Roughly lecture notes from Kevin Buzzard's Algebra 3 and Alessio Corti's Galois theory

1 Rings

Definition 1.1.1 (Ring)**.** A ring (with 1) is a set R with elements $0, 1$ and binary operations $+, \times$ such that

1. $(R, +)$ is an abelian group with identity 0,
2. $(R, \times)$ is a semigroup with 1 as the identity,
3. both left and right multiplication are distributive over addition.

Examples 1.1.2. The following are common examples of rings:

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all rings with their normal operations,
2. $n\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ with n a positive integer, are both rings,
3. $\mathbb{R}[x]$, informally the set of polynomials with real coefficients, and $\mathbb{Q}[x]$ are rings,
4. given some set X and a ring R the set of functions $f : X \to R$ is a ring
5. given a ring R, $M_{n\times n}(R)$ is a ring.

Definition 1.1.3 (Commutative ring)**.** A ring, R, is **commutative** iff $a \times b = b \times a$ for all $a, b \in R$.

Definition 1.1.4 (Subring)**.** A subset of a ring which is itself a ring under the same operators is a **subring**.

Lemma 1.1.5. If R is a ring and $0_R, 1_R, s, t \in S \subseteq R$ with $s + t, st, s - t \in S$ then S is a subring of R.

Proof. The only non-obvious axiom is that S is closed under additive inverses which is given by $s-t \in S$. □

Example 1.1.6. $\mathbb{Z}[\sqrt{n}]$ with $n \in \mathbb{Z}$ is a ring; and note $a + b\sqrt{n} = c + d\sqrt{n}$ iff $a = c$ and $b = d$.

Proof. $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{C}$ so by Lemma 1.1.5 take $r = a+b\sqrt{n}$ and $s = c+d\sqrt{n}$, and by simple manipulations have $r \pm s, rs \in \mathbb{Z}[\sqrt{n}]$. Arguing by contradiction that $\sqrt{d}$ is not rational gives the uniqueness. □

Corollary 1.1.7. The same argument extends to show $\mathbb{Q}[\sqrt{n}]$ is a ring and in fact a field.

Proof. Commutativity is inherited from $\mathbb{Q}$, if $r = a + b\sqrt{n} \neq 0$, $r^{-1} = \dfrac{a - b\sqrt{n}}{a^2 - b^2 d}$ with $a^2 - b^2 d \neq 0$ easily coming from the irrationality of $\sqrt{d}$. □

Propositions 1.1.8. Have R a ring with $r, s, r_i, s_j \in R$ for $i \in [1, n]$ and $j \in [1, m]$ respectively:

1. $r0 = 0r = 0$,
2. $(-r)s = r(-s) = -(rs)$ and $(-r)(-s) = rs$,
3. $\left(\sum_{i=1}^{n} r_i\right) \sum_{j=1}^{m} s_j = \sum_{i=1}^{n} \sum_{j=1}^{m} r_i s_j$,
4. if $rs = s$ then $r = 1$,
5. if $0 = 1$ in R, $R = \{0\}$.

Proof.
1. $0 + 0 = 0 \implies r(0 + 0) = r0 \implies r0 + r0 = r0 \implies r0 = 0$ and similarly for $0r$,
2. $r - r = 0 \implies (r - r)s = 0s = 0 \implies (-r)s + rs = 0 \implies (-r)s = -(rs)$ with $r(-s)$ and $(-r)(-s) = rs$ immediately following,
3. inducting on $m + n$ and distributivity,
4. $s = 1$ is sufficient,
5. for any r, $r = r1 = r0 = 0$, note $\{0\}$ is still a ring. □

Definition 1.1.9 (Invertible)**.** An element x of a ring R is invertible if there exists $y, z \in R$ with $yx = xz = 1$.

Definition 1.1.10 (Division ring)**.** A ring R is called a **division ring** if every element of R is invertible.

Remark 1.1.11. A commutative division ring is a field.

Definition 1.1.12 (Zero divisor)**.** An element a of a ring R is a **zero division** if there exists some $b \neq 0 \in R$ with $ab = 0$.

Definition 1.1.13 (Integral domain)**.** A ring with 1, R, is an **integral domain** iff R is commutative, has no zero divisors, and $0 \neq 1$.

