j$ and set

$$r = t_1 + t_2 = \cdots + t_n.$$

Then

$$x_j r = x_j t_1 + x_j t_2 \cdots + x_j t_n = x_j t_j = y_j,$$

since $x_j r_i = 0$ when $i \neq j$. This shows that the map $R/P \to End_D(A)$ is onto.

Now, as R/P is a matrix ring over a division ring, P is the intersection of finitely many maximal right ideals of R. Therefore $\cap\{\ P \mid P$ is the right annihilator of a simple right R-module $\} \subseteq J(R) = 0$. But, R is artinian, so there are finitely many distinct ideals $P_1, P_2, \ldots, P_m$ that are annihilators of simple right R-modules, such that

$$P_1 \cap P_2 \cap \cdots \cap P_m = 0.$$

The rings R/P_i are simple by Exercise 5.2 and what we have shown above, so each P_i is a maximal two-sided ideal. By the Chinese Remainder Theorem,

$$R = R/\cap_i P_i \cong R/P_1 \times R/P_2 \times \cdots \times R/P_m,$$

and R is a finite product of matrix rings over division rings. □

Lemma 22. *Let R be right artinian, and A a simple R-module with right annihilator P. If B is a finite dimensional subspace of A over the division ring $D = End_R(A)$, and $I = ann_R\ B_R$, then $aI = 0$ implies $a \in B$.*

Proof. The proof is by induction on $dim_D\ B = n$. If $n = 0$, then $R = ann_R\ B_R$, so $aR = 0$ implies $a = 0$. Let B be an n-dimensional subspace of A, and let B_1 be a subspace of B of dimension $n - 1$. By the induction hypothesis, with $I_1 = ann_R\ (B_1)_R$, $aI_1 = 0$ implies $a \in B_1$ for any $a \in A$. We must show that $aI = 0$ implies $a \in B$ where $I = ann_R\ B_R$. Equivalently, $cI \neq 0$ for any $c \in A \setminus B$.

Let $b \in B \setminus B_1$, and let $a \in A \setminus B$. We must show that $aI \neq 0$. If $br_1 = 0$ yet $ar_1 \neq 0$ for some $r_1 \in I_1$, then $r_1 \in I$, yet $0 \neq ar_1 \in aI$; we have finished. Suppose, on the other hand, that $br_1 = 0$ implies $ar_1 = 0$ for all $r_1 \in I_1$. In this case, $br_1 = br_2$ if and only if $b(r_1 - r_2) = 0$ if and only if $a(r_1 - r_2) = 0$ if and only if $ar_1 = ar_2$. Therefore, the map $\theta : bI_1 \to aI_1$ given by $\theta(br_1) = ar_1$ is a well-defined R-linear map.

By induction, $bI_1, aI_1 \neq 0$, and because A is simple, $bI_1 = aI_1 = A$. Thus, the map $\theta \in D = End_R(A)$. Note, $\theta(br_1) - ar_1 = 0 = (\theta(b) - a)r_1$ for all $r_1 \in I_1$. By induction again, $\theta(b) - a \in B_1$ and consequently, $a = a - \theta(b) + \theta(b) \in B$ since B is a D-linear space. This contradicts $a \notin B$, and therefore there exists $r_1 \in I_1$ such that $br_1 = 0$ while $ar_1 \neq 0$; that is, $aI \neq 0$ as desired. □

Corollary 23. *R is simple artinian if and only if $R \cong Mat_n(D)$ for some n and some matrix ring D.*

Proof. Assume that R is simple and artinian. As in the proof of the theorem, if P is the right annihilator of a simple right R-module, then $R/P \cong Mat_n(D)$ for some n and some matrix ring D. But R is simple, so $P = 0$. The converse is Exercise 5.2. □

Corollary 24. *The following are equivalent:*

(1) *R is semi-simple as a right module.*
(2) *R is semi-simple as a left module.*
(3) *Every right R-module is projective.*
(4) *Every left R-module is projective.*
(5) *Every right R-module is injective.*
(6) *Every left R-module is injective.*

Proof. For pedagogical reasons, the proof of this theorem will be carried out for the finitely generated case; the general case holds with very little adaptation.

(1) → (3): Every module H has a projective resolution:

$$\oplus_n R \to H,$$

where n is the size of a generating set for H. Write $R = I_1 \oplus I_2 \oplus \cdots \oplus I_m$ for simple (right or left) ideals $I_1, I_2, \ldots, I_m$ of R (Artin-Wedderburn Theorem). Since the image of a simple module is simple,

$$H = \Sigma_j X_j,$$

where X_j is isomorphic to one of the I_i's.

We can easily find a sub-collection of the X_j's indexed by $X_1, X_2, \ldots, X_k$ (after reindexing) so that $H = \oplus_j X_j$. Since each X_j is isomorphic to some I_i, we can write $H \cong I_1^{\ell_1} \oplus I_2^{\ell_2} \oplus \cdots \oplus I_m^{\ell_m}$. With $F = \oplus^{\ell} R$, $\ell = max\{\ell_1, \ell_2, \ldots, \ell_m\}$,

$$F \cong H \oplus K,$$

where $K = I_1^{k_1} \oplus I_2^{k_2} \oplus \cdots \oplus I_m^{k_m}$ with $k_j = \ell - \ell_j$, for all j.

(3) ↔ (5): Recall that a module A (respectively C) is injective (respectively projective) if and only if every short exact sequence

$$0 \to A \to B \to C \to 0,$$

splits. Hence, every module is injective if and only if every module is projective.

(5) → (1): Let $soc(R)$ (read, the socle of R) be the submodule of R generated by all of the simple right ideals of R. We need to show that $soc(R) = R$. By (5), $R = soc(R) \oplus X$ since $soc(R)$ is injective.

Suppose $0 \neq r \in X$. Let M be a right submodule of X maximal with respect to $r \notin M$. Then every submodule of X/M must contain $r+M$. It follows that the submodule C of X/M generated by $r+M$ is simple.

By (5), the simple submodule C of X splits out of X, so that $X = C \oplus Y$ for some module Y. Thus, $soc(R) \oplus C$ is contained in R and is a sum of simple modules, contrary to the maximality of $soc(R)$ as the sum of all simple modules. Therefore $X = 0$ and $R = soc(R)$.

