A summary of each topic covered in Math 332 (Abstract Algebra II) at Drexel University in 2024, taught by Joel Pereira.

1 Ring Theory

Definition 1.1 (Ring). *A ring is a set R equipped with two binary operations $+, \cdot$ s.t R is an abelian group under addition, with associative multiplication that distributes over addition $a(b+c) = ab + ac$, and $(b+c)a = ba + bc$. We have two sided distributivity by assumption in this course.*

A ring has **unity** if it has a multiplicative identity. It is called commutative if the multiplication is commutative. If $a \in R$ has an inverse $b \in R$ s.t $ab = 1$ then a is called a unit. A field is a commutative ring with unity s.t that all elements except the addititive identity are units.

Definition 1.2 (Zero-divisors). *If there are $a, b \in R$ s.t $a, b \neq 0$, and $ab = 0$ then a, b are called 0 divisors.*

Definition 1.3. *An integral domain is commutative ring with unity, and no zero-divisors.*

Theorem 1.4 (Cancellation Property). *If a, b, c are elements of an integral domain, and $a \neq 0$ then $ab = ac \implies a = c$.*

If we are working in an integral domain the things to keep in mind are the cancellation lemma, and that $ab = 0 \implies a = 0 \vee b = 0$ since an integral domain has no zero divisors.

Theorem 1.5 (either zero-divisor or unity). *An element of a ring is either a zero divisor or a unit (or neither)*

Proof. Let $r \in R$ be a zero divisor. Then $rs = 0$ for some $s \neq 0$. Now if r is a unit then $r^{-1}r = 1 \implies r^{-1}rs = s \implies s = 0$ □

Definition 1.6 (Subring). *$S \subseteq R$ is a subring of R is S is also a ring.*

Proposition 1.7 (Subring test). *If $S \subseteq R$ is closed under subtraction (addition), and multiplication then it is a subring of R.*

Any finite integral domain is a field.

Definition 1.8 (Characteristic). *The characteristic of a ring R is the smallest $n \in \mathbb{N}$ s.t $nx = 0$ for all $x \in R$. If n does not exist the R has characteristic 0.*

The characteristic of a ring is the same as the characterisic of its 1 (if it has a 1). IE what is the least $n \in \mathbb{N}$ s.t $n \cdot 1 = 0$. If there is no such n then R has characteristic 0, else its n.

Theorem 1.9. *The characteristic of an integral domain is 0 or prime.*

Definition 1.10 (Nilpotents). *For a ring R, $x \in R$ is called nilpotent if there is $n \in \mathbb{N}$ s.t $x^n = 0$.*

Nilpotents are all zero-divisors as if $x \neq 0$, then $x^n = x \cdot \underbrace{x^{n-1}}_{\neq 0} = 0 \implies x$ is a zero-divisor. Any nilpotent plus a unit is a unit in any commutative ring. IE if $r \in R$ is a unit then $(x + r)$ is a unit with inverse $(x + r)^{-1} = (r^{-1} - xr^{-2} + \cdots + (-1)^{n-1}r^{-n}x^{n-1})$

1.1 Chapter 12 Exercises, Gallian

Next two problems are just applications of the subring test 1.7.

Example 1.11 (Gallian 12.18). *Let R be a ring and $r \in R$. Let $S := \{x \in R | rx = 0\}$. Show S is a subring. Let $a, b \in S$, then $r(a + b) = ra + rb = 0 + 0 = 0$ so S is closed under addition. Similarly $r(ab) = (ra)b = 0b = 0$, so S is closed under multiplication.*

Example 1.12 (Gallian 12.19). *The center of a ring R is the set $C = \{x \in R | ax = xa\ \forall a \in R\}$. Ie it is the set of elements that commute with everything in the ring. Always non-empty since the identity commutes with everything. WTS C is subring. Let $x, y \in C$, and $r \in R$. Then $r(x + y) = \underbrace{rx + ry}_{\text{ring distributive property}} = \underbrace{(xr + yr)}_{\text{since } x,y \in C} = (x + y)r$. Thus $(x + y) \in C$, and C is closed under addition. Now to show closure undermultiplication were using associativity and that x, y are in the center. $r(xy) = (rx)y = (xr)y = x(ry) = x(yr) = (xy)r$, so $xy \in C$, and C is closed under multiplication.*

Example 1.13 (Gallian 12.34). *Let $n > 1$ be an integer, and R be a ring that satisfies $x^n = x$ for all $x \in R$, show that $ab = 0 \implies ba = 0$.*

$$ba = \underbrace{(ba)^n}_{x^n = x} = \underbrace{(ba)(ba)(ba)^{n-2}}_{\text{have to be careful here, } n>1 \implies n \geq 2 \text{ since } n \text{ is an integer, thus we have at least two } (ba) \text{ factors}}$$

$$= b \underbrace{(ab)}_{=0 \text{ by assumption}} a(ba)^{n-2} = b \cdot 0 \cdot a(ba)^{n-2} = 0$$

Always remember your multiplication is associative, its useful.

Example 1.14 (Gallian 12.37). *Suppose that $x^4 = x$ for all $x \in R$. Show that $2x = 0$ for all x. Notice that $(-x) = (-x)^4 = x^4 = x$ so every element is its additive inverse. Thus $2x = x + x = x - x = 0$. That every element is its additive inverse holds whenever we have $x^n = x$ for even n.*

Example 1.15 (Gallian 12.56). *Assume $a^2 = a$ for all $a \in R$. Show that $ab = ba$. We again want to use that $a = -a$ for all a.*

$$\begin{aligned}(a + b) &= (a + b)^2 = a^2 + ab + ba + b^2 \\ &= (a + b) + (ab + ba) \underbrace{\implies}_{\text{subtract } (a+b) \text{ from both sides}} ab + ba = 0\end{aligned}$$

$$\implies ab = \underbrace{-ba}_{=ba \text{ since } -a = a \text{ for all } a} = ba$$

Problems 44-48 seems like pretty straightforward applications of the subring test 1.7, but annoying to type up. As long as you can multiply 2x2 matrices, it should be fine.

1.2 Chapter 13 Exercises, Gallian

Example 1.16 (Gallan 13.18)**.** *Show that if R is an integral domain the only idempotents (a s.t $a^2 = a$), are 0, and 1. Of course 0 is idempotnent $0^2 = 0 \cdot 0 = 0$, so assume $a \neq 0$ and apply the cancellation property 1.4.*

$$a^2 = a = a \cdot e \underbrace{\Longrightarrow}_{1.4} a = e$$

Example 1.17 (Gallan 13.22)**.** *Show that if a is idempotent ($a^2 = a$) then $a^n = a$ for all $n \in \mathbb{N}$. We can use strong induction. Base case $n = 1$, then $a^1 = a$. Now assume for all $1 < k < n$ that $a^k = a$. Then $a^n = a \cdot \underbrace{a^{n-1}}_{=a \text{ by IH}} = a \cdot a = a^2 = a$.*

Example 1.18 (Gallan 13.31)**.** *Let R be a ring with unity 1, and such that the product of any non-zero elements is non-zero (purposefully obfuscuting way to say $ab = 0$ implies a or b is 0). Show that $ab = 1 \implies ba = 1$. These problems always have a trick that makes them easy, and without it, you really just have to play around.*

$$ab = 1 \implies aba = a \implies aba - a = 0 \implies \underbrace{a(ba - 1) = 0}_{a \neq 0 \implies ba - 1 = 0} \implies ba - 1 = 0$$

so that $ba = 1$ as desired.