Examples 1.1.14.
1. $\mathbb{Z}$ is an integral domain,
2. all fields are integral domains,
3. $\{0\}$ is not an integral domain,
4. a subring of an integral domain is also an integral domain,
5. $\mathbb{Z}/n\mathbb{Z}$ is an integral domain iff n is prime.

Proof of 5. ($\implies$) If $n = 1$ we have $\mathbb{Z}/1\mathbb{Z} = \{0\}$, otherwise take $n = ab$ then $ab = 0$ in $\mathbb{Z}/n\mathbb{Z}$ so neither are an integral domain. ($\impliedby$) By lifting a and b to the integers we have $a', b' < n$ prime so $a, b \nmid n$ hence $ab \nmid n$ therefore $ab \neq 0$ in $\mathbb{Z}/n\mathbb{Z}$ which is therefore an integral domain. □

Proposition 1.1.15. There is non-zero cancellation in integral domains.

Proof. Have $ar = as \implies a(r-s) = 0$ as a is non-zero $\implies r - s = 0 \implies r = s$ □

Lemma 1.1.16. A finite integral domain is a field.

Proof. Consider $a \in R$ an integral domain with $\varphi_a : R \to R$ by $\varphi_a(r) = ar$. By cancellation φ_a is injective and as R is finite φ_a is therefore also surjective and hence bijective. Take $a^{-1} = \varphi_a^{-1}(1)$. □

Corollary 1.1.17. $\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime.

Theorem 1.1.18 (Wedderburn)**.** A finite division ring is a field. *Proof hard so left until later...*

1.2 Ring homomorphisms

Definition 1.2.1 (Ring homomorphism)**.** Let R, S be rings, a function $f : R \to S$ is a **ring homomorphism** iff it satisfies

1. $f : (R, +) \to (S, +)$ is a group homomorphism,
2. $f(xy) = f(x)f(y)$ for all $x, y \in R$,
3. $f(1_R) = 1_S$.

A ring homomorphism $\varphi : R \to S$ is an **isomorphism** if there exists some $\psi : R \to S$ with $\varphi \circ \psi$ and $\psi \circ \varphi$ both identity maps.

Examples 1.2.2. The following are some common examples of ring homomorphisms:

1. $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ with $\varphi(t) = t \pmod{n}$, and $[0], [1]$ the identities,
2. $f : \mathbb{C} \to \mathbb{C}$ with $f(z) = \overline{z}$ is in fact a self-inverse ring isomorphism,
3. $\varphi_\lambda : \mathbb{R}[x] \to \mathbb{R}$ which evaluates a polynomial at $\lambda \in \mathbb{R}$,
4. structure preserving inclusions are also ring homomorphisms.

Definition 1.2.3 (Ideal)**.** For a ring R, a subset $I \subseteq R$ is a **left ideal**, denoted $I \trianglelefteq R$ iff

1. $(I, +)$ is a subgroups of $(R, +)$,
2. if $r \in R$ and $i \in I$, $ri \in R$.

Similarly, for **right ideals**. A subset I is a bi-ideal if it is both a left and right ideal.

Examples 1.2.4.
1. For any ring R, $\{0\}$ and R are always ideals,

2. $x\mathbb{R}[x]$ is an ideal for $\mathbb{R}[x]$,
3. $m\mathbb{Z}$ is an ideal for $\mathbb{Z}$ and in fact all ideals are of this form.

Definition 1.2.5 (Quotient ring)**.** Given a ring R with $I \lhd R$, have **cosets** of R by I be the subsets of R in the form $r + I := \{r + i : i \in I\}$, the set of these cosets, R/I is the **quotient ring** of R by I under the operations $(r + I) + (s + I) = (r + s + I)$ and $(r + I)(s + I) = (rs + I)$.

Proof. The structure of R translates directly to R/I so it is clearly a ring. □

Lemma 1.2.6. The kernel of a ring homomorphism $\varphi : R \to S$ is an ideal.

Proof. The kernel of φ is a subgroup of R and $\varphi(ir) = \varphi(i)\varphi(r) = 0\varphi(r) = 0$ so $ir \in \ker\varphi$ and similarly for ir hence $\ker\varphi$ is a bi-ideal. □

Lemma 1.2.7. The image of a ring homomorphism $\varphi : R \to S$ is a subring.