The equivalence of (2), (4) and (6) is handled analogously. The equivalence of (1) and (2) is a consequence of the Artin-Wedderburn Theorem. □

12. EXERCISE SET 5

1. Let V be the vector space of dimension n as a left module over the division ring D; where V consists of all n-tuples with entries in D.
   (a) Viewing V as a collection of row vectors, show that $S = Mat_n(D)$ is equal to $End_D(V)$ (which operates via right multiplication).
   (b) Show that V is a simple S-module.
2. A ring R is called *simple* if R has no proper 2-sided ideals. Show that $R = Mat_n(D)$ where D is a division ring is simple and artinian on either side (you can pick a side and do that case).
3. Let $R = R_1 \times R_2 \times \cdots \times R_m$ as rings. Given a side, show that R is artinian if and only if each R_j is artinian.
4. Let $R = R_1 \times R_2 \times \cdots \times R_m$ as rings. Show that R is semi-simple as a right (left) R-module if and only if each R_j is semi-simple as a right (left) R_j-module.
5. Show that a matrix ring over a division ring is semi-simple artinian (on either side). Conclude that a product of matrix rings over division rings is semi-simple artinian (on either side).
6. Let A_1, A_2 be simple right R-modules with endomorphism rings $D_i = End_R(A_i)$. Show $A_1 \cong A_2$ as R-modules if and only if $D_1 \cong D_2$ as rings. This in turn is equivalent to one of D_i being isomorphic to a subring of the other.

13. Field Theory

Throughout this subject matter, F is a field with subfield K. We will investigate the relationship between K and a subfield E of F containing K. We assume that the notation $K \leq E$ acknowledges the relationship that K is a subfield of E.

For fields $K \leq E$, E is a vector space over K; the dimension of E over K, is also called the *degree* of E over K, and is denoted by

$$[E \ : \ K] = dim_K \ E.$$

Theorem 25. *Let $K \leq E \leq F$ be fields. Then*

$$[F \ : \ K] = [F \ : \ E] \cdot [E \ : \ K].$$

Proof. Let $\mathcal{A} = \{ \ \alpha_i \mid i \in I\}$ be a basis for E as a vector space over K, and $\mathcal{B} = \{ \ \beta_j \mid j \in J\}$ be a basis for F as a vector space over E. We claim that the elements $\alpha_i\beta_j$ for $i \in I$ and $j \in J$ form a basis for F over K.

Suppose

$$\Sigma_{i,j} a_{i,j}\alpha_i\beta_j = 0,$$

for $a_{i,j} \in K$ (almost all zero) and $i \in I$, $j \in J$. Since the sum is finite, we obtain

$$\Sigma_j(\Sigma_i a_{i,j}\alpha_i)\beta_j = 0,$$

which implies $\Sigma_i a_{i,j}\alpha_i = 0$ for each j since $\Sigma_i a_{i,j}\alpha_i \in E$ and $\mathcal{B}$ is a basis for F over E. But then, $a_{i,j} = 0$ for all i, j because $\mathcal{A}$ is a basis for E over K. Therefore $\alpha_i\beta_j = \alpha_{i'}\beta_{j'}$ if and only if $i = i'$ and $j = j'$, and

$$\{\alpha_i\beta_j \mid i \in I, \ j \in J \ \},$$

is a K-independent set of cardinality $|I| \cdot |J|$.

If $\delta \in F$, then $\delta = \Sigma_j b_j\beta_j$ for some $b_j \in E$ (almost all zero) since $\mathcal{B}$ is a basis for F over E. For each j, write

$$b_j = \Sigma_i a_{i,j}\alpha_i,$$

with $a_{i,j} \in K$ (almost all zero). Then

$$\delta = \Sigma_j(\Sigma_i a_{i,j}\alpha_i)\beta_j = \Sigma_{i,j} a_{i,j}\alpha_i\beta_j.$$

Therefore

$$\mathcal{AB} = \{ \ \alpha\beta \mid \alpha \in \mathcal{A}, \ \beta \in \mathcal{B} \ \},$$

is a basis for F over K of cardinality $|\mathcal{A}| \cdot |\mathcal{B}|$. □

Example 8. *The element $\sqrt{2}+\iota \in \mathbb{C}$ is algebraic of degree 4 over $\mathbb{Q}$.*

Proof. Let $\alpha = \sqrt{2}+\iota$. Then $(\alpha-\sqrt{2})^2 = -1$, and so $\alpha^2+2+1 = 2\sqrt{2}\alpha$. Thus, α is a root to $(x^2+3)^2 - 8x^2$, and so the degree of α is less than or equal to 4. However, the degree of α coincides with the dimension of $\mathbb{Q}[\alpha]$ over Q.

Observe, $\sqrt{2} = \alpha^{-1}(\alpha^2+3)/2 \in \mathbb{Q}[\alpha]$, and consequently $\iota \in \mathbb{Q}[\alpha]$ as well. We have $\mathbb{Q} \leq \mathbb{Q}[\sqrt{2}] \leq \mathbb{Q}[\alpha]$, and so

$$[\mathbb{Q}[\alpha] \ : \ \mathbb{Q}] = [\mathbb{Q}[\alpha] \ : \ \mathbb{Q}[\sqrt{2}]][\mathbb{Q}[\sqrt{2}] \ : \ \mathbb{Q}].$$

Since $[\mathbb{Q}[\alpha] \ : \ \mathbb{Q}[\sqrt{2}]]$ is not 1 ($\iota \notin \mathbb{Q}[\sqrt{2}]$), but is less than or equal to 2 (α is a root to $x^2 - 2\sqrt{2}x + 3$), we conclude $[\mathbb{Q}[\alpha] \ : \ \mathbb{Q}[\sqrt{2}] = 2$, and α has degree 4. □

There are possible distinctions between subfields. For example, $\mathbb{Q}[\sqrt[3]{2}]$ contains a root to $x^3 - 2$ while $\mathbb{Q}[\sqrt[3]{2}, \sqrt{3}\iota]$ contains all roots.

Kronecker's Theorem . Let $f(x) \in K[x]$ be irreducible.