2 Ideals and Factor Rings

Definition 2.1 (Ideal (two sided))**.** *A subring S or R is an ideal if for any $s \in S$, and all $r \in R$ we have $rs \in R$, and $sr \in R$.*

We pretty much only think about commutative rings in this course anyway, so all our ideals are two sided. Ideals are important because when we quotient out our ring by an ideal we get another ring. We all have another isomorphism theorem for rings that is analogus to the same one for groups.

Proposition 2.2 (Ideal Test)**.** *$S \subseteq R$ is an ideal of R if*

1. *S is closed under subtraction (addition). IE $s_1 - s_2 \in S$ whenever $s_1, s_2 \in S$.*
2. *ar and ra are in S whenever $a \in S$, and $r \in R$.*

This is really just verifying the definition.

Theorem 2.3 (Factor Rings)**.** *Let $S \subseteq R$. Then the set of cosets of S given by $\{r + S | r \in R\}$ is a ring under the following operations iff S is an ideal of R.*

1. *Coset addition* $(a+S)+(b+S)=(a+b)+S$

2. *Coset multiplication* $(a+S)(b+S)=ab+S$

Untangling when were talking about operating on the cosets vs the ring elements can be pretty confusing.

Definition 2.4 (Prime Ideal)**.** *An ideal S of R is prime if for $a,b \in R$, whenever $ab \in S$ then $a \in S$ or $b \in S$.*

Definition 2.5 (Maximal Ideal)**.** *A proper ideal S of R is maximal if there is no larger ideal that properly contains. That is if I is some other ideal of R, and $S \subseteq I \subseteq R$ then either $I=S$ or $I=R$.*

This are very important classifications for ideals. They imply a lot. As the next thoerems show.

Theorem 2.6 (R/A is a ID iff A is a prime ideal)**.** *Let A be an ideal of R. Then R/A is a integral domain iff A is a prime ideal.*

Theorem 2.7 (R/A is a field iff A is maximal ideal)**.** *Let A be an ideal of R. Then R/A is a field iff A is a maximal ideal.*

So when you quotient out by a maximal ideal you get a field, and when you quotient out by a prime ideal you get an integral domain. Notice field subsumes integral domain. If everything is a unit, since unit implies not zero divisor, a field has no zero divisors. Then all maximal ideals are necessairily prime, but not vice versa.

More rigoriously this follows from the previous theorems. Let A be a maximal ideal then R/A is field. But then since a field is an integral domain we obtained an integral domain by quotienting out by A. Thus thoerem 2.6 yields that A is a prime ideal. Thus maximal ideals are prime. I think we also proved this in a less round about way in class.

3 Ring Homomorphisms

Another important topic. This is where we get the isomorphism theorems.

Definition 3.1 (Ring homomorphism)**.** *A ring homomorphism $\phi : R \to S$ is mapping that preserves the ring operations. That is for all $a,b \in R$*

$$\phi(a+b)=\phi(a)+\phi(b) \quad \textit{and} \quad \phi(ab)=\phi(a)\phi(b)$$

A bijective homomorphism is an isomorphism

Theorem 3.2 (Kernals equivalent to Ideals)**.** *Let $\phi : R \to S$ be a ring homomorphism. Then $Ker\phi = \{r \in R | \phi(r) = 0 \in S\}$ is an ideal of R. Conversely if I is an ideal of R then it is the kernal of the homomorphism*

$$\phi : R \to R/I \quad \textit{defined by} \phi(r) = r+I, \textit{IE r maps to its coset}$$

Theorem 3.3 (1st isomorphism theorem for rings)**.** *Let $\phi : R \to S$ be a ring homomorphism. Then $R/Ker\phi \cong \phi(R)$. The R mod the kernal of ϕ is isomorphic to the image of ϕ.*

These are all big thoerems. Pretty much the hits of quotient rings. Although were not covering the 2nd isomorphism theorem which is a bit more, disgusting.

3.1 Chapter 14 Exercises, Gallian

Example 3.4 (Gallian 14.3). *Let R be a commutative ring with unity, and $I = \langle a_1, a_2, ..., a_n \rangle = \{r_1 a_2 + r_2 a_2 + \cdots + r_n a_n | r_i \in R\}$, the ideal generated by $a_1, a_2, ..., a_n$.*

- *Show that I is an ideal. That it is a subring is obivous. Taking a sum or product of linear combinations of a_i's yields another linear combintation. That it is closed under multiplication by any $r \in R$ follows from the distributive property, and that R is closed under multiplication. Let $d = \sum_{i=1}^{n} r_i a_i$ then if $r \in R$*

$$rd = r\left(\sum_{i=1}^{n} r_i a_i\right) \underbrace{=}_{\text{distributive property}} \sum_{i=1}^{n} \underbrace{r \cdot r_i}_{\in R} a_i \in I$$

- *Show that if J is any ideal s.t $a_i \in J$ for all i then $I \subset J$. We just need to show that $d \in I \implies d \in J$. This is simple as if $d = (\sum_{i=1}^{n} r_i a_i)$, then since J is closed under multiplication by any element of R then $r_i a_i \in J$ for each i. Then since J is closed under addition the of the $r_i a_i$ is also in J. Thus $d \in J$.*

Example 3.5 (Gallian 14.12). *This was one of the first homework exercises. Just use the ideal test 2.2, and that $a \in \cap I_i \implies a \in I_i$ for all i.*

Example 3.6 (Gallian 14.16). *Show that if A, B are ideals their product $AB = \{a_1 b_1 + \cdots + a_n b_n | a_i \in A, b_i \in B\}$ is an ideal. The closure under addition, and multiplication are annoying to writeup, but easy enough to see. If I add a bunch of sums of products of elements in both ideals I get another sum of products of elements in the the ideal.*

$$a_{i_1} b_{i_1} + \cdots a_{i_n} b_{i_n} + a_{j_1} b_{j_1} + \cdots a_{j_n} b_{j_n} \in AB$$

If I take a product of sums of products of elements in both I still get another sum of products. That AB is closed under mulitplication by any $r \in R$ follows from A, B being ideals.

$$r(a_1 b_1 + \cdots + a_n b_n) = (ra_1) b_1 + \cdots + \underbrace{(ra_n)}_{(ra_i) \in A \text{ since } A \text{ an ideal}} b_n \in AB$$

Example 3.7 (Gallian 14.19). *Let I be an ideal of R s.t the unity of R is in I. Show that $I = R$. Since $I \subset R$ by definition we need only verify that $R \subset I$. Take any $r \in R$. Then since I is closed under multiplication by any ring element $rk \in I$ for all $k \in I$ then in particular $r \cdot 1 = r \in I$, and thus $R \subset I$, and conseqeuntly $R = I$.*

Example 3.8 (Gallian 14.20). *Let A, B be ideals of a commutative ring R s.t $A + B = \{a + b | a \in A, b \in B\} = \langle 1 \rangle = R$. Show that $A \cap B = AB$. If $x \in AB$ then $x = \sum_{i=1}^{n} a_i b_i$. Each of the $a_i b_i$ is in B since $a_i \in A$. Similarly since $a_i b_i = b_i a_i$ they are also in A. Then the sum $\sum_{i=1}^{n} a_i b_i$ is also in A, and B since ideals are closed under addition. Thus $AB \subset A \cap B$. Conversely suppose $x \in A \cap B$. Then since $A + B = R$ there is $a \in A, b \in B$ s.t $1 = a + b$. Then $x = xa + xb = ax + xb \in AB$.*

Exercise 27-29 also look annoying to write up.

