**Syllabus:**

- **Rings:** Chapter 10, all, Chapter 11, Sections 1-5. (If you like the stuff in 11.5, you should take Math 575).
- **Modules:** Chapter 12, all
- **Fields:** Chapter 13
- **Galois Theory:** Chapter 14.

**Monday April 16.** We had finished the material of the course friday, so we ate cookies and talked about projective space. Students also signed up for the **ORAL FINAL EXAM** to be held in addition to the regular exam Friday April 20, 1:30—3:30.

**Friday April 13.** Today we proved Theorems A and B, which as you recall were two “black boxes” in our proof of the Main Theorems of Galois Theory. Theorem A stated: If $H$ is any finite group of automorphisms of a field $K$, then the extension $K^H \hookrightarrow K$ is of degree $|H|$. The proof is a cool application of the orbit-stabilizer theorem from Math 512. First we observed that if $H$ acts on $K$ by (field) automorphisms, then $H$ also acts on $K[x]$ by ring automorphisms, just by acting on the coefficients. Furthermore, the set of elements of $K[x]$ fixed by $H$ is the subring $(K[x])^H = K^H[x]$. Now, take any $\beta \in K$. Let $\{\beta_1, \beta_2, \ldots, \beta_r\}$ be the orbit of $\beta = \beta_1$ under $H$. We saw that the polynomial $g(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_r)$ is fixed by $H$ so that $g(x) \in K^H[x]$. This means that $\beta$ is algebraic over $K^H$. Furthermore, $g(x)$ is irreducible, and hence is the minimal polynomial of $\beta$ over $K^H$. Indeed, by the “Crucial Lemma,” any polynomial $f \in K^H[x]$ satisfied by $\beta$ must also be satisfied by any $\sigma(\beta)$ where $\sigma \in H$. So all the $\beta_i$ must be roots of $f$. So $g$ is the smallest degree polynomial over $K^H$ satisfied by $\beta$, and hence its minimal polynomial. [Since the roots of $g$ are all distinct, incidentally, it also follows that $K$ is separable over $K^H$.] Now we prove Theorem A under the additional assumption that $K$ has a primitive element over $K^H$. [This is always the case; in the homework you proved this when $K^H$ is infinite (eg, characteristic zero).] That is, $K = K^H(\gamma)$ for some $\gamma \in K$. The degree of $K/K^H$ is therefore the degree of the minimal polynomial over $K^H$. We just showed that this degree is the cardinality of the orbit of $\gamma$ under $H$. By the orbit stabilizer theorem, $|H| = |\text{Orbit}(\gamma)||\text{Stab}(\gamma)|$. So we need to show that the stabilizer of $\gamma$ is trivial. But this is easy! Any $\sigma \in H$ fixing $\gamma$ obviously fixes all of $K$ (and therefore is the identity automorphism of $K$) since $\sigma$ is determined by where it sends $\gamma$. QED (Theorem A).

Theorem B states: A finite extension $F \subset K$ is Galois if and only if it is the splitting field for a separable polynomial. Again, let us only prove this in characteristic zero, for simplicity, although it is true in general. Again, we can assume $K = F(\gamma)$. Let $g(x)$ be the minimal polynomial for $\gamma$ over $F$. Theorem B will be proved it we can show that $K$ is the splitting field for $g$ if and only if $F \subset K$ is Galois. Let $\gamma_1, \ldots, \gamma_n$ be all the roots of $g(x)$ in...
\(\mathbb{F}\), and order them so that the first \(p\) are in \(K\), and the remaining are not. Of course, \(n\) is the degree of \(K/F\). If we can also show that \(p\) is the order of \(Gal(K/F) = G\), our claim will be proven. But this is easy: Each \(\sigma \in G\) is uniquely determined by where it sends \(\gamma\). There is unique an \(F\)-isomorphism \(F(\gamma_1) \rightarrow F(\gamma_i)\) sending \(\gamma_1\) to \(\gamma_i\) for all \(i\); this \(F\)-isomorphism is a \(F\)-automorphism of \(K\) if and only if \(\gamma_i\) is in \(K\). Furthermore, every \(F\)-automorphism of \(K\) is one of these, since any \(\sigma \in Gal(K/F)\) sends \(\gamma_1\) to some other root of \(g\). Thus the order of \(G\) is \(p\). The proof of Theorem B is complete (again, in characteristic zero). **Assignment:** Think of any questions you might have or topics you want addressed in the last lecture, and let me know by Sunday evening. I will try to accommodate them. Reread all the relevant sections of Artin and Stewart; make sure you get it all! The sign-up sheet for ORAL FINALS will be posted on my door MONDAY. In-class exam Friday April 20.