(1) There exists a field extension E of K that contains a root α to $f(x)$.
(2) If K' is a field isomorphic to K under $\sigma : K \to K'$, and E' is a field extension of K' containing a root α' of σf (where σf is the polynomial formed by applying σ to the coefficients of f), then there exists an isomorphism of fields

$$K[\alpha] \cong K'[\alpha']$$

with $k \in K \mapsto \sigma(k)$ and $\alpha \mapsto \alpha'$.

Proof. (1): Let $E = K[x]/(f)$, a field containing K canonically. The root to $g(y)$ is $\alpha = x + (g)$. Hence $E = K[\alpha]$ contains a root to $f(y)$.

(2): The extension of σ to a map from $K[x] \to K'[x]$ which sends $g(x) \in K[x]$ to σg, the polynomial in $K'[x]$ obtained by applying σ to each of the coefficients of $g(x)$ is an isomorphism of rings;

$$K[x] \cong K'[x].$$

Hence,

$$K[\alpha] \cong K'[\alpha'],$$

by the construction in (1) (necessarily σf is irreducible).

□

Corollary 26. *Given any polynomial $f(x) \in K[x]$, there is a field extension E of K such that $f(x)$ splits into a product of linear factors. Moreover, $E = K[\alpha_1, \alpha_2, \ldots, \alpha_m]$ where α_j are the roots of $f(x)$ in E.*

The field E in this corollary is called a *splitting field* for $f(x)$ over K. It is an easy proof by induction on the degree of $f(x)$ that splitting fields are unique up to isomorphism.

The *Galois group* of F over K is

$$G = Aut_K(F);$$

that is, G is the group (under composition of maps) of K-linear automorphisms $\sigma : F \to F$. If $\sigma \in G$, then $\sigma(k) = k\sigma(1) = k$ for all $k \in K$ (i.e., each element of K is fixed under σ). Conversely, if each element of K is fixed under a field automorphism $\sigma : F \to F$, then $\sigma(k \cdot a) = \sigma(k)\sigma(a) = k\sigma(a)$, so σ is K-linear.

Corollary 27. *If $\sigma \in G$ and $\alpha \in F$ is a root to $f(x) \in K[x]$, then $\sigma(\alpha)$ is also a root to $f(x)$.*

Proof. The map σ induces an automorphism of $F[x]$. On the one hand, $\sigma f = f$ since σ fixes K point-wise, and on the other, $f(x) = (x-\alpha)g(x)$ for some $g(x) \in K[x]$ and so $f = \sigma f = (x - \sigma(\alpha))\sigma g$. □

As a consequence, the more roots to a given $f(x)$, F possesses, the more automorphisms F has. Note that if $\theta : F \to F$ is an field automorphism and F contains $\mathbb{Q}$, then $n\theta(m/n) = f(m) = m$ and so $\theta(m/n) = m/n$. I.e., θ fixes $\mathbb{Q}$ automatically.

Example 9. *The extension field $\mathbb{Q}[\sqrt[3]{2}]$ of $\mathbb{Q}$ contains a single root of $x^3 - 2$ while $\mathbb{Q}[\sqrt[3]{2}, \sqrt{3}\iota]$ contains all roots $e^{2k\pi\iota/3}\sqrt[3]{2}$, $k = 0, 1, 2$ to $x^3 - 2$. The Galois group of $\mathbb{Q}[\sqrt[3]{2}]$ over $\mathbb{Q}$ is the trivial group, while there is an automorphism $\sigma : \mathbb{Q}[\sqrt[3]{2}, \sqrt{3}\iota] \to \mathbb{Q}[\sqrt[3]{2}, \sqrt{3}\iota]$ sending $\sqrt[3]{2}$ to $e^{2\pi\iota/3}\sqrt[3]{2}$.*

To see this, by the last theorem, there is an isomorphism

$$\theta : \mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[e^{2\pi\iota/3}\sqrt[3]{2}],$$

sending $\sqrt[3]{2}] \mapsto e^{2\pi\iota/3}\sqrt[3]{2}$. By the theorem again, this isomorphism extends to an automorphism of

$$\mathbb{Q}[\sqrt[3]{2}, \sqrt{3}\iota] =$$

$$(\mathbb{Q}[\sqrt[3]{2}])[\sqrt{3}\iota] = (\mathbb{Q}[e^{2\pi\iota/3}\sqrt[3]{2}])[\sqrt{3}\iota]$$

extending θ and sending $\sqrt{3}\iota \mapsto \sqrt{3}\iota$.

Example 10. *In the last example we constructed an automorphism of $F = \mathbb{Q}[\sqrt[3]{2}, \sqrt{3}\iota]$ sending $\sqrt[3]{2}$ to $e^{2\pi\iota/3}\sqrt[3]{2}$ and sending $\sqrt{3}\iota$ to $\sqrt{3}\iota$. Likewise, there are 5 other automorphisms of F; calling the one mentioned above, σ_1, we have:*

$$\begin{array}{lll}
\sigma_0: & \sqrt[3]{2} \mapsto \sqrt[3]{2} & \sqrt{3}\iota \mapsto \sqrt{3}\iota \\
\sigma_1: & \sqrt[3]{2} \mapsto e^{2\pi\iota/3}\sqrt[3]{2} & \sqrt{3}\iota \mapsto \sqrt{3}\iota \\
\sigma_2: & \sqrt[3]{2} \mapsto e^{2\pi\iota/3}\sqrt[3]{2} & \sqrt{3}\iota \mapsto -\sqrt{3}\iota \\
\sigma_3: & \sqrt[3]{2} \mapsto e^{4\pi\iota/3}\sqrt[3]{2} & \sqrt{3}\iota \mapsto \sqrt{3}\iota \\
\sigma_4: & \sqrt[3]{2} \mapsto e^{4\pi\iota/3}\sqrt[3]{2} & \sqrt{3}\iota \mapsto -\sqrt{3}\iota \\
\sigma_5: & \sqrt[3]{2} \mapsto \sqrt[3]{2} & \sqrt{3}\iota \mapsto -\sqrt{3}\iota
\end{array}$$

Note that F is the splitting field of $x^3 - 2$ and is of degree 6 over $\mathbb{Q}$, and there are 6 distinct automorphisms of F.