Example 3.9 (Gallian 14.39). *Show that the only ideals of a field F are $\{0\}$, and F itself. First its clear that $\{0\}$ is an ideal since for any $r \in F$ we have $r \cdot 0 = 0$, and of course $0 + 0 = 0 \cdot 0 = 0 \in \{0\}$. Now assume that $I \neq \{0\}$ is an ideal of F. Then there is $a \in I$ s.t $a \neq 0$. Then since F is a field there is $a^{-1} \in F$. Now since I is closed under multiplication by any ring element we have that $a^{-1}a = 1 \in I$, and thus by $I = F$ by exercise 19 above.*

You might have noticed pretty much all the rings we deal with in these problems are commutative. That because we only ever defined two sided ideals!

Example 3.10 (Gallian 14.61). *Let R by a commutative ring, and let A be any subset of R. Show that the annihilator of A, $Ann(A) = \{r \in R | ra = 0 \ \forall a \in A\}$ is an ideal. Take $x, y \in Ann(A)$, and $a\ inA$. Closure under addition: $a(x+y) = ax + ay = 0 + 0 = 0$. Closure under multiplication: $a(xy) = (ax)y = 0y = 0$. Closure under scaling by any $r \in R$: $a(\underbrace{rx}_{R\text{ commutative}}) = a(xr) = (ax)r = 0r = 0$.*

Example 3.11 (Gallian 14.62). *Let R be a commutative ring, and A an ideal of R. Show that the nil radical $N(A) = \{r \in R | r^n \in R \text{ for some } n \in \mathbb{N}\}$ is an ideal of R. Closure under multiplication, and scaling by element in R is easy. Really the only interesting one is addition. Let $a, b \in N(A)$ s.t $a^n \in A$, and $b^m \in A$. Then $(a+b)^{n+m} \in A$.*

$$\begin{aligned}(a+b)^{n+m} &= \sum_{k=0}^{n+m} \binom{n}{k} a^{n+m-k} b^k, \textit{ binomial formula} \\ &= \sum_{k=0}^{m} \binom{n}{k} a^{n+m-k} b^k + \sum_{k=m}^{n+m} \binom{n}{k} a^{n+m-k} b^k\end{aligned}$$

Then for $k \leq m$ we know that $a^{n+(m-k)} = a^n \cdot a^{m-k} \in A$, and thus $\binom{n}{k} a^{n+m-k} b^k \in A$. Similarly for $k \geq m$ we know that $b^k = b^m \cdot b^{k-m} \in A$, and thus $\binom{n}{k} a^{n+m-k} b^k \in A$. Then since A is closed under addition we know that the sum $(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n}{k} a^{n+m-k} b^k \in A$ as desired.

Example 3.12 (Gallian 14.63).

Example 3.13 (Gallian 14.64).

3.2 Chapter 15 Exercises, Gallian

Example 3.14 (Gallian 15.19). *Show that $\phi : Z_6 \to Z_{30}$ given by $\phi(x) = 6x$ is a ring homomorphism. We just need to show it preserves multiplication, and addition. First addition*

$$\phi(a+b) = 6(a+b) = 6a + 6b = \phi(a) + \phi(b) \mod 30$$

And multiplication

$$\phi(ab) = 6ab = \underbrace{36}_{36 \equiv 6 \mod 30} ab = \phi(a)\phi(b) \mod 30$$

Example 3.15 (Gallian 15.20)**.** *Is the mapping from $Z_{10} \to Z_{10}$ given by $x \to 2x$ a ring homomorphism? Now just consider that $\phi(1) = \phi(1^2) = \phi(1)^2 = 2^2 = 4$, but $\phi(1) = 2$.*

Example 3.16 (Gallian 15.51)**.** *Is there a ring homomorphism from the reals to some ring whose kernal is the integers. No because by 3.2 kernels of ring homomorphisms are ideals of the source ring, and $\mathbb{Z}$ is not an ideal of $\mathbb{R}$ since $1 \in \mathbb{Z}$, but $\sqrt{2} \cdot 1 \notin \mathbb{Z}$.*

Example 3.17 (Gallian 15.68)**.** *Explain why a commutative ring with unity, that is not an integral domain can't be contained in a field.*

He only says explain so I'm gonna be pretty vague. Every field is an integral domain, and if any subring of a field contained a zero divisor then so would the field. But then if this subring is isomorphic to our commutative ring then zero divisors in the ring imply a zero divisor in the subring. More formally let R be a commutative ring, and R' the subring of a field F that is isomorphic to R with isomorphism ρ. Then $ab = 0$ for $a, b \in R$, and

$$\rho(ab) = \rho(a)\rho(b) = \rho(0) = 0$$

Thus $\rho(a), \rho(b)$ are zero-divisors in R', and thus F has zero-divisors. A contradiction.

Example 3.18 (Gallian 15.68)**.** *This was one of the midterm questions. First midterm 3rd question.*

1. *part (a) is straight forward and mechanical.*

2. $$\phi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\right) = a - b = 0 \implies a = b$$

   So $\ker \phi = \{\begin{pmatrix} a & a \\ a & a \end{pmatrix} | a \in \mathbb{Z}\}$.

3. *By 1st isomorphism thm $R[x]/\ker\phi \cong Im\phi$. We want to show that $Im\phi = \mathbb{Z}$. Since ϕ is indeed map from R to $\mathbb{Z}$ we need only show its surjective to know that its image is indeed $\mathbb{Z}$. Then for some $z \in \mathbb{Z}$ consider the matrix $\begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix} \in R$. Then by defintion $\phi\left(\begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}\right) = z - 0 = z$, and thus ϕ is surjective, and $R[x]/\ker\phi \cong \mathbb{Z}$.*

4. *Is $\ker\phi$ a prime ideal? Yes since $R/\ker\phi \cong \mathbb{Z}$ is an integral domain , by thm 2.6 $\ker\phi$ must be a prime ideal.*

5. *Is $\ker\phi$ a maxiaml ideal? No since $\mathbb{Z}$ is not a field, by thm 2.7.*

4 Polynomial Rings

Much of the theory built up so far is instantiated in polynomial rings.

