GROUPS, RINGS, FIELDS AND GALOIS THEORY SUMMARY NOTES

HAO (BILLY) LEE

Abstract. These are summary notes I created for the REU program. I do not claim that they are without errors, nor readable. I didn’t use any references except for wikipedia to double check some definitions and theorems.

TO MY STUDENTS: DO ALL THE EXERCISES!!! In fact, you are not allowed to read ahead until you have done the exercises that appeared before.

1. Group Theory

Definition 1.1. A group \((G, \cdot)\) is a set \(G\) with a binary operation \(\cdot : G \times G \to G\) satisfying

1. Identity: There exists an identity element \(e\) such that \(g \cdot e = e \cdot g = g\) for all \(g \in G\).
2. Inverse: For all \(g \in G\), there exists an inverse \(g^{-1}\) such that \(g \cdot g^{-1} = e = g^{-1} \cdot g\).
3. Associativity: For all \(g, h, k \in G\), \((g \cdot h) \cdot k = g \cdot (h \cdot k)\).

Remark 1.2. Even though we often denote the group operation as multiplication, we can also denote the group operation by addition.

Definition 1.3. If \(g_1g_2 = g_2g_1\) in a group, it is called an abelian group. This property is usually called commutativity, and for everything else, we usually say “commutative” (ie. commutative ring). For historical reasons, we say abelian group instead (named after Abel). However, if you say commutative group, everybody will understand.

1.1. Definition and Examples of groups.

1. \((\mathbb{Z}, +)\), \((\mathbb{R}, +)\), \((\mathbb{R}\setminus\{0\}, \times)\)
2. Cyclic Groups: This is a group generated by one element

\[
\langle g \rangle = \{e, g, g^2, g^3, \ldots\}.
\]

This \(\langle \cdot \rangle\) notation will be used from now on to denote “the cyclic group generated by \(g\)”. Of course, the generator DOES NOT have to be unique (come up with an example yourself).

If the cyclic group is finite of order (size) \(n\), we usually denote this by \(C_n\) or \(\mathbb{Z}/n\mathbb{Z}\).

3. Symmetric Group:

\[
S_n = \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} \text{ bijections}\}.
\]

We can denote each \(\sigma \in S_n\) in cycle notation. For example, if \(\sigma \in S_6\) is the map

\[
\begin{array}{ccc}
1 & 2 & 3 \\
2 & 1 & \mapsto 3 \\
4 & 5 & \\
5 & 6 & \\
6 & & \\
& & \\
\end{array}
\]

then we can write \(\sigma = (12)(3)(456)\). The \((12)\) means that 1 gets mapped to 2, and 2 gets mapped to 1. The \((3)\) means that 3 gets mapped to itself. The \((456)\) means that 4 gets mapped to 5, 5 mapped to 6 and 6 mapped to 4. Each of these are called cycles. Note that we often ignore and omit 1-cycles, so \(\sigma = (12)(456)\).
Example 1.4. \((1\ 2\ 3)\ (2\ 3) = (1\ 2)\). This is because

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>(\rightarrow(2\ 3))</td>
<td>(\rightarrow(1\ 2\ 3))</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

The key thing to remember here, is that these cycles are still maps!! From composition of maps, we work from right to left!!

Exercise 1.5. Write down the multiplication table of \(S_3\).

(4) Dihedral Group: \(D_n\) is the group of symmetries of a regular \(n\)-gon. More explicitly, \(D_n = \langle x, y : x^n = 1, y^2 = 1, yxy = x^{-1} \rangle\).

This should be read as, the group generated by \(x, y\), (that is, all elements of the form

\[
1, x, x^2, x^3, ..., y, xy, x^2y, x^3y, ..., y^2, xy^2, x^2y^2, x^3y^2, ...
\]

subject to the condition that \(x^n = 1, y^2 = 1\) and \(yxy = x^{-1}\). You should draw a picture, and see that this group is in fact the group of symmetries. The \(x\) is a rotation by \(\frac{2\pi}{n}\), and \(y\) is one of the reflections.

Exercise 1.6. Check that from the symmetries definition, \(yxy = x^{-1}\).

Exercise 1.7. Check that \(|D_n| = 2n\), and give a set of representatives of the group \(D_n\).

Because of the above exercise, sometimes people use \(D_{2n}\) to denote the group of symmetries of a regular \(n\)-gon. I don’t like this notation... (if you like this notation, then shouldn’t we denote \(S_n\) by \(S_n!\) instead?).

1.2. Group Action. This is THE MOST IMPORTANT thing to know when studying groups. Seriously.

Definition 1.8. The LEFT action of a group \(G\) on a set \(X\) (denoted \(G \curvearrowright X\)) is a function \(f : G \times X \rightarrow X, (g, x) \mapsto gx\) satisfying

1. \(1 \cdot x = x\) for all \(x \in X\)
2. \((gh) \cdot x = g \cdot (h \cdot x)\) for all \(g, h \in G\) and \(x \in X\)

You can imagine what a right action would be.

Definition 1.9. A left action of a group \(G\) on \(X\) is said to be

1. Transitive if for all \(x, y \in X\), there exists \(g \in G\) such that \(g \cdot x = y\)
2. Faithful if for all \(g \neq h\) in \(G\), there exists \(x \in X\) such that \(g \cdot x \neq h \cdot x\)
3. Free if whenever \(g \cdot x = h \cdot x\) for some \(x \in X\) then \(g = h\)

Remark 1.10. I will be dropping the \(\cdot\) from now on

Example 1.11.

1. \(S_n\) acts on \(\{1, 2, ..., n\}\) canonically.

Exercise 1.12. Check that this action is transitive and faithful, but not free.

2. Suppose \(H\) is a subgroup of a group \(G\). Then \(H\) acts on \(G\) (viewed as just a set) by \(h \cdot g = hg\).
**Definition 1.13.** Suppose $G$ acts on $X$, then the orbit of $x \in X$ is defined to be

$$Gx = \{g \cdot x : g \in G\} \subseteq X.$$  

The set of orbits are denoted as $X/G$.