The splitting field of $x^p - 1$ has degree p. The splitting field in this case is $\mathbb{Q}[\rho]$ where $\rho = e^{2\pi\iota/p}$. Since $x^p - 1$ is irreducible (undergraduate exercise; $(x+1)^p - 1$ is irreducible by Eisenstein's Criterion) with ρ as a root, $\mathbb{Q}[\rho]$ has degree p over $\mathbb{Q}$). So the obvious conjecture that the splitting field of an irreducible polynomial of degree n has degree $n!$ is incorrect.

The Fundamental Theorem of Galois is a detailed description of the correspondence between subgroups of G and subfields of F containing K.

Given a subgroup H of G,

$$H' = \{\ t \in F \mid \theta(t) = t\ \forall\ \theta \in H\ \}.$$

Given a subfield E of F containing K,

$$E' = Aut_E(F) = \{\theta \in G \mid \theta(t) = t\ \forall\ t \in E\ \}.$$

In Hungerford, the field F is called a *Galois extension* of K, provided

$$G' = K.$$

Example 11. *The extension field $\mathbb{Q}[\sqrt[3]{2}]$ of $\mathbb{Q}$ has Galois group $\{\ 1_F\ \}$ and $\{\ 1_F\ \}' = F \neq \mathbb{Q}$, so $\mathbb{Q}[\sqrt[3]{2}]$ is not a Galois extension of $\mathbb{Q}$. We will show shortly that $\mathbb{Q}[\sqrt[3]{2}, \sqrt{3}\iota]$ is Galois over $\mathbb{Q}$.*

Fundamental Theorem of Galois . Let F be a finite dimensional Galois extension of K, and let G be the Galois group of F over K.

(i) There is a bijective, order-reversing correspondence between the subfields of F containing K and the subgroups of G given by

$$E \mapsto Aut_E(F) \ \text{ and } \ H \leq G \mapsto H' \leq F.$$

(ii) Under this correspondence, an intermediate field $K \leq E \leq F$ corresponds to a normal subgroup of G if and only if E is Galois over K; and $[E : K]$ is the index of $Aut_E(F)$ in G.

14. EXERCISE SET 6

1. Let $\alpha \in F$. Show that $K[\alpha]$ is a field if it has finite dimension over K.
2. Let $\alpha, \beta \in F$ be algebraic over K having degrees n and m respectively. Show that
$$[K[\alpha, \beta] \ : \ K] \leq m \cdot n,$$
and equality holds if n and m are relatively prime.
3. Let $f(x), g(x) \in K[x]$ and let F be an extension field of K. Show that the gcd of f and g is 1 in $F[x]$ if and onlt if the gcd of f and g is 1 in $K[x]$.
4. A irreducible polynomial $f(x) \in K[x]$ is called *separable* if $f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$ with $a \in K$ and $\alpha_1, \alpha_2, \ldots, \alpha_k$ distinct, in E for any splitting field E for $f(x)$. Show that an irreducible polynomial $f(x) \in K[x]$ is separable if and only the gcd of f and its derivative f' is 1 in $K[x]$.
5. Recall that a finite field is a field extension of $\mathbb{Z}_p$ for some p and consequently must have order p^n for some n. Show that F is a finite field if and only if F is the splitting field of $x^{p^n} - x$ for some prime p and natural number n. Consequently, two finite fields F_1, F_2 are isomorphic if and only if $|F_1| = |F_2|$. (Hint: $\Rightarrow$ If $|F| = p^n$, note that $F^* = F \setminus \{0\}$ is a finite abelian group of order p^{n-1}. Furthermore, $f = x^{p^n} - x$ has distinct roots (consider the gcd of f with its derivative f'). $\Leftarrow$ In the splitting field of $x^{p^n} - x$, the roots form a field; hence the splitting field is the collection of the roots.)
6. Let E, E' be subfields of F containing K and suppose $\sigma : E \cong E'$ is an isomorphism fixing K. Assume that F is the splitting field of a separable polynomial $f(x) \in K[x]$. Using Kronecker's Theorem and induction on $[F \ : \ E]$, argue that there are $[F \ : \ E]$ automorphisms $\tilde{\sigma} \in G$ such that $\tilde{\sigma}|_E = \sigma$.
7. Diminishing Returns: Let G be the Galois group of F over K. Show that $(Aut_{H'}(F))' = H'$ for every $H \leq G$ and that $Aut_E(F) = Aut_{(Aut_E(F))'}(F)$ for every intermediate field $K \leq E \leq F$.

15. The Fundamental Theorem of Galois

Before embarking on a proof of the Main Theorem of Galois, we will examine the hypothesis of that result. Let us recall the Fundamental Theorem of Linear Algebra:

If M is an $m \times n$ matrix over a field, then

$$\text{rank } M \ + \ \text{nullity } M \ = \ n.$$

To prove this, row reduce M. The number of columns in the row-reduced form that do not contain a leading nonzero entry of a row is the nullity of M (i.e., the dimension of the nullspace of A), and the number of columns containing a leading nonzero entry of a row is the rank of M (rank M = dimension of the column space of M = dimension of the row space of M).

Assume

$$[F \ : \ K] < \infty$$

throughout, and let

$$G = Gal(F/K) = Aut_K(F).$$

Remember that an automorphism $\sigma : F \to F$ fixes K if and only if σ is K-linear.

A Lemma of Dedekind . If $\sigma_1, \sigma_2, \dots, \sigma_m \in G$ are distinct, then they are linearly independent.

Proof. The proof will be by induction on m; clearly the case $m = 1$ is settled in the affirmative. Suppose, for the sake of induction, that

$$(1) \quad a_1\sigma_1 + a_2\sigma_2 + \cdots + a_m\sigma_m = 0,$$

with not all $a_i's$ equal to zero. By induction, we assume that all $a_i's$ are nonzero. Multiplying through by a_m^{-1} we may assume that $a_m = 1$.