Definition 4.1 (Polynomial Rings). *For a ring R define $R[x] = \{a_n x^n + \cdots + a_0 | a_i \in R, n \in \mathbb{N}\}$. $R[x]$ or R adjoin x is the ring of all polynomials in x. $p(x), q(x) \in R[x]$ are equal iff $p_i = q_i$ for all i. That is their coefficients are equal. Addition is defined component wise.*

$$p(x) + q(x) = \sum_{i=0}^{n} p_i x^i + \sum_{i=0}^{m} = \sum_{i=0}^{\max(m,n)} (p_i + q_i) x^i$$

Where $q_i = 0$ for $i > m$, and $p_i = 0$ for $i > n$. Multiplication is defined by generalized foil.

$$p(x)q(x) = \left(\sum_{i=0}^{n} p_i x^i\right)\left(\sum_{i=0}^{m} q_i x^i\right) = \sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} p_i q_{k-i}\right) x^k$$

Division of polynomials is well defined, and admits the following theorem.

Theorem 4.2 (Polynomial Division). *Let $\mathbb{F}$ be a field, and $f(x), g(x) \in \mathbb{F}[x]$, with $g(x) \neq 0$. Then there exists unique $q(x), r(x) \in \mathbb{F}[x]$ s.t*

$$f(x) = q(x)g(x) + r(x)$$

Where either $\deg r(x) < g(x)$ or $r(x) = 0$.

This is kind of a mouthful the way its written, but really its saying the samething as with division ofor the integers. The remainder is either 0 or less than the divisor, just in this case we deal with degree instead of value of the remainder. You can use this to prove some theorems pretty easily. For example $p(a) = a \iff (x-a)|p(x)$ is easy to show.

Theorem 4.3 (How many roots). *A polynomial of degree n over a field $\mathbb{F}$ has at most n roots with multiplicity.*

There are various relations between the ground field $\mathbb{F}$, and its polynomial ring $\mathbb{F}[x]$.

- If $\mathbb{F}$ is a integral domain then $\mathbb{F}[x]$ is an integral domain.
- If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a principle ideal domain. This means all ideals are generated by a single element, in this the minimal polynomial contained in the ideal.

Definition 4.4 (Irreducible). *A polynomial is irreducible over $\mathbb{F}$ if it cannot be factored into non-trivial polynomials over $\mathbb{F}$. That is if $f(x)$ is irreducible then $f(x) = g(x)h(x)$ iff $g(x)$ or $h(x)$ is a unit.*

The formal phrasing is weird but essentially we want to avoid non-trivial things like $p(x) = q^{-1}(x)\left(q(x)p(x)\right)$.

Theorem 4.5 (Maximal ideals). *Let $p(x) \in \mathbb{F}[x]$. Then the ideal generated by $p(x)$ denoted $(p(x))$ is maximal iff $p(x)$ is irreducible.*

This is a satisfying theorem. The next follows from it, and theorem 2.7.

Theorem 4.6 (Mod Fields). *$\mathbb{F}[x]/(p(x))$ is a field iff $p(x)$ is irreducible.*

Another proof of this would use Bezout's identity $ax + by = gcd(a, b)$. So only polynomials that do not share a factor with $p(x)$ will have inverses.

Theorem 4.7 ($I = \langle g(x) \rangle$). *Let F be a field then $F[x]$ is a principle ideal domain. (Every ideal is generated by a single element)*

Theorem 4.8 ($I = \langle g(x) \rangle$). *Let F be a field, and I a non-zero ideal in $F[x]$ with $g(x) \in I$. Then $\langle g(x) \rangle = I$ iff $g(x)$ is a polynomial of minimal degree in $F[x]$.*

4.1 Chapter 16 Exercises, Gallian

Example 4.9 (Gallian 16.21). *Let F be a field, and $f(x) \in F[x]$ have a zero a of multiplicity n. Then $f(x) = (x-a)^n q(x)$. If $b \neq a$ is a zero of $q(x)$, show it has the same multiplicity as a zero of $q(x)$ that it does for $f(x)$.*

Well use the fact if F is in integral domain then $F[x]$ is an integral domain. Let m denote the multiplicity of b as a root of $q(x)$, then $q(x) = (x-b)^m r(x)$ and $r(b) \neq 0$. Thus $f(x) = (x-a)^n(x-b)^m r(x)$. Thus $(x-b)^m | f(x)$ and the multiplicity of b as a root of $f(x)$ is at least m. Now if the multiplicity is greater then b must be a zero of $\frac{f(x)}{(x-b)^m} = (x-a)^n r(x)$. In otherwords we must have that $(b-a)^n r(b) = 0$, but then since $F[x]$ is an integral domain either $(b-a)^n = 0 \implies a = b$ or $r(b) = 0$. But then $a \neq b$ so we must have $r(b) = 0$, but $r(b) \neq 0$ so the multiplicity of b as a root of $f(x)$ mustb e m.

Example 4.10 (Gallian 16.23). *Let R be a commutative ring. Let $r \in R$, and for $f(x) \in R[x]$ define $\phi(f(x)) = f(r)$. Show that ϕ is a ring homomorphism.*

1. ***Addition:*** *well just thing of polynomials like functions $f(x) + g(x) = (f+g)(x)$. Then $\phi((f+g)(x)) = (f+g)(r) = f(r) + g(r) = \phi(f(x)) + \phi(g(x))$.*
2. ***Multiplication:*** *$\phi(f(x)g(x)) = \phi((fg)(x)) = (fg)(r) = f(r)g(r)$.*

Example 4.11 (Gallian 16.37). *Let F be a field $I \subset F[x]$ be the ideal $I = \{f(x) | f(1) = f(2) = 0\}$. By thm 4.8 we need only find a polynomial of minimal degree. Note that every polynomial in I has at least two roots. Thus they are all degree at least 2. Then a minimal polynomial that has $1, 2$ as roots is the product of monomials $g(x) = (x-2)(x-1)$. Thus by thm 4.8 $I = \langle g(x) \rangle$.*

Example 4.12 (Gallian 16.62). *Let $\phi : Q[x] \to Q$ be a ring homomorphism given by $\phi(f(x)) = f(1)$. Fine the monic polynomial $g(x)$ s.t $\ker \phi = \langle g(x) \rangle$. Clearly $\ker \phi = \{f(x) \in Q[x] | f(1) = 0\} = \langle (x-1) \rangle$. Since everything in $\ker \phi$ is degree at least 1. Then $Im\phi = Q$ since $\phi(f(x))$ is really just a sum of the coefficients of $f(x)$, all of which are in Q, and Q is a ring closed under addition so $\phi(f(x)) \in Q$. That ϕ is surjective follows from $\phi(rx) = r$ for any $r \in Q$. Thus $Q[x]/\langle x-1 \rangle \cong Q$ by 1st isomorphism thm.*

Example 4.13 (Gallian 16.70). *Let F be a field, and $I = \{f(x) \in F[x] | f(a) = 0\ \forall a \in F\}$.*

- *Show I is an ideal in $F[x]$. This is straight forward. Take $f(x), g(x) \in I$. Then $(f+g)(a) = f(a) + g(a) = 0 + 0 = 0$, so I is closed under addition. Then take $r(x) \in F[x]$. Then $r(a)f(a) = r(a) \cdot 0 = 0$, and F is closed under multplication by anything in $F[x]$.*