The stabilizer of $x \in X$ is defined to be

$$G_x = \{g \in G : gx = x\} \subseteq G.$$  

**Exercise 1.14.** Check that the stabilizer is in fact a subgroup of $G$.

**Exercise 1.15.** Check that being in the same orbit, is an equivalence relation.

**Definition 1.16.** Suppose $H \subseteq G$ is a subgroup of a group $G$. Define the index of $H$ in $G$ to be $[G : H] = \# (G/H)$ (from the earlier exercise in this subsection, we saw that $H$ acts on $G$, so this $G/H$ is just the set of orbits).

**Remark 1.17.** It is true that when $G$ and $H$ are finite,

$$[G : H] = \frac{|G|}{|H|}.$$  

However, this doesn’t make sense when $G$ and $H$ are infinite groups, this is why we used the previous definition.

**Example 1.18.** $\mathbb{Z}$ acts on $\mathbb{R}$ by translation (that is given $n \in \mathbb{Z}$ and $x \in \mathbb{R}$, $n \cdot x = x + n$. Make sure you understand what I just wrote, it’s not a mistake). Then $\mathbb{R}/\mathbb{Z} = [0, 1)$ (really, the $= \,$ here is an abuse of notation. What I really should write is

$$\mathbb{R}/\mathbb{Z} = \{x + \mathbb{Z} : x \in [0, 1)\},$$  

so I have chosen a canonical representation). If you are familiar with topology, notice that translation is a continuous map. So in fact, $\mathbb{R}/\mathbb{Z}$ is a topological space, which is isomorphic to the circle ([0, 1]/0 ∼ 1).

**Theorem 1.19.** Orbit-Stabilizer theorem. If $G$ is a finite group acting on a set $X$ then for all $x \in X$,

$$|Gx| = [G : G_x] = \frac{|G|}{|G_x|}.$$  

**Remark 1.20.** NOTE!! This says that it is not necessarily true that all the orbits are of the same size!

**Theorem 1.21.** *(Burnside’s Lemma).*

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

where

$$X^g = \{x \in X : gx = x\}$$  

is the set of elements fixed by $g$. *(We will use the generalization of this notation, so $X^G$ for example, means

$$\{x \in X : gx = x \text{ for all } g \in G\}$$  

is the set of elements fixed by everything).*

1.3. **Morphisms and Subgroups.**

**Definition 1.22.** $H$ is a subgroup of $G$ is $H \subseteq G$ is a subset that is also a group.

A subgroup $H$ is said to be normal, if for all $g \in G$, $gHg^{-1} = H$ (or $gH = Hg$).

**Remark 1.23.** You can think of normal subgroups in the following way. We saw that the group $H$ acts on the group $G$, so we have cosets $G/H = \{gH : g \in G\}$. If we want $G/H$ to be a group, then we need inverses (the identity is canonically $1H = H$). The guess for the inverse of $gH$ would be $g^{-1}H$. If this is the case, then we need

$$(gH)(g^{-1}H) = 1H = H.$$
This is true if \( ghg^{-1}H = H \) if \( ghg^{-1} = H \).

**Exercise 1.24.** What we have just shown, is that if \( G/H \) is a group, then \( H \) better be normal. Now finish it. That is, prove that if \( H \subseteq G \) is normal, then \( G/H \) is a group (check the other axioms).

**Definition 1.25.** A homomorphism between groups \( G \) and \( H \) is a map \( f : G \to H \) satisfying:

1. \( f(1_G) = 1_H \) (maps the identity element of \( G \) to that of \( H \))

2. \( f(g_1g_2) = f(g_1)f(g_2) \) for all \( g_1, g_2 \in G \)

An isomorphism between \( G \) and \( H \) is a bijective maps \( f : G \to H \) such that \( f \) and \( f^{-1} \) are homomorphisms.

**Exercise 1.26.** If \( f : G \to H \) is a bijective homomorphism, then \( f^{-1} \) is also a homomorphism.

**Remark 1.27.** Later on in your mathematical career (or if you can follow Peter May’s lectures), you will come across the notion of a category. Basically, a category consists of objects and morphisms between the objects. Groups form a category, so do vector spaces, topological spaces etc. The morphisms are then those maps between the elements of the objects that preserve the important properties. For groups, the morphisms are group homomorphisms, linear maps for vector spaces, and continuous maps for topological spaces.

**Definition 1.28.** Suppose \( f : G \to H \) is a group homomorphism. Define

\[
\text{im}(f) = \{ h \in H : \exists g \in G \text{ such that } f(g) = h \}
\]

is called the image. Define

\[
\ker(f) = \{ g \in G : f(g) = 1_H \}
\]

is called the kernel of \( f \).

**Exercise 1.29.** The kernel of \( f \) is a normal subgroup of \( G \), and \( \text{im}(f) \) is a subgroup of \( H \) (not necessarily normal).

**Theorem 1.30.** First isomorphism theorem. Suppose \( f : G \to H \) is a homomorphism, then \( G/\ker(f) \cong \text{im}(f) \) (\( \cong \) means isomorphic to). In particular, if \( f \) is surjective then \( G/\ker(f) \cong H \).

**Theorem 1.31.** Second isomorphism theorem. Let \( H \subseteq G \) be a subgroup and \( N \) another normal subgroup of \( G \). Then \( HN \subseteq G \) is a subgroup (EXERCISE!), \( H \cap N \) is a normal subgroup of \( H \) and \( (HN)/N \cong H/(H \cap N) \). This is best understood via the diagram

\[
\begin{array}{ccc}
HN & \cong & H \\
\downarrow & & \downarrow \\
N & H \cap N & H
\end{array}
\]

The theorem just says that the quotient of the left arrow is the same as the quotient of the right arrow.