Since $\sigma_1 \neq \sigma_n$, there exists $t \in F$ such that $\sigma_1(t) \neq \sigma_m(t)$. Evaluating (1) at ts for $s \in F$ arbitrary, and multiplying both sides by $\sigma_m(t)^{-1}$, we obtain

$$\sigma_m(t)^{-1}[a_1\sigma_1(ts) + a_2\sigma_2(ts) + \cdots + \sigma_m(ts)] =$$

$$a_1\sigma_m(t)^{-1}\sigma_1(t)\sigma_1(s) + \cdots + a_1\sigma_m(t)^{-1}\sigma_{m-1}(t)\sigma_{m-1}(s) + \sigma_m(s) = 0.$$

Evaluating (1) at s and subtracting this last equation, we have

$$a_1[1 - \sigma_m(t)^{-1}\sigma_1(t)]\sigma_1(s) + a_2[1 - \sigma_m(t)^{-1}\sigma_2(t)]\sigma_2(s) +$$

$$\cdots + a_{m-1}[1 - \sigma_m(t)^{-1}\sigma_1(t)]\sigma_{m-1}(s) = 0,$$

for every $s \in F$. That is,

$$a_1[1 - \sigma_m(t)^{-1}\sigma_1(t)]\sigma_1 + \cdots + a_{m-1}[1 - \sigma_m(t)^{-1}\sigma_1(t)]\sigma_{m-1} = 0.$$

This contradicts the inductive hypothesis since, in particular, $a_1[1 - \sigma_m(t)^{-1}\sigma_1(t)] \neq 0$. □

Lemma 28. *If $H \leq G$, then*

$$[F : H'] \geq |H|.$$

Proof. Let H consist of $\sigma_1, \sigma_2, \ldots, \sigma_m$, and let $u_1, u_2, \ldots, u_k$ be a basis for F over H'. Suppose to the contrary that $m > k$, and consider the system of linear equations

$$\begin{gathered}\sigma_1(u_1)x_1 + \sigma_2(u_1)x_2 + \cdots + \sigma_m(u_1)x_m = 0\\ \sigma_1(u_2)x_1 + \sigma_2(u_2)x_2 + \cdots + \sigma_m(u_2)x_m = 0\\ \cdots\cdots\cdots\cdots\\ \sigma_1(u_k)x_1 + \sigma_2(u_k)x_2 + \cdots + \sigma_m(u_k)x_m = 0\end{gathered}$$

over F. We know there exists a nontrivial solution $(x_1, x_2, \ldots, x_m)$.

For any $\beta \in F$, write $\beta = \Sigma_j b_j u_j$ for $b_j \in H'$. Multiplying the i^{th} equation by b_i and adding we obtain

$$\sigma_1(\beta)x_1 + \sigma_2(\beta)x_2 + \cdots + \sigma_m(\beta)x_m = 0$$

contradicting Dedekind's Lemma. □

Theorem 29. *If $H \leq G$, then*

$$[F : H'] = |H|.$$

Proof. It remains to show that

$$[F : H'] \leq |H|.$$

Let H consist of $\sigma_1, \sigma_2, \ldots, \sigma_m$, and suppose that F contains $m + 1$ elements $u_1, u_2, \ldots, u_{m+1}$ which are linearly independent over H'. Consider the system of linear equations

$$\begin{gathered}\sigma_1(u_1)x_1 + \sigma_1(u_2)x_2 + \cdots + \sigma_1(u_{m+1})x_{m+1} = 0\\ \cdots\cdots\cdots\cdots\\ \sigma_m(u_1)x_1 + \sigma_m(u_2)x_2 + \cdots + \sigma_m(u_{m+1})x_{m+1} = 0\end{gathered}$$

Let j be the minimal number of nonzero components in a nontrivial solution to the system. Choose a nontrivial solution with j terms and reorder the $u_j's$ (if necessary) so that this solution is of the form

$(a_1, a_2, \dots, a_j, 0, \dots, 0)$ such that $a_1, \dots, a_j$ are nonzero, and $a_j = 1$. Note that $j > 1$. Because any σ_i is H'-linear, not all of the $a_i's$ can belong to H'. Assume (by reordering the $u_i's$) that $a_1 \notin H'$; so, $\sigma_k(a_1) \neq a_1$ for some k.

Applying σ_k to the ℓ^{th}-row in the system

$$(1) \quad \sigma_\ell(u_1)a_1 + \sigma_\ell(u_2)a_2 + \cdots + \sigma_\ell(u_j)a_j = 0$$

we obtain

$$\sigma_k\sigma_\ell(u_1)\sigma_k(a_1) + \sigma_k\sigma_\ell(u_2)\sigma_k(a_2) + \cdots + \sigma_k\sigma_\ell(u_j)\sigma_k(a_j) = 0.$$

But $\sigma_k H = H$, and so for every i there exists an ℓ such that $\sigma_k\sigma_\ell = \sigma_i$.

Subtract the equation

$$\sigma_i(u_1)\sigma_k(a_1) + \sigma_i(u_2)\sigma_k(a_2) + \cdots + \sigma_i(u_j)\sigma_k(a_j) = 0.$$

from the equation pointed to by (1) but corresponding to i to obtain a new system whose i^{th} row is

$$\sigma_i(u_1)[a_1 - \sigma_k(a_1)] + \cdots + \sigma_i(u_j)[a_j - \sigma_k(a_j)] =$$

$$\sigma_i(u_1)[a_1 - \sigma_k(a_1)] + \cdots + \sigma_i(u_{j-1})[a_{j-1} - \sigma_k(a_{j-1})] = 0,$$

since $a_j = 1$. But $a_1 - \sigma_k(a_1) \neq 0$, so we have found a solution to the original system with fewer than j nonzero terms; a contradiction. □

The hypothesis of the Fundamental Theorem of Galois poses a restriction on the field extension F (unlike the previous results of this section). F is called a *Galois extension* of K if F satisfies any (hence all) of the conditions of the next result.

Galois Extension Theorem . The following are equivalent:

(1) $[F : K] = |G|$.
(2) $G' = K$.
(3) Every monic irreducible polynomial in $K[x]$ that has a root in F, is separable and splits in $F[x]$.
(4) F is the splitting field of a separable polynomial in $K[x]$.