**Wednesday April 11.** We proved the following theorem: If an irreducible polynomial over \(\mathbb{Q}\) of prime degree \(p\) has exactly two non-real roots, then its Galois group is \(S_p\). [The proof is quite simple: Let \(K\) be the splitting field, and \(G\) the Galois group of \(K/\mathbb{Q}\). We already know \(G\) is a subgroup of \(S_p\), the permutation group of the roots. If \(\alpha\) is any root of the polynomial, then the intermediate extension \(\mathbb{Q} \subset \mathbb{Q}(\alpha)\) is of degree \(p\). The corresponding subgroup of \(G\) is index \(p\), so we know that \(p\) divides the order of \(G\) and since \(p\) is prime, there must be an element of order \(p\). The only order \(p\) elements in \(S_p\) are the \(p\)-cycles. On the other hand, complex conjugation \(\tau\) is also an element of \(G\), and since \(\tau\) fixes the real roots of \(f\) it must be the transposition of the two non-real roots. But it is easy to check that \(S_p\) is generated by any transposition and any \(p\)-cycle. QED.] We then applied the theorem to check that the Galois group of \(x^5 - 6x + 3\) has Galois group \(S_5\). Because \(S_5\) is not solvable, by the theorem from last time, the extension \(\mathbb{Q} \subset K\) is not radical. It follows that the roots of \(x^5 - 6x + 3\) are not expressible in radicals over \(\mathbb{Q}\). **Information about the Final:** There will be a T/F exam during the regularly scheduled time slot for our final: Friday April 20 at 1:30 in the usual room. The real fun will be the ORAL EXAM: Next monday, I will place a sign-up sheet outside my door for you to sign up for a 30-minute oral exam. Some problems to work on will be distributed.

**Monday April 9.** We began talking about “solvability by radicals.” First, we informally defined an element \(\alpha \in \mathbb{F}\) to be expressible by radicals over \(F\) if \(\alpha\) can be written from elements of \(F\) using \(+, -, \times, \div, \sqrt{\cdot}\) where \(n \in \mathbb{N}\). For example, \((\sqrt[6]{77} + 3\sqrt[10]{77})\frac{4}{3} + 5\) is expressible in radicals over \(\mathbb{Q}\). **An amazing fact you may not know:** there are algebraic numbers, such as the roots of \(x^5 - 6x + 3\) which are not expressible in radicals!!! Formally, we say \(\alpha \in \mathbb{F}\) is expressible in radicals over \(F\) if \(\alpha \in K\) where \(K\) is some finite radical extension over \(F\). Here, \(F \subset K\) is a finite radical extension means that we can write \(K = F(\alpha_1, \ldots, \alpha_n)\) where each \(\alpha_i\) satisfies \(\alpha_i^{a_i} = a_i \in F(\alpha_1, \ldots, \alpha_{i-1})\). Note that radical extensions need not be Galois (for example, \(\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{3})\) is radical but not Galois). However, the “Galois closure” of a radical extension is Galois. For example, the splitting field of \(X^4 - a\) over \(F\) will factor as \(F \subset F(\zeta_t) \subset F(\zeta_t, \sqrt[4]{a})\) which is radical (and Galois, provided
$X^t - a$ is separable, which it always is in characteristic zero, or even in characteristic $p$ if $p$ does not divide $t$). The brilliant observation of Galois was this: **if a finite Galois field extension $F \subset K$ is radical, then its Galois group is very special.** Indeed, let us think about the splitting field of $X^t - a$ (when the characteristic $p$ does not divide $t$). It factors as