**Theorem 1.32.** Third Isomorphism Theorem. Let \( G \) be a group, \( N \subseteq G \) a normal subgroup. Then

1. If \( H \) is another subgroup of \( G \) with \( N \subseteq H \subseteq G \) then \( H/N \) is a subgroup of \( G/N \). If \( H \) is normal in \( G \), then \( H/N \) is normal in \( G/N \).

2. Every subgroup of \( G/N \) is of the form \( H/N \) for some subgroup \( H \) of \( G \) of the above form. Similarly, for normal subgroups.

3. The quotient \( G/N \cong G/\overline{N} \).

1.4. Misc but important theorem.

**Theorem 1.33.** (Lagrange) Let \( G \) be a finite group. Then every subgroup \( H \subseteq G \) divides the order of \( G \) (so \( |H| \mid |G| \)). This implies that if \( g \in G \), then \( g \) must have order dividing \( |G| \) (because \( g \) is a subgroup).
Theorem 1.34. (Cauchy) If $p$ is a prime number with $p | |G|$ (finite group) then there exists $g \in G$ with order exactly $p$.

Theorem 1.35. (Cayley’s) Every finite group is isomorphic to a subgroup of some symmetric group $S_n$ for some $n$. That is, there exists an injective map $G \rightarrow S_n$ for some $n$.

Remark 1.36. This last theorem isn’t really as useful as it seems. I’ve only ever used it once to show that every finite group is the Galois group of some arbitrary extension of fields.

Remark 1.37. There are also the Sylow theorems, that we can probably ignore.

I will put more exercises up.

2. Rings

Definition 2.1. A ring $R$ is a set with two binary operations $+: R \times R \rightarrow R$ and $\cdot: R \times R \rightarrow R$ such that $(R, +)$ is a group, multiplication is associative and distributivity $a(b + c) = ab + ac$

for all $a, b, c \in R$.

Exercise 2.2. Prove that $0 \cdot a = 0$ for all $a \in R$ and $-a = (-1) \cdot a$ for all $a \in R$ (these are not given by the axioms!!).

Example 2.3. The polynomial ring over $\mathbb{Z}$ and $\mathbb{R}$ (denoted $\mathbb{Z}[x]$ and $\mathbb{R}[x]$). More specifically,

$$\mathbb{Z}[x] = \{a_n x^n + a_{n-1} x^{n-1} + ... + a_0 : a_0, ..., a_n \in \mathbb{Z}\}.$$ 

You can imagine what $R[x]$ means for general ring $R$, and what $R[x_1, ..., x_n]$ means. These are all rings.

Remark 2.4. From now on, we will assume that all of our rings are commutative (that is, $ab = ba$ for all $a, b \in R$).

Definition 2.5. A field is a commutative ring, where every non-zero element is invertible, AND $0 \neq 1$. (This last thing is important. The zero ring, $R = \{0\}$ is a ring (where $0 = 1$), but it is not a field. The smallest field is $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ which has two elements. You can go look up some wikipedia articles on “field of one element”, but... we don’t care about that).

Definition 2.6. A ring that is NOT commutative, but every non-zero element is invertible is called a division ring. We won’t talk more about these (though they are important).

Definition 2.7. An element $r \in R$ is a zero divisor, if there exists $x \in R \setminus \{0\}$ such that $rx = 0$. A ring $R$ is called an integral domain if it has no non-zero zero divisors (no zero divisors other than zero).

Exercise 2.8. $\mathbb{Z}$ is an integral domain, while $\mathbb{Z}/6\mathbb{Z}$ is not. If you don’t know what $\mathbb{Z}/6\mathbb{Z}$ means, read the next section first.

Prove that fields are integral domains.

2.1. Morphisms and ideals.

Definition 2.9. A ring homomorphism between rings is a map $f: R \rightarrow S$ satisfying

(1) $f(0) = 0$
(2) $f(a + b) = f(a) + f(b)$
(3) $f(ab) = f(a)f(b)$

Exercise 2.10. Prove that for all $n \in \mathbb{Z}$, $f(n) = n$. Prove that for all $r \in R$, $f(r^{-1}) = f(r)^{-1}$ (make sure you understand what this means). Prove that for all $\frac{a}{b} \in \mathbb{Q}$, $f(\frac{a}{b}) = \frac{f(a)}{f(b)}$.

Definition 2.11. An ideal $I$ is a subset of $R$ such that

(1) $0 \in I$
Exercise 2.12.

1. Let $R$ be a ring, show that $R$ is an ideal.
2. Let $R = \mathbb{Z}$, prove that for all $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$ is an ideal. This is the canonical example of an ideal, which is all the “multiples” of some element. For an element $r \in R$, we will often denote $rR$ by $(r)$ as the ideal generated by $r$. Prove that this is an ideal.
3. Let $I, J \subseteq R$ be ideals. Show that
   \[
   I + J = \{x + y : x \in I, y \in J\}
   \]
   \[
   I \cap J = \{x : x \in I, x \in J\}
   \]
   \[
   IJ = \left\{ \sum_{i=1}^{n} x_iy_i : n \geq 0, x_i \in I, y_i \in J \right\}
   \]
   are all ideals. Now, let $R = \mathbb{Z}$ and let $I = (n)$ and $J = (m)$. What are $I + J$, $I \cap J$ and $IJ$.

Now that these are defined, we will introduce more notations. For $r_1, ..., r_n \in R$, we will also denote $(r_1, ..., r_n)$ to be the ideal generated by $r_1, ..., r_n$. This is
\[
(r_1, ..., r_n) = (r_1) + ... + (r_n).
\]
(4) To understand why the definition of $IJ$ is a bit weird, prove that $\{x_iy_i : x_i \in I, y_j \in J\}$ is NOT necessarily an ideal.

(5) For a general ring $R$, we know that $(0)$ is an ideal (this is called the zero ideal). Show that when $R = \mathbb{Z}$, $(0) = \{0\}$.

What is the set $(0)$ when $R = \mathbb{Z}/6\mathbb{Z}$?