- *When F is finite find a minimal degree $g(x)$ s.t $I = \langle g(x) \rangle$. Since each $f(x) \in I$ must be 0 at all points of F, we must $\deg f(x) \geq |F|$. Then a monic polynomial of degree $|F|$ is $g(x) = \prod_{a \in F}(x - a)$. Thus $I = \langle \prod_{a \in F}(x - a) \rangle$.*

- *Prove that I is infinite when F is finite. Not sure how to state this with any precision. You can always increase your multiplicity of roots to get a distict polynomial even if the roots stay the same.*

- *Prove that $I = \{0\}$ when F is infinite. This is just because polynomials have bounded degree, and therefor bounded number of roots. So you cannot have polynomial with zeros at infinitely many points (except the zero polynomial).*

Example 4.14 (Gallian 16.75)**.** *Suppose that F is a field, and $\phi : \mathbb{Z} \to F$ is an onto homorphism (ie $Im\phi = F$). Show that F is isomorphic to $\mathbb{Z}_p$ for some prime p. By 1st isomorphism thorem we have*

$$\frac{\mathbb{Z}}{\ker \phi} \cong Im\phi = F$$

Then $\frac{\mathbb{Z}}{\ker \phi}$ is a field, and by thm 2.7 $\ker \phi$ is a maximal ideal. Then the maximal ideals of $\mathbb{Z}$ are $p\mathbb{Z}$ for some prime p. Then

$$F \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \cong \mathbb{Z}_p$$

Where the last congruence follows from 1st isomorphism theorem using the map $\rho : \mathbb{Z} \to \mathbb{Z}_p$ given by $\rho(n) = n \mod p$.

5 Extension Fields

Definition 5.1 (Extension Field)**.** *A field $E \supseteq F$ is called an extension of F if the operations $(+, *)$ of F are those of E restricted to F.*

This is basically saying if we operate only with those elements of F we get back elements of F. In otherwords F inside of E is a field. IE F is a subring of E that is a field.

These are two existence theorems that aren't really operational, but are good to know.

1. If $f(x) \in F[x]$ is non constant, then there is a extension of F that contains a zero of $f(x)$. We can always add a root.

2. A polynomial $f(x)$ splits in E if it can be factored into linear monomials in E. A splitting field for $f(x) \in F[x]$ is unique, always exists, and is some field extension of $F[x]$.

For (2) note we must specify the field F for the splitting field to be unique. For example $(x^2 - 2)$ splits in $\mathbb{R}$, but if we specify we mean $(x^2 - 2) \in \mathbb{Q}[x]$ then the unique splitting field is $\mathbb{Q}(\sqrt{2})$, not all of $\mathbb{R}$.

Theorem 5.2 ($F(a) \cong \frac{F[x]}{\langle p(x) \rangle}$)**.** *Let $p(x) \in F[x]$ be irreducible, with* $\deg p(x) = n$*, and a a root of $p(x)$ (note $a \notin F$ since $p(x)$ irreducible). Then*

$$\frac{F[x]}{\langle p(x) \rangle} \cong F(a) = \{c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1 a + c_0 | c_i \in F\}$$

This easily implies $F(a)$ as a vector space over F has dimension n. This will also get into when were adding roots (algebraic elements) to F the extension is isomorphic to $F[x]$ mod the minimal polynomial of the root.

Example 5.3. *What can we use this for? Describe the elements of $Q(\sqrt[3]{5})$. By theorem 5.2 since $(x^3 - 5) \in Q[x]$ is irreducible in $Q[x]$, with root $\sqrt[3]{5}$, and has degree 3 we know that $Q(\sqrt[3]{5}) = \{c_2 \sqrt[3]{5}^2 + c_1 \sqrt[3]{5} + c_0 | c_i \in Q\}$.*

6 Algebraic Extensions

What happens when we add roots of polynomials to a field? Thats basically the focus of this chapter.

Definition 6.1 (Types of extensions)**.** *Let F be a field, and E some extension of F.*

1. *If $a \in E$ is the root of some polynomial in $F[x]$ then a is called **algebraic** over F.*
2. *If a is not **algebraic** over F then it is called **transcedental** over F.*
3. *If all $a \in E$ are algebraic over F then E is called an **algebraic extension** of F.*
4. *If E is not an algebraic extension it is called a **transcedental extension***
5. *The field $F(a)$ is called a **simple extension** of F.*

Theorem 6.2 (Characterization of extension)**.** *Let be E an extension of F, and $a \in E$.*

1. *If a is transcendental then $F(a) \cong F(x)$. (note $F(x) \neq F[x]$, $F(x)$ contains the inverse of x, and is thus all rational functions).*
2. *If a is algebraic over F then $F(a) \cong \frac{F[x]}{\langle p(x) \rangle}$ where $p(x)$ is the minimal polynomaial of a, ie minimal degree polynomial with a as a root.*

Basically this theorem tells us that simple extensions of F are either isomorphic to the rational functions, or to some polynomial ring with bounded degree or equivalently a vector space with basis vectiors that are powers of a.

You can probably see how 5.2 will be used to prove 6.2. Namely if a is the root of some polynomial in $F[x]$ then there is some irreducible polynomial that a is a root of (if $a \in F$ then this is just the monic $(x - a)$). Call this irreducible $p(x)$ then by thm 5.2 $F(a) \cong F[x]/\langle p(x) \rangle$.

A few useful properties.

1. If a is algebraic over F then there is a unique irreducible monic $p(x)$ that has a as a root. This is what we call the minimal polynomial of a.

2. If $p(x)$ is the minimal polynomial of a, and $f(x) \neq p(x)$ s.t $f(a) = 0$ then $p(x)|f(x)$.

Now we really start thinking of simple extensions as vector spaces. They are really pretty simple ones. In both cases they are essentially polynomial vector spaces, either with infinite dimension in the case of a being transcendental or finite dimensional if a is algebraic. We pretty much ignore the transcendental case for the rest of the course.

Definition 6.3 (Degree of an extension). *Let E be an extension of F, and denote*

$$[E : F] := (\text{ dimension of } E \text{ as an extension of } F)$$

- *If $[E : F] = n$ then we say E has degree n over F.*
- *If $[E : F]$ is finite then E is called a finite extension of F, else an infinite one*

As proved in the book, finite extensions are algebraic extensions, and vice versa. So the the finite extensions are precisely those obtained by adding roots of polynomials to F.

Theorem 6.4 (The useful identity). *Let $K \supseteq E \supseteq F$ be finite extensions of F (ie K is also an extension of E) then*

$$[K : F] = [K : E][E : F]$$

I really like this perspective of thinking of field extension as vector spaces. Then we can really think about these problems in terms of vector spaces and subspaces. For example in the above theorem since $E \subseteq K$ since and its an extension of F we know its a subset of K that is also a vector space, thus it is a subspace of K. Then of course we can take a basis of E and extend it to a basis for K, so K does indeed extend E. The proof for 6.4 is pretty much just saying that if we have a basis for K over E, and a basis for E over F, then taking all sums of products of those basis vectors gives us a basis for K over F.