Proof. (1) → (2) By the last theorem,

$$[F : G'] = |G|.$$

Since

$$|G| = [F : K] = [F : G'][G' : K] = |G|[G' : K],$$

$[G' : K]$ must be 1.

(2) → (3) By the previous theorem, $[F : G'] = |G| = [F : K]$. Let $p(x) \in K[x]$ be monic, irreducible, with a root α in F, and consider

$$g(x) = \Pi_j(x - \alpha_i),$$

where $\alpha_1, \ldots, \alpha_k$ are the distinct members of the set $\{\sigma(\alpha) \mid \sigma \in G\}$. If we apply any $\sigma \in G$ to the coefficients of $g(x)$ we find that σ fixes $g(x)$, and therefore $g(x) \in G'[x] = K[x]$. Since the gcd of $g(x)$ and $p(x)$ in $F[x]$ is not 1, the gcd of $g(x)$ and $p(x)$ in $K[x]$ cannot be 1. Therefore, p divides g implying that p is separable.

(3) → (4) If $\alpha \in F$, then α is algebraic and is the root of a separable (irreducible) polynomial $p(x)$. If the splitting field E of $p(x)$ inside F, differs from F, let $\beta \in F \setminus E$; β is a root to a separable polynomial $p_2(x) \in K[x] \leq E[x]$, and the splitting field of $p(x)p_2(x)$ inside F properly contains E. Since $[F : K] < \infty$, we will obtain F as a splitting field of a separable polynomial in $K[x]$ after a finite number of steps.

(4) → (1) By Exercise 6.6, there are $[F : K]$ automorphisms which extend the identity map $1_K : K \to K$. I.e., $[F : K] = |G|$.

□

Let $Sub\ G$ denote the set of subgroups of G and $Int\ F/K$ the (lattice of) intermediate subfields of F containing K. Both sets $Sub\ G$ and $Int\ G$ have *containment* as the partial order.

Fundamental Theorem of Galois . Let F be a Galois extension of K. Then:

(i) The map $Sub\ G \to Int\ F/K$ given by $H \mapsto H'$ is an order-reversing bijection with inverse $E \mapsto Aut_E(F)$.
(ii) $Aut_{H'}(F) = H$ and $E = Aut_E(F)'$.
(iii) $[E : K] = [G : Aut_E(F)]$ and $[G : H] = [H' : K]$.
(iv) E is Galois over K if and only if $Aut_E(F)$ is normal in G.

Proof. If $H_1' = H_2'$, then it is easy to see that $(H_1H_2)' = H_1' = H_2'$. Theorem 29 reveals

$$[F : (H_1H_2)'] = |H_1H_2| = [F : H_1'] = |H_1|.$$

Thus, $H_1 = H_1H_2$. Similarly $H_2 = H_1H_2 = H_1$. Note; the hypothesis was not needed for this part. We next argue that $Aut_{E_1}(F) = Aut_{E_2}(F)$ implies $E_1 = E_2$. Now, E_1E_2 (consists of finite sums of products a_1a_2, $a_i \in E_i$) is finite dimensional over K, hence is a subfield of F containing both E_1, E_2. It readily checks that $Aut_{E_1E_2}(F) = Aut_{E_i}(F)$, so we may assume that $E_1 \subseteq E_2$, in order to show that $E_1 = E_2$.

If there exists an $\alpha \in E_2 \setminus E_1$, then α is a root to an irreducible and separable polynomial $p(x) \in K[x]$ which splits in F (Galois Extension Theorem). Let $g(x)$ be an irreducible factor of $p(x)$ in $E_1[x]$ that has α as a root. Then $g(x)$ is separable (it divides $p(x)$) and has degree at least 2, so there exists another root α' to $g(x)$ in F. By Exercise 6.6, there exists $\sigma \in G$ such that σ fixes E_1 and $\sigma(\alpha) = \alpha'$. Then $\sigma \in Aut_{E_1}(F)$ but is not in $Aut_{E_2}(F)$. Thus, $E_1 = E_2$.

To finish (i) we need to establish (ii). But (ii) follows from Exercise 6.7; we know $H' = (Aut_{H'}(F))'$ and so by what we have shown above, $H = Aut_{H'}(F)$. Similarly, $E = (Aut_E(F))'$. We next verify the claims about the indices:

By Theorem 29, $[F : H'] = |H|$ and by Lagrange's Theorem and Theorem 25, $[H' : K] = [G : H]$. Putting in $E = H'$ we obtain $[E : K] = [G : Aut_E(F)]$ since $H = Aut_E(F)$ from (ii).

If E is Galois over K, then E is the splitting field of a separable polynomial $g(x)$ in $K[x]$. If $\sigma \in G$, then σ must permute the roots of $g(x)$ in some fashion, and so $\sigma(E) \subseteq E$. Therefore $\sigma^{-1}\delta\sigma(a) = \sigma^{-1}\sigma(a) = a$ for every $a \in E$ and $\sigma^{-1}\delta\sigma \in Aut_E(F)$, for $\delta \in Aut_E(F)$. Conversely, suppose $p(x) \in K[x]$ is irreducible with a root $\alpha \in E$ (we already know that p is separable since F is Galois), yet another root α' of p is in $F \setminus E$. Then, there exists $\sigma \in G$ such that $\sigma(\alpha) = \alpha'$ and σ fixes E by Exercise 6.6. For $H = Aut_E(F)$, $H_1 = \sigma H \sigma^{-1}$ fixes α'. Since

$$[F : H_1'] = |H_1| = |H| = [F : H'] = [F : E],$$

it is impossible for H_1' to contain E. Hence $H_1 \neq H$. I.e., if E is not Galois, then $Aut_E(F)$ is not normal in G. $\square$

16. The Galois Group, Finite Fields and Simple Extensions

Every finite dimensional extension F of K is

$$F = K[\alpha_1, \alpha_2, \dots, \alpha_k],$$

for some elements $\alpha_1, \alpha_2, \dots, \alpha_k$, algebraic over K. It turns out, in the case of a Galois extension, that

$$F = K[\alpha]$$

for a single algebraic element α. This is also the case in the context $\mathbb{Q} \subseteq K$.