Proof. By Lemma 1.1.5 and ring homomorphism axioms. □

Theorem 1.2.8. Have $\varphi : R \to S$ a ring homomorphism, $\operatorname{im}\varphi$ is naturally isomorphic to $R/\ker\varphi$.

Proof. Have $\psi : R/\ker\varphi \to \operatorname{im}\varphi$ by $\psi(r + I) = \varphi(r)$.

(well defined) $r + \ker\varphi = r' + \ker\varphi \implies r - r' \in \ker\varphi \implies \varphi(r) = \varphi(r')$,

(injective) the same argument but backwards,

(subjective) any $\varphi(r)$ for $r \in R$ is $\psi(r + I)$. □

Proposition 1.2.9. A commutative ring R is a field iff its only 2 ideals are $\{0\}$ and R.

Proof. $(\implies)$ as R a field $\{0\} \neq R$, if there is some other ideal $0 \neq I \subseteq R$, $x \in R \implies 1 = (x)^{-1}x \in I \implies 1r = r \in I$ for general $r \in R$ so $I = R$.
$(\impliedby)$ given some $r \in R$ have $I = \{ar : a \in R\}$ clearly a non-empty ideal so $I = R$ therefore there exists some $a \in R$ with $ar = 1$. □

Proposition 1.2.10. Given $f : R \to S$ a ring homomorphism with J a left (or right or bi) ideal of S, $f^{-1}(J)$ is a left (respectively) ideal of R.

Proof. □

Definition 1.2.11 (Prime ideal)**.** Let R be a commutative ring, a proper ideal $I \subset R$ is a **prime ideal** iff $ab \in I$ for $a, b \in R \implies a \in I$ or $b \in I$.

Proposition 1.2.12. If $I \subset R$ is a prime ideal, R/I is an integral domain.

Proof. □

Definition 1.2.13 (Maximal ideal)**.** A proper ideal I in a commutative ring R is **maximal** iff there are no other proper ideals J with $I \subset J$.

Proposition 1.2.14. I is a maximal ideal of R iff R/I is a field.

Proof. □

Corollary 1.2.15. Maximal ideals are prime in commutative rings.

Proof. □

Corollary 1.2.16. $\{0\}$ is a prime ideal of a commutative ring R iff R is an integral domain. $\{0\}$ is a maximal ideal of R iff R is a field.

Proof. □

Corollary 1.2.17. The maximal ideal of $\mathbb{Z}$ are $p\mathbb{Z}$ for prime p, the remaining non-maximal prime ideal is $\{0\}$.

Proof. □

1.3 Generators of ideals

Definition 1.3.1 (Generated ideal)**.** Have R a commutative ring (this is not necessary just much simpler) with finite $X = \{x_1, \dots, x_n\} \subseteq R$, the **ideal generated by** X is the set $I := \{r_1 x_2 + \cdots + r_n x_n : r_i \in R\}$. Write $I = (x_1, \dots, x_n)$.

Lemma 1.3.2. Under the same definitions as above, I is the smallest ideal of R containing X.

Proof. □

Remark 1.3.3. If X is infinite then I is still the collection of finite *linear combinations* of X in R.

Definition 1.3.4. An ideal I of the commutative ring R is **finitely generated** if $I = (x_1, \dots, x_n)$ for some $x_i \in R$. Furthermore, I is **principal** if $I = (x)$ for some $x \in R$.

Definition 1.3.5. A commutative ring R is **Noetherian** if all ideals of R are finitely generated; and call R a **principal ideal domain** if all ideals of R are principal.

Remark 1.3.6. Consider R being Noetherian roughly as R being "finite dimensional" and R being a PID as being "leq 1 dimensional".

1.4 Factorisation

Throughout this section we will always have R be an integral domain.

Definition 1.4.1 (Unit)**.** $r \in R$ is a **unit** if there exists some $y \in R$ with $x \times y = 1_R$. We write $R^\times$ for the group of units in R under multiplication.

Examples 1.4.2. Some common examples of units in rings:

1. $\mathbb{Z}^\times = \{1, -1\}$,
2. $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$,
3. given $d < -1$, $\mathbb{Z}[\sqrt{d}]^\times = \{1, -1\}$,
4. given a field F, $F[x]^\times = F^\times$.

Definition 1.4.3 (Associates)**.** If $x, y \in R$, x and y are **associates** iff $x = uy$ for some unit u.