Theorem 6.5 (Degree of minimal poly is degree of extension). *Let a be algebraic over F with minimal polynomial $p(x)$ with $\deg p(x) = n$. Then $[F(a) : F] = n$.*

This is stated as example 2 in chapter 20 of the book, but its really useful so good to have as a theorem. It follows simply from 5.2, as that shows that $\{1, a, ..., a^{n-1}\}$ is a basis for $F(a)$.

Theorem 6.6. $[E : F] = 1$ *iff* $E = F$.

This is another useful result that is a exercise in the book.

Example 6.7 (Gallian 20.9). *If $[F(a) : F] = 5$ find $[F(a^3) : F]$. Since $F(a^3) \subseteq F(a)$ we know that $F(a)$ extends $F(a^3)$, and by 6.4*

$$[F(a) : F] = 5 = [F(a) : F(a^3)][F(a^3) : F]$$

Then one of the factors is 1, and the other is five (since if p is a prime its only divisors are 1, and itself p). Note that $(x^3 - a^3) \in F(a^3)[x]$, and $(a^3 - a^3) = 0$ so $[F(a) : F(a^3)] \leq 3$. Thus it cannot be 5, so it must be one, and there for $[F(a^3) : F] = 5$. The same strategy works for $F(a^2), F(a^4)$ over F, when $[F(a) : F]5$. This result is generalized in the next example.

I'm really just doing the practice problems at this point.

Example 6.8 (Gallian 20.10)**.** *Let $[E : F] = p$ be prime. Show that $F(a) = F$ or $F(a) = E$ for all $a \in E$. Really using thm 6.4 this just turns into show that either $[E : F(a)]$ or $[F(a) : F]$ is 1. Clearly E is an extension for $F(a)$ for all $a \in E$ so write*

$$[E : F] = [E : F(a)][F(a) : F] = p$$

Since p is prime it can't have two non-trivial divisors so either $[E : F(a)]$ or $[F(a) : F]$ is 1, and by 6.6 either $E = F(a)$ or $F(a) = F$ as desired.

Example 6.9 (Gallian 20.11)**.** *Let $[E : F] = n$. Prove if $f(x)$ is irreducible over F, and does not have a root in E its degree does not divide n. Well show the contrapositive. Assume $a \in E$ is a root of irreducible $f(x)$. Then by thm 6.5 $[F(a) : F] = \deg f(x)$. Then by 6.4 $[E : F] = [E : F(a)][F(a) : F] = [E : F(a)] \cdot \deg f(x)$. So the degree of $f(x)$ divides $[E : F] = n$.*

Example 6.10 (Gallian 20.13)**.** *Let a be a root of $f(x) \in F[x]$ in some extension of F. Find $g(x) \in F[x]$ s.t $g(ab + c) = 0$. This is just the polynomial $f(\frac{x-c}{b})$. Which we know exists because $c, b \in F$ a field so c, b have additive, and multiplicative inverses.*

Example 6.11 (Gallian 20.59)**.** *Let a, b belong to some field extension of F. Prove $[F(a, b) : F(a)] \leq [F(a, b) : F]$. Since $F(a, b)$ extends both $F(a)$, and $F(b)$ we can use thm 6.4 to write*

$$[F(a, b) : F] = [F(a, b) : F(a)][F(a) : F]$$

Then $[F(a, b) : F(a)] \Big| [F(a, b) : F] \implies [F(a, b) : F(a)] \leq [F(a, b) : F]$ (if something divides something else its upperbounded by that thing).

Example 6.12 (Gallian 20.53)**.** *This exercise is incomplete! Let a be a complex 0 of $x^3 - 1$. Show that $Q(\sqrt{a}) = Q(a)$. $x^3 - 1 = (x - 1)(x^2 + x + 1)$, so the complex roots of $x^3 - 1$ are the roots of $x^2 + x + 1 \in Q[x]$. They are both imaginary so $a \notin Q$, and of course since they are the roots of $x^2 + x + 1$, we know $[Q(a) : Q] = 2$ for either root a. Now using thm 6.4*

$$[Q(\sqrt{a}) : Q] = [Q(\sqrt{a}) : Q(a)][Q(a) : Q] = 2 \cdot [Q(\sqrt{a}) : Q(a)]$$

$[Q(\sqrt{a}) : Q] \leq 6$, $[Q(\sqrt{a}) : Q(a)] \leq 2$, $[Q(a) : Q] \leq 3$.

7 Galois Theory

This is all about automorphisms of fields.

Definition 7.1 (Automorphism, Galois Group, Fixed Field)**.** *Let E be an extension of F.*

1. *An automorphism of E is a ring isomorphism from E to E.*

2. *The Galois group of E over F denoted Gal (E/F) is the set of automorphisms of E that fix F, ie F is a subset of its fixed field*

3. *The fixed field of a subgroup of Gal (E/F) is the set of all elements any automorphism in Gal (E/F) sends to themselves. IE the set*

$$E_H = \{x \in E | \phi(x) = x, \ \forall \phi \in \text{Gal}\,(E/F)\}$$

is called the fixed field of H.

This next theorem is basically all that we covered of Galois theorem. In retrospect we really only touched it for a second. Which I guess is why theres only two review exercises for it. Lets try to to break this down, and explain some of its consequences.

Theorem 7.2 (The fundamental theorem of Galois theory)**.** *Let F be a field of characteristic 0 or a finite field (better to think about it as finite). In this thm K denotes a subfield of K that contains F.*

1. *If E an extension of F is the splitting field of some polynomial in $F[x]$ then there is a bijection from the set of subfields of E that contain F to the subgroups of the Galois groups Gal (E/F). This bijection sends a subfield $K \subset E$ to the subgroup Gal (E/K). More formally*

$$\rho : \{ \text{ subfields of } E \text{ that contain } F\} \to \{ \text{ subgroups of Gal}\,(E/F)\}, \quad \rho(K) = \text{Gal}\,(E/K)$$

is a bijection whenever E is a splitting field.

2. $[E : K] = |\text{Gal}\,(E/K)\,|$, *and* $[K : F] = |\text{Gal}\,(E/F)\,|/|\text{Gal}\,(E/K)\,|$.

I'm not going to write down the other parts of the theorem because we didn't talk about them so probably not important for the course. The main thing we talked about is (1), and really it seems to be the coolest part anyway. Instead of asking about subspaces of a vector space, we can think about subgroups of its automorphism group. In practice both of these things can be intractable to enumerate, but I bet it still has some interesting consequences in finite cases.

Example 7.3 (Gallian 30.7)**.** *Let $A = \{a_1, a_2, ..., a_n\}$ be the set of roots of $f(x) \in F[x]$, and let $K = F(a_1, a_2, ..., a_n) = \{c_0 + c_1a_1 + c_2a_2 + \cdots + c_na_n | c_i \in F\}$, be the splitting field of $f(x)$. Show that Gal (K/F) is isomorphic to S_A the set of permutations of A. This is interesting, and follows from the fact all any automorphism can do is shuffle around the roots. Let $\phi \in$ Gal (K/F) then if $k \in K$*

$$\phi(k) = \phi(k_0 + k_1a_1 + k_2a_2 + \cdots + k_na_n) = k_0 + k_1\phi(a_1) + k_2\phi(a_2) + \cdots + k_n\phi(a_n)$$

So ϕ is entirely determined by what it does to the a_i's. Of course it can't send any of the a_i to an element of F since it fixes F, so it must send each a_i to another a_j. Then since it is a bijection the restriction of ϕ to A is a bijection from A to itself (a permutation). I'm not going to prove that every permutation corresponds to a valid automorphism, but I think thats pretty obivious. In short the isomorphism from Gal (K/F) to S_A would just send each $\phi \in galK/F$ to its restriction to A ($\phi \to \phi|_A$).