Lemma 30. *Any finite subgroup of $F^* = F \setminus 0$ is cyclic.*

Proof. Observe that an abelian group C of order n is cyclic if and only if for each divisor d of n, C has at most 1 cyclic subgroup of order d. To see this, if $C = \langle c \rangle$ is cyclic (written multiplicatively), then $\langle c^{n/d} \rangle$ is the only cyclic subgroup of order d. Conversely, write $C = C_1 \times C_2 \times \cdots \times C_j$ with C_i primary. Then, C is cyclic if and only if the $C_i's$ correspond to distinct primes. But, if C_i and C_ℓ are p-primary for a given prime p, then C has two cyclic subgroups of order p contrary to the assumption.

Let C be a subgroup of order n of the multiplicative group F^* and let d divide n. Any cyclic subgroup B of F^* of order d consists of the roots of $x^d - 1$ in F. Therefore, there is at most one such subgroup B and so C can have at most one cyclic subgroup of order d. Thus, C is cyclic. □

Corollary 31. *If F is a finite field, then F^* is cyclic.*

Primitive Element Theorem . If F is a finite dimensional Galois extension of K, then

$$F = K[\alpha],$$

for some algebraic element α.

Proof. By the lemma, it suffices to assume that F is infinite. It suffices to argue that for $\alpha, \beta \in F$, that $K[\alpha, \beta] = K[\delta]$ for some $\delta \in F$. By the Galois Correspondence Theorem, there are only finitely many intermediate subfields of F containing K. On the other hand, there are infinitely many distinct elements of the form $\alpha + a\beta$ for $0 \neq a \in F$. Choose two such elements; $\alpha + a\beta, \alpha + b\beta$ with $a \neq b$, such that

$$K[\alpha + a\beta] = K[\alpha + b\beta].$$

Evidently, $\alpha, \beta \in K[\alpha + a\beta]$, and so $\delta = \alpha + a\beta$ satisfies our purpose. □

If F is the splitting field of a separable polynomial $f(x) \in K[x]$ of degree n, then clearly

$$|G| \;=\; [F \;:\; K] \;\leq\; n!,$$

since any $\sigma \in G$ must permute the roots of $f(x)$ and is determined by how σ permutes the roots of $f(x)$. That is,

$$G \;\leq\; S_n,$$

the symmetric group on n letters.

Theorem 32. *If F is the splitting field of an irreducible polynomial $f(x)$ of degree p (a prime) over $\mathbb{Q}$, and $f(x)$ has exactly two non-real roots, then*

$$G \cong S_p.$$

Proof. Since $|G| \;=\; [F \;:\; \mathbb{Q}]$ is divisible by p, G has an element σ of order p by Cauchy's Theorem. We now argue that σ is a cycle of length p: Express σ as a product of disjoint cycles $\delta_1 \cdots \delta_i$; the order of σ, p, is the least common multiple of the lengths of the $\delta_j's$; hence one of the $\delta's$ (hence σ) is a cycle of length p.

Let E be the subfield of F generated by all of the real roots of f and let α and $\bar{\alpha}$ be the two complex roots. Since F is the splitting field of f over E, the irreducible polynomial for α over E must have degree 2 (i.e., the irreducible factor of f in $E[x]$ having α as a root must be of degree 2 since the only roots that do not split out of f over E are α and $\bar{\alpha}$). There is an automorphism of F fixing E but sending $\alpha \;\mapsto\; \bar{\alpha}$. In summary, under the identification of G with S_p, G contains a transposition and a cycle of length p. Since S_p is generated by any such pair, $G = S_p$. □

Definition . Given a field extension K of $\mathbb{Q}$, a polynomial $f(x) \in K$ is said to be solvable by radicals if the roots of $f(x)$ can be expressed using algebraic combinations and radical combinations of the coefficients of $f(x)$.

Example 12. *For $f(x) = x^3+ax+b$, the roots of $f(x)$ are given below:*

$$x = A + B \;=\; -\frac{A+B}{2} + \frac{A-B}{2}\sqrt{-3} \;=\; -\frac{A+B}{2} - \frac{A-B}{2}\sqrt{-3},$$

where $A \;=\; \sqrt[3]{-\frac{b}{2} + \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}}$, and $B \;=\; \sqrt[3]{-\frac{b}{2} - \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}}$. The general cubic $x^3 + ux^2 + vx + w$ can be transformed into a cubic in the

above form by setting

$$a = \frac{1}{3}(3v - u^2), \text{ and } b = \frac{1}{27}(2u^3 - 9uv + 27w).$$

Example 13. *Given the general quartic equation* $x^4+ax^3+bx^2+cx+d$, *the roots can be found as follows:*

Let y *be any root to* $y^3 - by^2 + (ac - 4d)y - a^2d + 4bd - c^2$; *and*

$$R = \sqrt{\frac{a^2}{4} - b + y}.$$

If $R \neq 0$, *take*

$$D = \sqrt{\frac{3a^2}{4} - R^2 - 2b + \frac{4ab - 8c - a^3}{4R}}$$

and

$$E = \sqrt{\frac{3a^2}{4} - R^2 - 2b - \frac{4ab - 8c - a^3}{4R}}.$$

If $R = 0$, *take*

$$D = \sqrt{\frac{3a^2}{4} - R^2 - 2b + 2\sqrt{y^2 - 4d}}$$

and

$$E = \sqrt{\frac{3a^2}{4} - R^2 - 2b - +2\sqrt{y^2 - 4d}}.$$

The four roots of the original quartic are

$$x = -\frac{a}{4} + \frac{R}{2} \pm \frac{D}{2} \text{ and } -\frac{a}{4} - \frac{R}{2} \pm \frac{E}{2}.$$

Recall that a finite group G is *solvable* if there exists a chain

$$G_0 = \langle 1 \rangle < G_1 < \cdots < G_n = G$$

such that G_i is normal in G_{i+1}, and G_{i+1}/G_i is cyclic for all i.

Big Theorem of Galois . Let K be a subfield of $\mathbb{C}$, and let $f(x) \in K[x]$. Then, $f(x)$ is solvable by radicals if and only if the Galois group of the splitting field of $f(x)$ over K is a solvable group.