Definition 2.13. For an ideal $I \subseteq R$, define $R/I = \{a + I : a \in R\}$ (the set of left cosets when viewing $I$ as a group under addition).

Exercise 2.14. Show that $R/I$ is a ring.

Fact 2.15. There is a one-to-one correspondence of ideals in $R/I$ with ideals in $R$ that contains $I$. (This follows from the third isomorphism for groups, with a little more work).

Definition 2.16. An ideal $I \subseteq R$ is said to be maximal, if $I \neq R$, AND whenever $J$ is another ideal with $I \subseteq J \subseteq R$, then $I = J$. (People sometimes forget the $I \neq R$ conditions, please don’t!)

An ideal $I \subseteq R$ is said to be prime, if whenever $xy \in I$ then $x \in I$ or $y \in I$.

Remark 2.17. The study of prime ideals is SUPER SUPER SUPER important in number theory and algebraic geometry. In essence, we can think of prime ideals as the generalization of prime numbers in $\mathbb{Z}$. We know that elements of $\mathbb{Z}$ has unique factorization, but this is not true for general rings. In number theory, we will encounter a special type of ring called Dedekind domains, which have unique factorization of ideals, where prime ideals are the analog of prime numbers.

Exercise 2.18.

1. Prove that maximal ideals are prime ideals. (This may be easier if you do the next exercise first)
2. Prove that $I$ is a prime ideal iff $R/I$ is an integral domain. Prove that $I$ is a maximal ideal iff $R/I$ is a field. (For the second one, use the 1-1 correspondence of ideals in $R/I$ and those of $R$ containing $I$).
3. For $R = \mathbb{Z}$, and $n \in \mathbb{Z}$, show that $n\mathbb{Z}$ is a prime ideal iff $n$ is prime, or $n = 0$. Next, show that if $n = 0$, $n\mathbb{Z}$ is not maximal, but if $n$ is a prime number, then $n\mathbb{Z}$ is maximal. (Hint: zero divisors)
(4) Suppose \( f : R \to S \) be a ring homomorphism. Show that \( \ker f \) is an ideal. Show that \( f^{-1} \) of a prime ideal is a prime ideal (for \( I \) a prime ideal, \[ f^{-1}(I) = \{ r \in R : f(r) \in I \}. \]

**Theorem 2.19. First isomorphism theorem.** Let \( f : R \to S \) be a ring homomorphism. Then \( R/\ker(f) \cong \text{im}(f) \). In particular, if \( f \) is surjective, then \( S \cong R/\ker(f) \).

**Remark 2.20.** This is a VERY VERY VERYVERYYYYYYY important theorem. It is hard to appreciate this at first glance, but I will try to convince you of this. In general, the set \( R/I \) is rather mysterious. We know that it’s the set of cosets \( \{ a + I \} \), but if we start listing out all the elements \( 0 + I, 1 + I, \ldots \) ugh… what comes next? It is not always clear! In fact, if I just pick \( r_1, r_2 \in R \), how can I check that \( r_1 + I \) and \( r_2 + I \) are not the same? If I can’t even do this… how can I define a map \( R/I \) to anything…?

This theorem tells us something beautiful. I only need to define a map \( f : R \to S \) with kernel \( I \), then I have defined a map \( R/I \to S \), and I know what the image is!

**Example 2.21.** Let \( \mathbb{Q}(i) = \{ a + bi : a, b \in \mathbb{Q} \} \). Prove that this is a field (in particular, it is a ring) on your own. The goal is to show that \( \mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}(i) \).

This exercise is super super important when we talk about Galois theory. I want to use the first isomorphism theorem, which means that I need to find a ring homomorphism \( f : \mathbb{Q}[x] \to \mathbb{Q}(i) \). From a previous exercise, for all \( a \in \mathbb{Q} \), \( f(a) = a \), so I am already very restricted. Notice that given a polynomial \( a_nx^n + \ldots + a_1x + a_0 \), by the properties of a homomorphism, \[ f(\sum a_i x^i) = \sum f(a_i) x^i \]

is the evaluation map. This is clearly surjective, because given \( a + bi \in \mathbb{Q}(i) \), we see that \( a + bx \to a + bi \). Now, we just need to show that \( \ker(f) = (x^2 + 1) \). Suppose \( p(x) \in \ker(f) \). Now, I need to show that \( p(x) \) is a multiple of \( x^2 + 1 \). By division algorithm, \[ p(x) = a(x)(x^2 + 1) + r(x) \]

for some polynomials \( a(x), r(x) \in \mathbb{Q}[x] \) with \( \deg(r) < \deg(x^2 + 1) = 2 \). Now, evaluate the equation at \( i \), to see that \( r(i) = 0 \). Since \( \deg r = 0,1 \) and \( r(i) = 0 \)… we see that \( r(x) = 0 \) (is the zero polynomial). Hence, \( p(x) \in (x^2 + 1) \) is a multiple. Clearly, \( (x^2 + 1) \subseteq \ker(f) \), and so we are done by the first isomorphism theorem.

**Remark 2.22.** For another example of first isomorphism theorem, see Chinese remainder theorem in the preceding section.

**Exercise 2.23.** Prove that \( \mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} : a, b \in \mathbb{Q} \} \cong \mathbb{Q}[x] / (x^2 - 2) \).

2.2 Properties of a ring.

**Definition 2.24.** An element \( r \in R \) is called a unit, if \( r \) is invertible. The set of units is often denoted by \( R^\times \). Notice that if \( R = F \) is a field, then \( F^\times = F\setminus\{0\} \).

An element \( r \in R \) is irreducible, if it cannot be written as the product of two non-units.

**Definition 2.25.** A unique factorization domain (short form UFD) is an integral domain, where every non-zero element \( r \in R \) can be written to be of the form \( r = up_1 \ldots p_n \).
where \( u \in R^\times \) and \( p_i \)'s are irreducible. Additionally, if \( r = wq_1...q_m \) then \( m = n \) and there exists a permutation \( \sigma \in S_n \) so that \( \frac{p_i}{q_{\sigma(i)}} \) is a unit for all \( i \).