Proposition 1.4.4. Association is an equivalence relation on any integral domain, $x \sim y$ iff $(x) = (y)$.

Proof. □

Proposition 1.4.5. If $x \in R$ is a unite, $(x) = R$.

Proof. □

Definition 1.4.6 (Irreducible)**.** $r \in R \setminus R^\times$ is **irreducible** if it cannot be written as the product of two elements of $R \setminus R^\times$.

Examples 1.4.7. Common examples of irreducible elements in rings:

1. the irreducible elements of $\mathbb{Z}$ is all $\pm p$ for a prime p,
2. the irreducible elements of $\mathbb{Z}[i]$ are the set of associates of primes congruent to 3 modulo 4,
3. in $\mathbb{R}[x]$ the polynomial $x^2 + 1$ is irreducible, however in $\mathbb{C}[x]$, $x^2 + 1 = (x + i)(x - i)$; and in fact by the fundamental theorem of algebra, irreducible elements in $\mathbb{C}[x]$ are all order 1 polynomials.

Proof of 2. □

Definition 1.4.8. A reminder of a very familiar definition, a number p is **prime** iff $p | ab \implies p | a$ or $p | b$.

Lemma 1.4.9. All primes of R are irreducible.

Proof. □

Proposition 1.4.10. If $0 \neq r \in R$, then r is prime iff (r) is a prime ideal.

Proof. □

Definition 1.4.11 (Euclidean domain)**.** R is a Euclidean domain if there exists some $\varphi : R^* \to \mathbb{Z}_{\geq 0}$ satisfying:

1. $\varphi(ab) \geq \varphi(a)$ for all $a, b \neq 0$,
2. if $a, b \in R$ with $b \neq 0$ there exists $q, r \in R$ with $a = qb + r$ with either $r = 0$ or $\varphi(r) \leq \varphi(b)$.

Examples 1.4.12.

1. $\mathbb{Z}$ is a euclidean domain with $\varphi(n) = |n|$,
2. given some field k, $k[x]$ is a euclidean domain with $\varphi(p) = \deg(p)$

Theorem 1.4.13. R is a Euclidean domain $\implies$ R is a PID.

Proof. □

Corollary 1.4.14. If k is a field, $k[x]$ is a PID. *Proof.* Obvious □

Lemma 1.4.15. All irreducibles in a PID are prime.

Definition 1.4.16 (Unique factorisation domain)**.** R is a **unique factorisation domain** if:

(U1) if $r \neq 0 \in R$, $r = ur_1 \dots r_n$ for some unit u and $r_i \in R$ with $n \geq 0$,

(U2) if $r = ur_1 \dots r_n = vs_1 \dots s_m$ for units u, v and $r_i, s_i \in R$ with $m, n \geq 0$, $m = n$ and (after reordering) r_i and s_i are associates for all i.

Examples 1.4.17. $\mathbb{Z}$, $k[x]$, $\mathbb{Z}[i]$ and any ED are all UFDs.

Theorem 1.4.18. All PIDs are UFDs.

Proof. □

1.5 Localisation

Definition 1.5.1 (Multiplicative subset)**.** Given $S \subseteq R$ a commutative ring, S is a **multiplicative subset** of R if $1 \in S$ and $s, t \in S \implies st \in S$.

Definition 1.5.2 (Localisation)**.** Have R an integral domain with S a multiplicative subset without 0, the **localisation** of R at S is the set of equivalence classes of $(R \times S)/\sim$ with $(r_1, s_1) \sim (r_2, s_2) \iff r_1 s_2 = r_2 s_1$. Denoted R_S or $S^{-1}R$

Theorem 1.5.3. Have R an integral domain, the localisation of R by $R \setminus \{0\}$ called the **field of fractions** is a unique field up to isomorphism and is denoted $\mathrm{Frac}(R)$

Proof. □

Corollary 1.5.4. Any integral domain is a subring of a field.

Lemma 1.5.5. Have R a commutative ring with S a multiplicative subset of R and $\varphi : R \to A$ a ring homomorphism such that $\varphi(s)$ is a unit in A for all $s \in S$. There exists some $\tilde{\varphi} : R_S \to A$ extending φ.

Proof. □

Examples 1.5.6.