$$F \subset F(\zeta_t) \subset F(\zeta_t, \sqrt[n]{a}) = K$$

where $\zeta_t$ is a primitive $t$-th root of unity. We proved a lemma: the Galois group of $K/F(\zeta_t)$ is always abelian. The fundamental theorem of Galois theory tells us it is also normal in $\text{Gal}(K/F)$ because the cyclotomic extension $F \subset F(\zeta_t)$ is Galois. Furthermore; $\text{Gal}(F(\zeta_t)/F) \cong G/H$. Now, you have computed on your homework that the Galois group of the cyclotomic extension $F \subset F(\zeta_t)$ is naturally isomorphic to $(\mathbb{Z}/t\mathbb{Z})^\times$. Thus we have just found an sequence of subgroups:

$$G \supset H \supset \{e\}$$

where each group is normal in its predecessors and the quotients are all abelian. That is: the group $G$ is SOLVABLE! Our next goal is to prove the following theorem: A finite Galois extension $F \subset K$ is radical if and only if its Galois group is solvable. **Assignment:** Read Stewart Chapter 14 (reviews solvable groups) and Chapter 15.

**Friday April 6.** We worked out the full Galois correspondence in the example of the splitting field of $x^4 - 2$ over $\mathbb{Q}$. We computed all the subgroups of the Galois group (which is isomorphic to $D_4$, so you’ve done it before). We then computed all the intermediate fields. We looked at the actions of Galois groups on on the set of intermediate fields $\mathcal{F}$ and on the set of subgroups $\mathcal{G}$. We saw which extensions were normal over $\mathbb{Q}$. Most of this is worked out also in Stewart; Chapter 13, although Stewart does not emphasize that the Galois correspondence between $\mathcal{G}$ and $\mathcal{F}$ also respects the $G$-actions on these sets.

**Wednesday April 4.** We proved the Second Main Theorem of Galois theory: Fix a finite Galois extension $F \subset K$; then under the Galois correspondence between the intermediate fields and subgroups of the Galois group $G = \text{Gal}(K/F)$, the Galois extensions of $F$ precisely correspond to the normal subgroups of $G$. Furthermore, when $F \subset E$ is Galois, its Galois group is $G/H$ where $H$ is the group corresponding to $E$. The proof is very interesting and instructive. If we let $\mathcal{F}$ denote the set of intermediate fields and let $\mathcal{G}$ denote the set of subgroups of $G$, we showed that the natural action of $G$ on $\mathcal{F}$ (discussed last time, in which $E \mapsto gE$ corresponds (under the Galois correspondence) to the natural action of $G$ on $\mathcal{G}$ by conjugation ($H \mapsto gHg^{-1}$). It then is easy to check that $H \in \mathcal{G}$ is normal if and only if it is fixed by $G$. Similarly, we showed that $E \in \mathcal{F}$ is fixed by $G$ if and only if $E$ is Galois. The point in the latter statement is that if $E$ is Galois, we can write it as a splitting field $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where the $\alpha_i$ are all the roots of some (separable) polynomial of degree $n$; it then follows from the “Crucial Lemma” that every $F$-automorphism of $K$ sends each $\alpha_i$ to some other $\alpha_j$, that is, each $g \in G$ sends $E$ back to $E$. Likewise, last time we showed the converse: that if $E$ is fixed (set-wise) by $G$, then $E$ is Galois. **Read:** Stewart Chapter 13, which gives a cool example, and 14, which reviews “solvable” groups.
Monday April 2. We took Quiz 6. Fix a Galois extension $F \subset K$, with Galois group $G$. Given an intermediate field $E$, we know that $E \subset K$ is always Galois, and its Galois group $H$ is exactly the group corresponding to $E$ under the “Galois correspondence.” Question: What about $F \subset E$? When is it Galois?