**Definition 2.26.** An integral domain is said to be a principal ideal domain (short form PID) if every ideal \( I \subseteq R \) is of the form \( (r) \) for some \( r \in R \).

**Example 2.27.** \( \mathbb{Z} \) is a unique factorization domain. So is \( \mathbb{Z}[x], \mathbb{R}[x] \)

**Exercise 2.28.** \( \mathbb{Z} \) is a principal ideal domain. Hint: division algorithm. In fact, \( \mathbb{Z} \) is actually an Euclidean domain, and Euclidean domains are principal ideal domains (this last part is very easy to show, once you have done the exercise. It’s just division algorithm). You can look this up on wikipedia, we won’t cover this further.

Prove that \( \mathbb{R}[x] \) is a principal ideal domain (hint: division algorithm)

**Theorem 2.29.** Principal ideal domains are unique factorization domains.

2.3. Important Theorems.

**Theorem 2.30.** Chinese Remainder Theorem, integral version. Let \( n_1,...,n_k \) be positive integers, that are pairwise coprime. Let \( 0 \leq a_i < n_i \) for all \( i \), then there is exactly one \( 0 \leq x < N = n_1...n_k \) such that \( x \equiv a_i \mod n_i \) for all \( i \).

**Exercise 2.31.** Find \( x \in \mathbb{Z}/12\mathbb{Z} \) such that \( x \equiv 1 \mod 4, x \equiv 0 \mod 3 \).

**Definition 2.32.** Let \( R_1 \) and \( R_2 \) be rings. Let \( R_1 \times R_2 = \{(a_1, a_2) : a_i \in R_i \} \) is called the product ring. Define

\[
(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)
\]

\[
(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2).
\]

**Exercise 2.33.** Show that \( R_1 \times R_2 \) is a ring.

**Theorem 2.34.** Chinese Remainder Theorem, general ring version. Two ideals \( I, J \subseteq R \) are said to be coprime if \( I + J = R \) (that is, there exists \( i \in I, j \in J \) such that \( i + j = 1 \)). Now, let \( I_1,...,I_k \) be ideals of \( R \) that are pairwise coprime. Let \( I = I_1 \cap ... \cap I_k \), then

\[
R/I \cong R/I_1 \times ... \times R/I_k.
\]

**Proof.** DO READ THIS PROOF!!!!!!!!!

I will do this in the case of \( k = 2 \) (so we just have \( I_1 \) and \( I_2 \)). By the first isomorphism theorem, I just need to define a surjective map \( f : R \to R/I_1 \times R/I_2 \) with kernel \( I_1 \cap I_2 \). Define \( r \mapsto (r + I_1, r + I_2) \). Exercise: check that this is a ring homomorphism, and that it is surjective. Now, to find its kernel. \( r \in \ker(f) \) iff

\[
(r + I_1, r + I_2) = (0 + I_1, 0 + I_2) = (I_1, I_2)
\]

iff \( r \in I_1 \) and \( r \in I_2 \) iff \( r \in I_1 \cap I_2 \). \( \square \)

**Fact 2.35.** The integral version of CRT follows immediately from this, which we write

\[
\mathbb{Z}/n_1...n_k\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z}.
\]

3. Field and Galois Theory

3.1. Vector spaces.

**Definition 3.1.** A vector space \( V \) over a field \( K \) is a group under addition satisfying:

1. \( k(v_1 + v_2) = kv_1 + kv_2 \) for all \( k \in K, v_1, v_2 \in V \)

If we let \( K \) be a ring instead, this is called a module.
Definition 3.2. Given $v_1, \ldots, v_n \in V$, define the span of these vectors to be the space

$$\text{span} \{v_1, \ldots, v_k\} = \{k_1 v_1 + \ldots + k_n v_n : k_1, \ldots, k_n \in K\}$$

is called the set of linear combinations of the $v_i$'s.

Definition 3.3. A basis of $V$ over $K$ is a set $\{v_1, \ldots, v_n\}$ such that $\text{span} \{v_1, \ldots, v_n\} = V$ and for all $v \in V$, there are UNIQUE $k_1, \ldots, k_n$ such that $v = k_1 v_1 + \ldots + k_n v_n$.

Theorem 3.4. The cardinality of two bases are the same.

Definition 3.5. The dimension of $V$ over $K$ is defined to be the size of any basis. (Note, not all vector spaces are finite dimensional).

3.2. Field Extensions.

Definition 3.6. Let $K \subseteq L$ be a subfield, then $L$ is said to be a field extension of $K$ (often written as $L/K$. This does not mean quotient... as ambiguous as it may be). We can view $L$ as a vector space over $K$. Then the index $[L : K]$ is defined to be the dimension of this vector space (not necessarily finite).

Definition 3.7. Suppose $L/K$ is a field extension. An element $a \in L$ is said to be algebraic over $K$, if there exists a non-zero polynomial $p(x) \in K[x]$ such that $p(a) = 0$ (so $a$ is a root of a polynomial over $K$).

An element that is algebraic over $\mathbb{Q}$ is called an algebraic number.

Remark 3.8. Suppose $a$ is algebraic over $K$, so we have $p(x) \in K[x]$ such that $p(a) = 0$. Suppose $q(x)$ is another such polynomial, then we can do division algorithm

$$p(x) = a(x)q(x) + r(x)$$

to find a polynomial $r(x)$ of degree strictly less than $q$. Since $p(a) = 0 = q(a)$, we see that $r(a) = 0$. This means that by continuously preforming with process, we can find a UNIQUE monic (first coefficient is zero) polynomial of least degree $r(x)$ such that $r(a) = 0$. This is called the minimal polynomial.