Example 7.4 (Gallian 30.8)**.** *Show that the Galois group of a polynomial of degree n has order dividing $n!$. Let K be the splitting field of $f(x) \in F[x]$, with $\deg f(x) = n$, and $A = \{a_1, a_2, ..., a_m\}$ be set of its roots. By the previous exercise Gal $(K/F) \cong S_A$, thus $|\text{Gal}\,(K/F)\,| = |S_A| = m!$. Then since a polynomial of degree n has at most n distinct roots $m \leq n \implies m!|n!$.*

8 Cyclotomic Extensions

Cyclotomic polynomials, and the roots of unity have lots of surprising connections to other things. For example in 531 we proved an identity for the q-binomial coefficient $\binom{n}{k}_q$ when q is a root of unity. Of course they have lots of connections to cryptography as well. First DeMoivre's theorem.

Theorem 8.1 (DeMoivre's Theorem)**.** *For all $n \in \mathbb{N}$, and $\theta \in \mathbb{R}$ we have*

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

Now we can define the n-th roots of unity.

Theorem 8.2 (Zeros of $x^n - 1$)**.** *Let $w = \cos(\frac{2\pi}{n} + i\sin(\frac{2\pi}{n})$, then*

$$(x^n - 1) = (x-1)(x-w)(x-w^2)\cdots(x-w^n)$$

Proof. Since $x^n - 1$ has degree n (and thus at most n zeros) it suffices to show that $(w^k)^n - 1 = 0$ for all $k \in \{0, 1, .., n\}$, and that each of the w^k is distinct.

1. Maybe that they are distinct is obvious, but anyway

$$\begin{aligned} w^k = w^m &\iff [\cos(\frac{2\pi}{n} + i\sin(\frac{2\pi}{n})]^k = [\cos(\frac{2\pi}{n} + i\sin(\frac{2\pi}{n})]^m \\ &\iff 1 = [\cos(\frac{2\pi}{n} + i\sin(\frac{2\pi}{n})]^{m-k} \\ &\implies m - k = 0 \iff m = k \end{aligned}$$

2. $(w^k)^n - 1 = 0 \iff w^{nk} = 1$ which follows from DeMoivre's theorem.

$$\begin{aligned} w^{nk} &= [\cos(\frac{2\pi}{n} + i\sin(\frac{2\pi}{n})]^{nk} \\ &= \cos(\frac{2nk\pi}{n} + i\sin(\frac{2nk\pi}{n}) \\ &= \cos(2k\pi) + i\sin(2k\pi), \text{ cos of some multiple of } 2\pi \text{ is 1, and likewise sin is 0} \\ &= 1 + 0 = 1 \end{aligned}$$

So $\{1, w, w^2, ..., w^{n-1}\}$ are n zeros of $x^n - 1$, and since $x^n - 1$ has at most n zeros it factors into the roots of unity. □

The n-th roots of unity form a cyclic group of order n, and are thus isomorphic to $\mathbb{Z}_n$.

Proof: n-th roots of unity are isomorphic to the group $\mathbb{Z}_n$. That they are a group is also probably obvious, but anyway

1. Identity: $1 = w^0 = w^n$ is obviously the identity
2. Inverses: For $k \in \{0, 1, ..., n\}$ we know $n - k \in \{0, 1, .., n\}$, and $w^k \cdot w^{n-k} = w^{n-k+k} = w^n = 1$

I'm skipping associativity. Clearly it is cyclic since it is generated by w. Thus it is isomorphic to $(\mathbb{Z}_n, +)$ with the obvious bijection $w^k \to k$. Then as generators must map to generators, and k generates $\mathbb{Z}_n$ iff $\gcd(n, k) = 1$ we know that w^k s.t $\gcd(k, n) = 1$ generate $\{1, w, .., w^{n-1}\}$. Of course there are $\phi(n)$ $k < n$ coprime to n the n-th roots of unity also have $\phi(n)$ generators. □

Definition 8.3 (Primitive Root of Unity). *$w^k \in W_n = \{1, w, .., w^{n-1}\}$ is called a primitive root of unity if it generates W. Ie $\langle w^k \rangle = W$.*

Of course this happens exactly when $\gcd(k, n) = 1$. Now we can define the n-th cyclotomic polynomial.

Definition 8.4 (n-th Cyclotomic Polynomial). *Let W_n be the n-th roots of unity, and denote its $\phi(n)$ primitive roots by $w_1, w_2, ..., w_{\phi(n)}$. Then the n-th cyclotomic polynomial is given by*

$$\Phi_n(x) = \Pi_{i=1}^{\phi(n)}(x - w_i)$$

Ie it is the unique polynomial with 0s at each of the primitive n-th roots of unity.

Theorem 8.5 (Recursion for $\Phi_n(x)$). *For each $n \in \mathbb{N}$, $x^n - 1 = \Pi_{d|n}\Phi_d(x)$. Where $d|n$ means the product runs over all divisors of n.*

Theorem 8.6. *$\Phi_n(x)$ is monic, has integer coefficients, and is irreducible over $\mathbb{Z}$.*

Theorem 8.7 (Galois Group of $\Phi_n(x)$). *Let w be a primitive n-th root of unity, then Gal $(Q(w)/Q) \cong U(n)$.*

Note $Q(w)$ is the splitting field of $x^n - 1$, also $U(n) = \{k < n | \gcd k, n = 1\}$.

Theorem 8.8 ($U(n)$ as a direct product). *Let $U(n)$ denote the group of multiplicative units mod n. Then if $n = ab$ for coprime a, b, $U(n) \cong U(a) \oplus U(b)$. $U(n)$ is isomorphic to a direct product of its factors (in a sense).*

This might be useful for some of the exercises, but it comes from chapter 8. It is theorem 8.3 in gallian.

Example 8.9 (Gallian, 31.1). *Find the minimal polynomial of $\cos(\pi/3) + i\sin(\pi/3)$. Recall that th minimal polynomial of some field element a is the unique monic irreducible polynomial with a as a root. Since $\Phi_n(x)$ is monic, and irreducible, and all its roots are the primitive n-th roots of unity, then $\Phi_n(x)$ is the minimal polynomial for any of the primitive n-th roots. Now $\cos(\pi/3) + i\sin(\pi/3) = \cos(2\pi/6) + i\sin(2\pi/6)$ is a primitive 6-th root of unity ($w \in W_6$), thus its minimal polynomial is $\Phi_6(x)$.*

Example 8.10 (Gallian, 31.2). *Factor $x^{12} - 1$ as a product of irreducible polynomials in Z. By thm 8.5*

$$x^{12} - 1 = \Pi_{d|12}\Phi_d(x) = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x)$$

Each is irreducible in Z, by thm 8.6.