We observed that $G$ acts on the set $\mathcal{F}$ of all intermediate fields. That is, if $E$ is an intermediate field, then $gE$ is also an intermediate field, for each $g \in G$ (BE SURE YOU SEE WHY!!). Consider a field $E$ that is a fixed point for this $G$-action on $\mathcal{F}$; that is, consider a field $E$ satisfying $g(x) \in E$ for all $x \in E$ for every element $g \in G$. We proved that such an intermediate field is Galois, and that its Galois group is isomorphic to $G/H$ where $H$ is the subgroup of $G$ corresponding to $E$. The proof is conceptually instructive: because each $g \in G$ takes $E$ back to $E$ (as a set), the restriction of $g : K \to K$ to the subset $E$ gives a well-defined map $g|_E : E \to E$ which is easily checked to be an $F$-automorphism of $E$. That is, restriction to $E$ induces a group homomorphism $G \to \text{Gal}(E/F)$. It is easy to check that the kernel of this map is $\text{Gal}(K/E) = H$ (in particular, $H$ must be normal!). This means that $G/H \hookrightarrow \text{Gal}(E/F)$. So $[G : H] = |G/H|$ divides $|\text{Gal}(E/F)|$, which in turn divides $[E : F]$. But since the Galois correspondence implies that $[G : H] = [E : F]$, we must have equality all along, that is $G/H \cong \text{Gal}(E/F)$. Next time will will investigate further the action of the Galois group on the set $\mathcal{F}$ of all intermediate fields and use it to prove the Second Main theorem of Galois theory. Keep reading the assigned sections!

Friday March 30. We stated two theorems (which will be proven later). Theorem A: If $H$ is a group of automorphisms of some field $K$, then $|H| = [K : K^H]$. Theorem B: A finite extension $F \subset K$ is Galois if and only if it is the splitting field of some separable polynomial. [Recall: A polynomial $g(x) \in F[x]$ if each of its irreducible factors has the property that it has no multiple roots in any extension field. You showed on the homework that every polynomial is separable over any field $F$ of characteristic zero.] Assuming these two theorems, we were able to prove much of the Galois Correspondence. Specifically, we proved the “First Theorem” stated last time, and the “Galois Correspondence” theorem.) Read: Artin 14.4 and 14.5. Also, Stewart chapter 9, 11, 12, 13.