1. if $S = \{1\}$, $S^{-1}R = R$,
2. if $p \in \mathbb{Z}$ is a prime and $S = \{1, p, p^2, \dots\}$, $S^{-1}\mathbb{Z} = \mathbb{Z}[\frac{1}{p}]$ which is a subring of $\mathbb{Q}$,
3. have $P = (p)$ for a prime $p \in \mathbb{Z}$ and $S = \mathbb{Z}/P$ then $S^{-1}\mathbb{Z} = \mathbb{Z}_{(p)}$

Proposition 1.5.7. $\mathbb{Q}$ has uncountably many subrings.

1.6 Zorn's lemma

Definition 1.6.1 (Partial order)**.** A **partial order** on a set is a binary relation, $\leq$ satisfying:

(P1) for all $s \in S$, $s \leq s$,

(P2) if $s \leq t$ and $t \leq s$ then $s = t$,

(P3) if $s \leq t$ and $t \leq u$ then $s \leq u$.

Definition 1.6.2 (Chain)**.** A **chain** in a poset S is a subset $T \subseteq S$ where $\leq$ is total.

Definition 1.6.3 (Upper bound, maximal element)**.** An **upper bound** for $W \subseteq S$ a poset is some $s \in S$ such that for all $w \in W$, $w \leq s$. A maximal element of S is an element $x \in S$ such that $x \leq y \implies x = y$ for all $y \in S$.

Example 1.6.4. Have $s_1 \subseteq s_2 \subseteq \cdots$ subsets of X, then $s = \bigcup_{n \geq 1} s_n$ and X are both upper bounds.

Axiom 1.6.5 (Zorn's Lemma)**.** If S is a poset such that every chain in S has an upper bound, S has a maximal element (and possibly multiple).

Remark 1.6.6. Zorn's lemma is equivalent to the axiom of choice.

Theorem 1.6.7. If R is a ring with $I \lhd R$, there exists some maximal ideal m with $I \subseteq m \subset R$.

Proof. □

Corollary 1.6.8. If $R \neq \{0\}$ then it has a maximal ideal.

Proposition 1.6.9. An ideal I of a commutative ring R is the unique maximal ideal iff R is the disjoint union of I and $R^\times$.

Definition 1.6.10 (Local)**.** A commutative ring is **local** if it has a unique maximal ideal.

Proposition 1.6.11. Have R an integral domain with $P \subset R$ a prime ideal and $S = R/P$, $S^{-1}R$ is a local ring with unique maximal ideal $S^{-1}P$.

Proof. □

1.7 Polynomial rings

Definition 1.7.1 (Polynomial ring)**.** Let R be a commutative ring, formally, the **polynomial ring** $R[x]$ is the set of infinite sequences with terms in R and finitely many nonzero terms. Informally it is convenient to view this as the set of polynomials with coefficients in R. $R[x, y] := (R[x])[y]$.

Proposition 1.7.2. If R is an integral domain, so is $R[x]$.

Proof. □

Corollary 1.7.3. If R is an integral domain, so is $R[x_1, \ldots, x_n]$.

Theorem 1.7.4 (Hilbert basis theorem)**.** If R is Noetherian, so is $R[x]$.

Proof. □

Corollary 1.7.5. If R is a field or PID, $R[x_1, \ldots, x_n]$ is Noetherian.

Proof. R is clearly Noetherian so by induction on n. □

Lemma 1.7.6. Have $\varphi : A \to B$ a surjective ring homomorphism, if A is Noetherian then B is Noetherian.

Proof. □

Corollary 1.7.7. If R is a PID with $I \trianglelefteq R[x_1, \ldots, x_n]$ then $R[x_1, \ldots, x_n]/I$ is Noetherian.

Proof. □

1.8 Factorisation in polynomial rings

Definition 1.8.1 (π-adic valuation)**.** For some element $\pi \in X \subseteq R$ a UFD, the **π-adic valuation** on $F = \operatorname{Frac} R$ is the map $val_\pi : F^* \to \mathbb{Z}$ such that given some $f \neq 0 \in F$ written $f = u\pi^e \prod_{x_i \neq \pi \in X} x_i^{p_i}$, have $val_\pi(f) := e$.

Proposition 1.8.2. val_π is a group homomorphism $(F^*, \times) \to (\mathbb{Z}, +)$.

Remark 1.8.3. It can be useful to consider $val_\pi(0) := +\infty$ to have $val_\pi : F \to \mathbb{Z} \cup \{+\infty\}$.