Example 8.11 (Gallian, 31.16). *Prove that $x^9 - 1$, and $x^7 - 1$ have isomorphic galois groups over Q. Let w_9 be a primitive 9-th root of unity, and w_7 be a primitve 7-th root. Then $Q(w_9)$, and $Q(w_7)$, are the splitting fields of the above polynomials. The galois group of $x^9 - 1$ over Q is Gal (w_9/Q), and similarly Gal (w_7/Q) is the galois group of $x^7 - 1$. By thm 8.7 Gal $(w_9/Q) \cong U(9)$, and Gal $(w_7/Q) \cong U(7) = \mathbb{Z}_7^\times$ (anything is a generator since 7 is prime). Now $U(9) = \{1, 2, 4, 5, 7, 8\}$ is also cyclic group of order 6 (with generator 2). Thus both galois groups are cyclic order 6, and are therefor isomorphic.*

Example 8.12 (Gallian, 31.18). *Prove that the galois groups of $x^{10} - 1$, and $x^8 - 1$ are not isomorphic. Similar to the previous exercise Gal $(w_10/Q) \cong U(10) = \{1, 3, 7, 9\}$ and is thus cyclic order 4 (check for a generator), and Gal $(w_8/Q) \cong U(8) = \{1, 3, 5, 7\}$ is not cyclic. $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \mod 8$. So they are not isomorphic.*

9 Algebraic Coding Theory

Definition 9.1 (Linear Codes). *An (n, k) linear code over a finite field F is k-dimensional subspace V of the vector space*

$$F^n = \underbrace{F \oplus F \oplus \cdots \oplus F}_{ntimes}$$

Over F.

- *The vectors $v \in V$ are called code words*
- *When $F = \mathbb{Z}_2$ the code is called binary*

So a linear code is vector space. The code words are our vectors.

Example 9.2 (Gallian 29.21). *How code words are their in a $(6, 4)$ ternary linear code. Since the code is ternary were working in a vector space over $\mathbb{Z}_3$. Since $k = 4$ were working in a 4 dimensional subspace. Then we need only count number of linear combinations we can have of our 4 basis vectors. Let v_1, v_2, v_3, v_4 be our basis vectors. Then*

$$|\{c_1v_1 + c_2v_2 + c_3v_3c_4v_4|c_i \in \mathbb{Z}_3| = 3^4 = 81$$

Since we have 3 choices for each coefficient, and 4 coefficients to choose. In general if $|F| = q$, and we have a (n, k) linear code over F, then we have q^k code words, by the same argument as above.

Definition 9.3 (Hamming Distance/Weight). *Let $u, v \in F^n$.*

- *The hamming weight of u is given by wt $(u) =$ (# non-zero components of u).*

- *The hamming distance from u to v is given by*

  $d(u,v) = (\text{\# components in which } u \text{ differs from } v) = (\text{\#non-zero components in } (u-v)) = wt\,(u-v)$

- *The hamming weight of an (n,k) linear code is the minimum weight of any non-zero code word. Ie if C is the set of code words an (n,k) linear code, then hamming weight of (n,k) equals $\min_{v \in C | v \neq 0} wt\,(v)$.*

Any linear code is metric under $d(\cdot,\cdot)$ as well show in one of the exercises. The hamming distance satisfies the triangle inequality.

Theorem 9.4. *For any $u, v, w \in F^n$ we have that $d(u,v) \leq d(u,w) + d(w,v)$.*

Theorem 9.5. *If the hamming weight of a (n,k) linear code is at least $2t+1$ it can correct t or fewer errors,* **or** *detect any $2t$ or fewer errors. It cannot do both simultaneously.*

Basically it can correct errors roughly half its weight, and correct errors roughly its weight. The proof is instructive. Just using nearest neighbor decoding we know if a transmitted code v is received as v', and it contains at most t erros, then its closest code word will be v.

Remark 9.6 (Generator Matrices)**.** *For an (n,k) linear code over a field F, any $k \times n$ matrix with linearly independent rows can serve as a generator matrix for the code, there are definitely simple linear algebraic reasons for this that I don't want to think about rn, however the standard generator matrix is prefered. It just has the $k \times k$ identity in its 1st k columns. More formally its the block matrix $G = [I_{k\times k}|A_{k\times(n-k)}]$. This has the effect of having the first k components of the codeword being equal to the original message.*

Definition 9.7 (Parity Check Matrix)**.** *Let the $k \times n$ block matrix $G = [I_k|A]$ be the standard generator matrix of the (n,k) linear code. Then the $n \times k$ block matrix $H = \left[\frac{-A}{I_{n-k}}\right]$ is called the parity check matrix of (n,k).*

Below is the **decoding procedure** for recovering a message from a word w given the parity matrix H of a linear code (n,k) over F.

1. Given a received word w compute wH.
2. If $wH = 0$ then assume no error was made, and that our message is indeed w.
3. Denote the i-th row of H by H_i. If $wH = sH_i$ for some $s \in F$, then assume there was an error in the i-th component and that the original message is $w - [0, 0, ..., \underbrace{s}_{\text{component } i}, ..., 0]$. That is subtract s from the i-th row of w.
4. If neither of the above occured than assume that more than two errors occured, and therefor we cannot decode the message.

Theorem 9.8 (Parity Check Matrix decoding)**.** *Parity-check matrix decoding will correct any single error if and only if the rows of the parity-check matrix are nonzero and no one row is a scalar multiple of any other row (ie the rows are independent).*

So basically if were acked to determine if a parity check matrix can correct any errors it suffices to check that all its rows are linearly independent. Which in the binary $\mathbb{Z}_2$ just means that they are non-zero, and distinct.

Example 9.9 (Gallian 29.4)**.** *For any vector space V, and $u, v, w \in F^n$ prove that hamming distance has the following properties.*

1. *$d(u, v) = d(v, u)$:*

   $$d(u,v) = wt\,(u-v) = (\#\text{ non-zero components of } u-v) = (\#\text{ non-zero components of } v-u) = d(v,u$$

   Where the 2nd equality jst follows from negating something non-zero cannot make it zero.

2. *Show that $d(u, v) = 0$ iff $u = v$*

   $$d(u,v) = wt\,(u-v) = (\#\text{ non-zero components of } u-v) = 0 \implies u_i - v_i = 0 \forall i \in [n]$$

   Thus $u_i = v_i$ for all i and therefor $u = v$.

3. *Show that $d(u, v) = d(u + w, v + w)$.*

   $$d(u+w,v+w) = wt\,(u+w-(v+w)) = wt\,(u+w-v-w) = wt\,(u-v) = d(u,v)$$

Example 9.10 (Gallian 29.4)**.** *Can the parity check matrix*

$$H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

correct a single error? No, by thm 9.8 since its rows are not independent $H_2 = 01 = H_5$.

Example 9.11 (Gallian 29.4)**.** *Can the parity check matrix*

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

correct a single error? Yes, by thm 9.8 since its rows are distinct and non-zero (suffices to just check distinct and non-zero since its binary, what scalers do you have?)