Wednesday March 28. We stated the main theorems of Galois theory and looked at them in the examples computed last time. First Theorem: If $F \subset K$ is any finite extension, then the order of its Galois group divides the degree of the extension. This gives rise to a definition: A finite extension $F \subset K$ is Galois if equality holds. We observed that the examples studied last time were all Galois. A non-Galois extension is $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$. [We also remarked (it will eventually be proved) that the splitting field of any separable polynomial is Galois, so for example, any splitting field extension in characteristic zero is Galois. These are what Galois was actually studying.] Now, the Galois Correspondence says: If $F \subset K$ is a Galois extension with Galois group $G$, then there is a bijective order reversing correspondence between the subgroups of $G$ and intermediate fields between $F$ and $K$. The bijection is given by $H \mapsto K^H$, the fixed field of the subgroup $H$. Its inverse sends the intermediate field $E$ to the group $\text{Gal}(K/E)$ [Caution: Note which extension is involved!] which is obviously
Monday March 26. We completed the worksheet from Wednesday and/or did Worksheet on Cyclotomic Extensions. Katie, Alex, and Nick explained three different examples of the “Galois correspondence” on the blackboard at the end. Katie did the splitting field for \( x^3 - 2 \) over \( \mathbb{Q} \), an extension of degree 6. Its Galois group is the full group of all permutations of the three roots. There are six subgroups, which correspond to the six intermediate extensions: the full group fixes only \( \mathbb{Q} \); the three cyclic groups of order two each fix one root, so the corresponding three fixed fields are \( \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2} \omega), \mathbb{Q}(\sqrt[3]{2} \omega^2) \), where \( \omega \) is a third root of unity; the cyclic group of order 3 fixes \( \mathbb{Q}(\omega) \); and the trivial group fixes the full splitting field. Alex explained the splitting field for \( (x^2 - 5)(x^2 + 1) \) over \( \mathbb{Q} \), an extension of degree 4. Its Galois group is a Klein 4-group, generated by the transpositions \( \tau \) (switching \( \sqrt{5} \) and \( -\sqrt{5} \)) and \( \sigma \) (switching \( i \) and \( -i \)). There are three proper non-trivial subgroups, each of order 2, with the corresponding fixed fields \( K^\tau = \mathbb{Q}(i), K^\sigma = \mathbb{Q}(\sqrt{5}) \) and \( K^{\tau \sigma} = \mathbb{Q}(i\sqrt{5}) \). Finally, Nick explained the splitting field \( K_5 \) for \( x^5 - 1 \), which is an extension of degree 4 over \( \mathbb{Q} \), generated by a primitive fifth root of unity \( \zeta_5 \). The Galois group is cyclic of order 4, generated by the permutation \( \phi \) of the primitive fifth roots of unity \( \zeta_5 \mapsto \zeta_5^2; \zeta_5^2 \mapsto \zeta_5^4; \zeta_5^4 \mapsto \zeta_5^3; \zeta_5^3 \mapsto \zeta_5 \). This group has only one proper non-trivial subgroup, namely the order two subgroup generated by \( \phi^2 \) (which switches \( \zeta_5 \) and \( \zeta_5^4 \), as well as \( \zeta_5^2 \) and \( \zeta_5^3 \)). The Galois group \( G \) thus has only one chain of subgroups: \( \{ e \} \subset \langle \phi^2 \rangle \subset G \). These correspond to the fixed fields: \( K_5 \supset \mathbb{Q}(\zeta_5 + \zeta_5^4) \supset \mathbb{Q} \). Next time we will state the Main theorem of Galois Theory and see these all as examples of it. Read: Artin 14.1 and 14.2.

Stewart: Chapter 8 through 8.6 (third edition)

Friday March 23. Exam 2

Wednesday March 21. We did a worksheet analyzing the field extension \( \mathbb{Q} \subset K = \mathbb{Q}(\omega, \sqrt[3]{2}) \). Many students discovered the following main points: 1) \( K \) is the splitting field of the polynomial \( x^3 - 2 \) over \( \mathbb{Q} \), and its degree \([K : \mathbb{Q}]\) is six; 2) its Galois group \( G \) is isomorphic to the full group of all permutations of the three roots \( \{ \sqrt[3]{2}, \sqrt[3]{2} \omega, \sqrt[3]{2} \omega^2 \} \); 3) each subgroup \( H \) of \( G \) gives rise to an intermediate field \( K^H \) (between \( \mathbb{Q} \) and \( K \)) consisting of the elements of \( K \) fixed by \( H \); 4) For the order 3 subgroup \( H \) of \( G \) consisting of the 3-cycles (and the identity), this fixed field \( K^H \) is \( \mathbb{Q}(\omega) \); 5) For each of the three order two
subgroups (generated by a transposition), the fixed field is one of the three extensions of \( \mathbb{Q} \) obtained by adjoining only one of the three elements \( \sqrt[3]{2}, \sqrt[3]{2}\omega, \) or \( \sqrt[3]{2}\omega^2 \); 6). The fixed field of \( G \) is \( \mathbb{Q} \) and the fixed field of \( \{e\} \) is all of \( K \); 7). Each intermediate field \( E \) gives rise to a subgroup of \( G \), namely the group of \( E \)-automorphisms of \( K \); 8) There is a one-one order reversing correspondence between the subgroups of \( G \) and the intermediate extensions of \( \mathbb{Q} \subset K \). This is the beginning of the beautiful Galois correspondence! Stay tuned for more Monday. **Friday is the second exam, in class. No make-up exams!** Over the weekend, I hope you’ll be reading more in Artin, Stewart, and the supplementary texts by Emil Artin and Dummit and Foote.