Definition 1.8.4. Given $0 \neq q \in F[x]$ with $q = f_0 + f_1 x + \ldots + f_n x^n$ and $\pi \in X$, have $val_\pi(q) := \min_{i : f_i \neq 0} \{val_\pi(f_i)\}$.

Lemma 1.8.5.
1. $val_\pi(xy) = val_\pi(x) val_\pi(y)$,
2. if $val_\pi(x)$ and $val_\pi(y) > 0$, $val_\pi(x + y) = 0$.

Proof. □

Definition 1.8.6 (Content)**.** The **content** of $f \neq 0 \in F[x]$ is the finite product

$$cont(f) := \prod_{\pi \in X} \pi^{val_\pi(f)},$$

and say f is **primitive** when $cont(f) = 1$.

Remark 1.8.7. Given $f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, $cont(f) = \gcd(a_0, a_1, \ldots, a_n)$.

Lemma 1.8.8. $cont(f) \in R \iff f \in R[x]$, furthermore f is primitive iff $f \in R[x]$ with the coefficients of f having gcd 1.

Proof. □

Lemma 1.8.9. If $f \neq 0 \in F[x]$ and $\lambda \in F^\times$ then $cont(\lambda f) = u\lambda cont(f)$ for some unit u.

Proof. □

Lemma 1.8.10. Have R a UFD with $F = \operatorname{Frac}(R)$, if $f, g \neq 0 \in F[x]$ then $cont(fg) = cont(f)cont(g)$.

Proof. □

Corollary 1.8.11 (Gauss' Lemma)**.** Given a UFD R with $f \neq 0 \in F[x]$ and $\deg(f) \geq 1$. If f is irreducible in $R[x]$ then f is irreducible in $F[x]$.

Proof. □

Theorem 1.8.12. If R is a UFD, so is $R[x]$. Furthermore, the irreducible elements of $R[x]$ are the elements of R and primitive polynomials which are also units in $F[x]$.

Proof. □

Corollary 1.8.13. If R is a UFD, $R[x_1, \ldots, x_n]$ is a UFD. *Proof.* Trivial. □

2 Modules

2.2 Quotient modules

2.3 Snake lemma

2.4 Injective and projective modules

2.5 Hom

2.6 Tensor product

2.7 Semisimple modules

3 Galois

We will be working within the category of fields with objects fields and morphisms field homomorphisms.

Remark 3.1.1. Every morphism $\sigma : K \to L$ is injective, leading to $\mathrm{Hom}(K, L)$ being denoted as $\mathrm{Emb}(K, L)$.

Proof. Have $a \neq b \in K$, $\sigma(a) = \sigma(b) \implies \sigma(a-b) = 0_L \implies 1_L = \sigma(a-b)\sigma((a-b)^{-1}) = 0_L$. ※ □

Often a *ground field* k is considered and it is assumed that all fields K we have the extension $k \subset K$. We therefore find ourselves working in a modification of the category of fields where given our fixed ground field k, objects are extensions of k and morphisms are embeddings over k.

Definition 3.1.2 (Embedding over k)**.** Given $k \subset K$ and $k \subset L$, the **embedding over** k from K to L is

$$\mathrm{Emb}_k(K, L) := \{f \in \mathrm{Emb}(K, L) : \forall a \in k, f(a) = a\}.$$

Sometimes called k-embeddings of K in L.

Remark 3.1.3. If $K \subset L$ a field extension, L is a K-vector space. *Proof.* simple axiom checking. □

Definition 3.1.4 (Degree)**.** The **degree** of the extension $K \subset L$ is $[L : K] = \dim_K(L)$.

Proposition 3.1.5. If $[L : K] = 1$ then $L = K$.

Proof. □

Remark 3.1.6. If $k \subset K$ is finite then every element of $\mathrm{Emb}_k(K, K)$ is surjective (directly from rank-nullity) so $\mathrm{Emb}_k(K, K) = \mathrm{Aut}_k(K, K)$ a group. Unless stated otherwise assume all extensions to be finite.

Theorem 3.1.7 (Tower Law)**.** Given a tower $K \subset L \subset M$ of extensions, $[M : K] = [M : L][L : K]$.

Proof. □

3.2 Axioms

3.3 Fundamental theorem

3.4 Proof of axioms

3.5 Discriminants