Exercise 3.9. Show that minimal polynomials are irreducible

Definition 3.10. Suppose $L/K$ is a field extension. Suppose $a \in L$, define

$$K[a] = \{k_n a^n + \ldots + k_1 a + k_0 : k_0, \ldots, k_n \in K, n \geq 0\}.$$

Think about it as you take the polynomial ring $K[x]$ and just evaluate all of them at $a$. This is called the field generated by $a$ over $K$. I will let you define $K[a_1, \ldots, a_k]$ for $a_1, \ldots, a_k \in L$ (use multivariable polynomials and evaluate).

Now, define $K(a)$ to be the field of fractions of $K[a]$, that is, $K(a) = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in K[a], \beta \neq 0 \right\}$. In fact, $K(a)$ is already equal to $K[a]$ if $a$ is algebraic, which we will see soon. $K(a)$ is called the field generated by $a$.

Example 3.11. $\mathbb{Q}(i)$ is the field generated by $i$. In a previous exercise, I defined this to be $\{a + bi : a, b \in \mathbb{Q}\}$, which I will justify now. First, we see very clearly, that $\mathbb{Q}[i]$ is the image of the map $\mathbb{Q}[x] \to \mathbb{C}$ by $p(x) \mapsto p(i)$. We have already seen that the kernel of this map is $(x^2 + 1)$. By the first isomorphism theorem,

$$\mathbb{Q}[i] \cong \mathbb{Q}[x]/(x^2 + 1).$$

Suppose $p(x) \in \mathbb{Q}[x]$, then by division algorithm, we can find $r(x)$ of degree 0 or 1 such that $p(x) + (x^2 + 1) = r(x)$. This shows that $\mathbb{Q}[x]/(x^2 + 1)$ is in bijection with the set of linear polynomials in $\mathbb{Q}[x]$. Therefore, $\mathbb{Q}[i] \cong \{a + bi : a, b \in \mathbb{Q}\}$.

Now, I just need to show $\mathbb{Q}[i] = \mathbb{Q}(i)$.

Fact 3.12. This works in general. That is, suppose $a$ is algebraic over $K$, with minimal polynomial $p(x)$, then

$$K(a) = K[a] \cong K[x]/(p(x)).$$
and the last thing can be represented by all polynomials of degree strictly less than \( p \). Therefore, \( K(\alpha) = \{ q(\alpha) : \deg(q) < \deg(p) \} \).

**Theorem 3.13.** If \( \alpha \) is algebraic over \( K \), then \( K[\alpha] = K(\alpha) \).

**Proof.** Suppose \( x^n + a_{n-1}x^{n-1} + \ldots + a_0 \) is the minimal polynomial of \( \alpha \). Then we see that
\[
-a_0 = \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha = \alpha \left( \alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1 \right).
\]
Therefore,
\[
\alpha^{-1} = \frac{\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1}{-a_0}.
\]
Here, \( a_0 \neq 0 \), else our polynomial is not a minimal polynomial (not irreducible). This shows that \( \alpha^{-1} \in K[\alpha] \), which implies that \( K(\alpha) \subseteq K[\alpha] \).

**Definition 3.14.** An extension \( L/K \) is called separable, if the minimal polynomial of all \( \alpha \in L \) has distinct roots. I am not going to say more, look it up on wikipedia if you need to. Everything we will encounter in the REU term is separable.

**Theorem 3.15.** *Primitive element theorem.* Suppose \( L/K \) is a finite separable extension. Then there exists \( \alpha \in L \) such that \( L = K(\alpha) \).

**Definition 3.16.** An extension \( L/K \) is called normal, if whenever \( p(x) \in K[x] \) is an irreducible polynomial, either \( p(x) \) is irreducible in \( L[x] \) or splits into linear factors in \( L[x] \).

An extension that is separable and normal is called Galois.

**Definition 3.17.** Suppose \( p(x) \in K[x] \) is a polynomial. The splitting field of \( p(x) \) over \( K \), is the smallest field extension \( L \) of \( K \) such that \( p(x) \) splits into linear factors in \( L[x] \). In general, \( L \) is a splitting field over \( K \), if it is the splitting field of some set of polynomials over \( K[x] \).

**Fact 3.18.** Splitting fields are normal extensions! This is our canonical example of a Galois extension. In fact, if \( L/K \) is finite and separable, and \( L \) is Galois over \( K \) then \( L \) is a splitting field over \( K \). Basically, since we don’t talk about non-separable extensions, just think Galois extensions are splitting fields.

**Corollary 3.19.** All degree two extensions over \( \mathbb{Q} \) (called quadratic fields) are Galois.

**Proof.** Suppose \( K = \mathbb{Q}(\alpha) \). Since the extension is of degree 2, we see that the degree of the minimal polynomial \( p(x) \) of \( \alpha \) is 2. Since \( \alpha \) is a root, \(-\alpha \) must be the other root. Therefore, \( p(x) \) splits, and we see that \( K \) is the splitting field of \( p(x) \), and so \( K/\mathbb{Q} \) is Galois.

**Example 3.20.** \( K = \mathbb{Q}(\sqrt{2}) \) is not Galois over \( \mathbb{Q} \). It is was, then it would be normal. In particular, \( x^4 - 2 \) should remain irreducible or split into linear factors. But
\[
x^4 - 2 = \left( x - \sqrt{2} \right) \left( x + \sqrt{2} \right) \left( x - \sqrt{2i} \right) \left( x + \sqrt{2i} \right).
\]
The first two terms are in \( K[x] \). The last two can’t be, because \( \sqrt{2i} \in \mathbb{C} \setminus \mathbb{R} \), while \( K \subseteq \mathbb{R} \). Therefore, \( x^4 - 2 \) factors over \( K[x] \), but not into linear factors.

Corollary: \( L = \mathbb{Q}(\sqrt{2}, i) \) is Galois over \( \mathbb{Q} \), because it is the splitting field of \( x^4 - 2 \) (it’s easy to see why this is the smallest extension).