Example 14. *The polynomial $x^5 - 4x^2 + 2 \in \mathbb{Q}[x]$ is irreducible by Eisenstein's Criterion, and has exactly 2 non-real roots. Hence, the Galois group of $x^5 - 4x^2 + 2$ over $\mathbb{Q}$ is S_5; a group that is not solvable. Therefore, the polynomial is not solvable by radicals.*

Example 15. *The polynomial $f(x) = x^p - 1$ splits into $(x-1)(x^{p-1} + \cdots + 1)$. For any prime p, $g(x) = x^{p-1} + \cdots + x + 1$ is irreducible. To see this observe that $f(x+1) = xg(x+1)$ is equal to*

$$x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-1}x + 1 - 1.$$

So $g(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-1}$.

The coefficient of x_j, $j < p-1$, is $\binom{p}{p-j}$ and is divisible by p, while the constant term, p, is not divisible by p^2. So $g(x+1)$, hence g, is irreducible. Therefore, the splitting field $F = \mathbb{Q}[\rho]$ of $f(x)$ (and g) has degree $p-1$ where $\rho = e^{2\pi\iota/p}$. The Galois group of f (and g) is abelian and is isomorphic to the cyclic group $\mathbb{Z}^*_{(p)}$. The isomorphism sends $\sigma \in G$ to $j \in \mathbb{Z}^*_{(p)}$ where $\sigma(\rho) = \rho^j$.

Theorem 33. *Let K be a subfield of $\mathbb{C}$. The splitting field of $x^n - 1$ over K has an abelian Galois group of order at most $\varphi(n)$ (where φ is the Euler phi-function). If $K = \mathbb{Q}$, then G has order $\varphi(n)$.*

Proof. The splitting field F is obtained as $F = K[\rho]$ where $\rho = e^{2\pi\iota/n}$. If $\sigma \in G$ (the Galois group), then $\sigma(\rho) = \rho^j$. Evidently, ρ^j must be a primitive n^{th} root of unity, and so j must be relatively prime to n. I.e., the map from G into $\mathbb{Z}^*_{(n)}$ has image in $\mathbb{Z}^u_{(n)}$, the group of units in $\mathbb{Z}^*_{(n)}$. This establishes the first part.

Set

$$g_m(x) = \Pi_\delta(x - \delta),$$

where the product is indexed over all primitive m^{th} roots of unity. Evidently

$$(x^n - 1) = \Pi_{d|n} g_d(x).$$

We will prove by induction that $g_d(x) \in \mathbb{Z}[x]$.

For the sake of induction, set $f(x) = \Pi\{(x-\delta) \mid \delta \text{ is a primitive } d^{th}-\text{root of unity, for } d|n,\ d < n\} = \Pi_{d|n, d<n} g_d(x)$. By induction, $f(x) \in \mathbb{Z}[x]$ and is monic. Performing long division by $f(x)$ on $x^n - 1$ in $\mathbb{Z}[x]$, we find that the quotient $g_n(x)$, must be in $\mathbb{Z}[x]$. We will now argue that $g_n(x)$ is irreducible over $\mathbb{Q}$. □

For a sketch of the proof of Galois' Big Theorem, first assume that f is solvable by radicals. By the definition of f being solvable by radicals, the splitting field F of f is related to K as follows:

$$K = E_0 \subseteq E_1 = E_0[\alpha_1] \subseteq E_2 = E_1[\alpha_2] \subseteq \cdots \subseteq E_n = E_{n-1}[\alpha_n],$$

such that E_n contains the splitting field F, and for each j there exists m_j with $\alpha_j^{m_j} \in E_{j-1}$. Note that if ρ is a primitive k^{th} root of unity and δ is a primitive ℓ^{th} root, then $\delta\rho$ is a primitive $lcm\{k, \ell\}^{th}$ root of unity. With regard to this chain, we will assume that α_1 is a primitive $m = lcm\{m_1, m_2, \ldots, m_n\}$ root of unity, and furthermore, that each m_j is a prime. Because of this, note that each E_j is the splitting field over E_{j-1} (it splits $x^{m_j} - \alpha_j$); and an easy proof by induction using the Galois Extension Theorem, shows that E_n is a splitting field over K.

Because F is Galois over K, $Aut_F(E_n)$ is a normal subgroup of the Galois group H of E_n over K, and the Galois group of f is isomorphic to $H/Aut_F(E_n)$. Since quotient groups of solvable groups are solvable, it is enough to argue that H is solvable. Since each E_j is a splitting field over E_{j-1} of prime degree, we obtain

$$Aut_{E_n}(E_n) \leq Aut_{E_{n-1}}(E_n) \leq Aut_{E_{n-2}}(E_n) \leq \cdots \leq Aut_K(E_n) = H,$$

with $Aut_{E_{j-1}}(E_n)/Aut_{E_j}(E_n) \cong Aut_{E_{j-1}}(E_j)$ primary, cyclic. Hence H is solvable.

17. EXERCISE SET 7

1. In the Galois extension $F = \mathbb{Q}[\sqrt[3]{2}, \sqrt{3}\iota]$ over $K = \mathbb{Q}$, find all intermediate subfields. Acknowledge the subfields that are Galois over K
2. Do the same as in 1. but for $x^4 - 5$ over $\mathbb{Q}$.
3. Determine the Galois group of (the splitting field for) $(x^3 - 2)(x^2 - 3)$ over $\mathbb{Q}$.
4. Assume that F is Galois over K. Show that $[H_1 \ : \ H_2] = [H_2' \ : \ H_1']$ for any subgroups $H_2 \leq H_1$ of G, and $[E_1 \ : \ E_2] = [Aut_{E_2}(F) \ : \ Aut_{E_1}(F)]$ for any intermediate fields $E_2 \leq E_1$ between F and K.
5. Let G be the Galois group of the polynomial $x^{11} - 1$ over the rational field $\mathbb{Q}$. Determine this well-known group. Show all of the necessary work.
6. Determine the Galois group of the polynomial $x^{10} - 1$ over the rational field $\mathbb{Q}$. Show all of the necessary work.
7. Determine the Galois group of $x^5 - 6x + 3$ over the rational field $\mathbb{Q}$. Show all of the necessary work.