**Theorem 3.21.** Suppose \( L/K \) is a finite separable extension. Then there exists a minimal field extension \( M/L \) such that \( M/K \) is Galois (that is, given any other Galois extension \( N/K \) that is Galois and \( N \) containing \( L \), we must have \( M \subseteq N \). This is the minimality). \( M \) is called the Galois closure of \( L/K \).

**Example 3.22.** In the previous example, \( L \) the the Galois closure of \( K/\mathbb{Q} \).

**Exercise 3.23.** Prove that \( K = \mathbb{Q}(\zeta_3) \) is Galois over \( \mathbb{Q} \), where \( \zeta_3 \) is the primitive third root of unity.
Exercise 3.24. Prove that \( K = \mathbb{Q}(\sqrt{2}i) \) is not Galois. What is its Galois closure?

Exercise 3.25. What is the splitting field of \( x^2 + 1 \) over \( \mathbb{R} \)?

3.3. Galois Theory.

**Definition 3.26.** For a field extension \( L/K \), define

\[ \text{Aut}(L/K) = \{ \text{field homomorphisms } f : L \rightarrow L, \text{ such that } f(x) = x \forall x \in K \}. \]

So it is the set of automorphisms (field homomorphisms from \( L \) to itself) such that the base field is fixed.

**Remark 3.27.** I didn’t define what field homomorphisms are, it’s just the same as ring homomorphisms.

Automorphisms really means isomorphisms between itself (i.e. \( f : G \rightarrow G \) an isomorphism of a group to itself is also called an automorphism). But here, I defined it as just field homomorphisms to itself (called endomorphisms). Why? Are all field endomorphisms of this form isomorphisms? Yes!

Injectivity: the kernel is an ideal. Since \( L \) is a field, the only ideals are \((0)\) and \(L\), but it can’t be \(L\), because \(f(1) = 1\).

Surjectivity: View \( L \) as a vector space over \( K \). It is clear that \( f \) is a \( K \)-linear map (because it fixes \( K \) and is a homomorphism. CHECK THIS!!!), and so \( f \) is a vector space homomorphism between two vector spaces of the same dimension. Injectivity implies surjectivity in this case.

**Theorem 3.28.** If \( L/K \) is a finite Galois extension, then \(|\text{Aut}(L/K)| = [L : K]\). In this case, we write \( \text{Gal}(L/K) = \text{Aut}(L/K) \) and this is called the Galois group of \( L/K \).

**Remark 3.29.** Notice that I said Galois “group”. Yes, it is a group, where the operation is composition of functions. The identity map is the identity element. Since everything is an automorphism (so an isomorphism) everything is invertible.

**Example 3.30.** Very Important example!!! Let \( K = \mathbb{Q}(i) \). We want to find \( \text{Gal}(K/\mathbb{Q}) \), which means we need all field homomorphisms \( f : K \rightarrow K \). By definition, we already know how to map the \( \mathbb{Q} \) part. Now, to decide what we can map \( i \) to. Key observation: we can extend \( f : K \rightarrow K \) to a map \( f : K[x] \rightarrow K[x] \) by declaring \( x \mapsto x \). Under this map, \( x^2 + 1 \mapsto x^2 + 1 \) because \( \mathbb{Q} \) is fixed. However, in \( K[x] \),

\[ x^2 + 1 = (x + i)(x - i). \]

This means that \( f \) as a map from \( K \rightarrow K \), must map \( i \) to \( \pm i \). You can check that both define field homomorphisms of the form we want. Therefore, \( \text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{1, c\} \) where \( c \) is complex conjugation.

**Exercise 3.31.** Let \( K = \mathbb{Q}(\sqrt{2}) \). What is \( \text{Gal}(K/\mathbb{Q}) \)?

**Fact 3.32.** Suppose \( L/K \) is finite and Galois, and let \( \alpha \in L \). Suppose \( p(x) \in K[x] \) is the minimal polynomial of \( \alpha \). Since Galois extensions are normal, and \( p(x) \) has a root over \( L \) (which is \( \alpha \)), it must split into linear factors in \( L[x] \). That means that we can write

\[ p(x) = (x - \alpha_0) \ldots (x - \alpha_n) \in L[x] \]

where \( \alpha_0 = \alpha \). Now, similar to the example above, we can extend \( f : L \rightarrow L \) to a map \( f : L[x] \rightarrow L[x] \) by \( x \mapsto x \). Then \( p(x) \mapsto p(x) \) is fixed, because all of its coefficients are in \( K \). This means that \( \alpha \) must be mapped to some \( \alpha_i \). What this shows is that all elements of the Galois group simply PERMUTES the roots of \( p(x) \).

Now, suppose \( L = K(\alpha) \). Then we know that once we declare what we send \( \alpha \), we are done. In this case, we see that \( \text{Gal}(L/K) \subseteq S_{n+1} \) (is a subgroup of the symmetric group). Here, we have \( n+1 \), just because \( p(x) \) has degree \( n+1 \) by my convention.

**Example 3.33.** Important example!!! Let \( K = \mathbb{Q}(\sqrt{2}) \). We know this is not Galois by a previous example, but we can still find \( \text{Aut}(K/\mathbb{Q}) \). Similar to the observation above, we just need to find out what we can send \( \sqrt{2} \). From before, we saw that

\[ x^4 - 2 = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{2}i)(x + \sqrt{2}i). \]
However, since $\pm \sqrt{2} i$ is not in $K$, we can only send $\sqrt{2}$ to $\pm \sqrt{2}$ (the other two roots are not in $K$). This means that $|\text{Aut} (K/Q)| = 2$. However, $[K : Q] = 4$ (with basis $1, \sqrt{2}, \sqrt{3}/4$). Once again, this affirms the fact that $K/Q$ is not Galois.

Last time, we saw that $L = \mathbb{Q}(\sqrt{2}, i)$ is Galois. Let find its Galois group. Since $\sqrt{2}$ and $i$ are “independent”, we can just find out what we can send each to and that will give us all the field homomorphisms. (There is a technical notion that justifies what I am saying, but... I’m too lazy to say what algebraically independent means). Well, $x^2 + 1 = (x + i)(x - i)$ so we can still only send $i$ to $\pm i$. However, for $\sqrt{2}$, this time we can map $\sqrt{2}$ to $\pm \sqrt{2}$ or $\pm \sqrt{2} i$. This means that our Galois group should have 8 elements. Indeed, $[L : K] = 8$ with basis $1, i, \sqrt{2}, \sqrt{2} i, \sqrt{3}/4, 2^{3/4}, 2^{1/4}$.

For future examples, let’s name these 8 automorphisms, and see how they act on the roots of $x^4 - 2$. You should make this chart yourself first, and then check with mine. This is a very simple exercise. Just write down what you are sending $i$ and $\sqrt{2}$, then from the homomorphism property you know what all the roots get mapped to.

<table>
<thead>
<tr>
<th></th>
<th>$i$</th>
<th>$\sqrt{2}$</th>
<th>$-\sqrt{2}$</th>
<th>$\pm \sqrt{2}i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f_1$</td>
<td>$i$</td>
<td>$\sqrt{2}$</td>
<td>$-\sqrt{2}$</td>
<td>$\sqrt{2}i$</td>
</tr>
<tr>
<td>$f_2$</td>
<td>$i$</td>
<td>$-\sqrt{2}$</td>
<td>$\sqrt{2}$</td>
<td>$-\sqrt{2}i$</td>
</tr>
<tr>
<td>$f_3$</td>
<td>$i$</td>
<td>$\sqrt{2}i$</td>
<td>$-\sqrt{2}i$</td>
<td>$\sqrt{2}$</td>
</tr>
<tr>
<td>$f_4$</td>
<td>$i$</td>
<td>$-\sqrt{2}i$</td>
<td>$\sqrt{2}i$</td>
<td>$-\sqrt{2}$</td>
</tr>
<tr>
<td>$f_5$</td>
<td>$-i$</td>
<td>$\sqrt{2}$</td>
<td>$-\sqrt{2}$</td>
<td>$\sqrt{2}i$</td>
</tr>
<tr>
<td>$f_6$</td>
<td>$-i$</td>
<td>$-\sqrt{2}$</td>
<td>$\sqrt{2}$</td>
<td>$-\sqrt{2}i$</td>
</tr>
<tr>
<td>$f_7$</td>
<td>$-i$</td>
<td>$\sqrt{2}i$</td>
<td>$-\sqrt{2}i$</td>
<td>$\sqrt{2}$</td>
</tr>
<tr>
<td>$f_8$</td>
<td>$-i$</td>
<td>$-\sqrt{2}i$</td>
<td>$\sqrt{2}i$</td>
<td>$-\sqrt{2}$</td>
</tr>
</tbody>
</table>

Notice that $L/K$ is also Galois (it’s the splitting field of $x^2 + 1$ over $K$). This means that $\text{Gal} (L/K) = \{\pm 1\}$ is just the identity map on $K$ and complex conjugation. From the above chart, that is $\{f_1, f_5\}$, so we see that $\text{Gal} (L/K)$ is a subgroup of $\text{Gal} (L/Q)$. You should check that it is NOT a normal subgroup, which is actually why $\text{Gal} (K/Q)$ is not Galois. As we will see in the next theorem.

**Definition 3.34.** Let $S \subseteq \text{Aut} (E) = \{f : E \rightarrow E \text{ field automorphisms}\}$. Define

$$E^S = \{x \in E : f(x) = x \text{ for all } f \in S\}$$

is called the fixed field of $S$ inside $E$. Well, you should prove that it’s a field.

**Example 3.35.** $L^{\{f_1, f_5\}} = K$ (you should check this! it’s not hard). Is this a coincidence, that somehow subgroups of $\text{Gal} (L/K)$ gives us a field $K$ that is between $L/Q$? A better question, would I ask this question if it was (were? I’m bad at English).

**Theorem 3.36.** Fundamental theorem of Galois theory. Suppose $L/K$ is a finite Galois extension. There is a 1–1 correspondence of intermediate fields (ie. fields $F$ such that $K \subseteq F \subseteq L$) and subgroups of $G = \text{Gal} (L/K)$. More specifically,

- if $H \subseteq G$ is a group, then $L^H$ is an intermediate field of $L/K$
- if $K \subseteq F \subseteq L$ is an intermediate field, then $L/F$ is Galois, and $\text{Aut} (L/F) = \text{Gal} (L/F)$ is a subgroup of $G$

This defines a bijection.

Additionally, if $K \subseteq F \subseteq L$ is such that $\text{Gal} (L/F)$ is a normal subgroup of $G = \text{Gal} (L/K)$, then $F$ is a normal extension of $K$, in fact Galois (subextensions of separable is separable). We also know that

$$\text{Gal} (F/K) = \frac{\text{Gal} (L/K)}{\text{Gal} (L/F)}.$$
Now, there is a lot of information to unwrap here, so I will illustrate this with our long example. First, let me find all the subgroups of $G = \text{Gal}(L/Q)$.

These are exactly:

Before I continue, let me just tell you how you may do this for yourself. Remember that the size of subgroups must divide the size of the whole group. This means that the only possible subgroups are of order 2 and 4. Order two must be generated by an element of order two, which are just $f_2, f_5, f_6 f_7$ and $f_8$. To find the order four subgroups, just add another element to that of the order 2 ones, and see what it generates (remember that if you get 5 elements, it must be the whole group). We will find everything this way, because and order four group must contain an element of order 2. You should try some of these yourself to practice group theory facts!

Anyways, now, let’s find the corresponding intermediate fields.

Notice how the diagram is flipped upside down! You should try this for yourself, seriously!

**Exercise 3.37.** What is the Galois closure of $\mathbb{Q}(\sqrt{1-\sqrt{2}})$? Find the Galois group, all the subgroups and all the intermediate fields like what I did. (I’m decently sure that the Galois group should also be $D_4$, so the diagram will be the same. You should try and see this yourself).