**Monday March 19.** We proved the following important Proposition: if \( F \subset K \) is any field extension, and \( \alpha \in K \) satisfies some polynomial \( g(x) \) with coefficients in \( F \), then the Galois group sends \( \alpha \) to some other root of \( g \). This means that the Galois group acts on the roots (in \( K \)) of any polynomial defined over \( F \) by permutations. As an immediate consequence, we saw that the Galois group of \( \mathbb{Q}(\sqrt[3]{2}) \) over \( \mathbb{Q} \) is trivial. Indeed, any \( \mathbb{Q} \)-automorphism of \( \mathbb{Q}(\sqrt[3]{2}) \) must fix \( \sqrt[3]{2} \) (since the other two roots, \( \sqrt[3]{2}\omega \) and \( \sqrt[3]{2}\omega^2 \) where \( \omega = e^{2\pi i/3} \), are not in the field). The Galois group is trivial because the field is somehow “too small.”

**Definition:** a splitting field of a polynomial \( f \) over \( F \) is the smallest field \( K \) which contains all the roots of \( f \).\(^1\) Splitting fields have interesting Galois groups! We observed that \( \mathbb{Q}(i, \sqrt{5}) \) is the splitting field for \((x^2 - 5)(x^2 + 1)\) over \( \mathbb{Q} \). We saw last time its Galois group was the Klein 4-group, and interpreted the elements as essentially (certain) permutations of the roots. The field \( \mathbb{Q}(\sqrt[3]{2}) \) is a not a splitting field of any polynomial over \( \mathbb{Q} \). Enlarging it to \( K = \mathbb{Q}(\omega, \sqrt[3]{2}) \), we get a degree six extension which is the splitting field for \( x^3 - 2 \). Our proposition implies that its Galois group can be viewed as a subgroup of the permutation group of the three roots of \( x^3 - 2 \). By explicit construction, we found \( \mathbb{Q} \)-automorphisms of degree 3 and 2, hence the Galois group is all of \( S_3 \). We stated (without proof, yet), that if \( \mathbb{Q} \subset K \) is a splitting field, then its degree is equal to the order of the Galois group! In fact, much much more is true: the structure of the Galois group will tell us “everything” about the field extension. **Assignment:** Read Artin 14.1, 14.2; Stewart Chapter 7 (second edition) or Chapter 8 (third edition).

**Friday March 16.** We defined a real number to be constructible if its absolute value is the length a segment constructed in any number of steps from two given point (we also consider 0 to be constructible.) We showed that the set of constructible numbers is a field \( K \). We proved that every \( \alpha \in K \) has degree \( 2^n \) for some \( n \). The point was the “key proposition” from last time, together with the multiplicative property of degree of field extensions. As a conclusion, we gave the example that “the cube can not be duplicated.”

We then started talking about Galois theory. If \( F \subset K \) is an extension, then an \( F \)-automorphism of \( K \) is a field isomorphism \( \pi : K \rightarrow K \) such that \( \phi(\lambda) = \lambda \) for all elements

---

\(^1\)By “smallest” we mean that if the roots of \( f \) live in some intermediate field \( K' \) (\( F \subset K' \subset K \)) then \( K' = K \). Any two splitting fields of \( f \) over \( F \) are isomorphic (as extensions of \( F \)– that is, by an isomorphism fixing \( F \)). All this is obvious for subfields of \( \mathbb{C} \).
of the ground field $F$. That is, it is a “automorphism in the category of extensions of $F$”—meaning that not only is it an (iso)morphism respecting the field structure of $K$, but it also respects our ground field $F$ by not touching it. The set of all $F$-automorphisms of $K$ forms a group under addition, called the Galois group of the extension $F \subset K$. We looked at the example of $K = \mathbb{Q} \subset \mathbb{Q}(\sqrt{5}, i)$ which is a degree 4 extension of $\mathbb{Q}$. There are exactly four $\mathbb{Q}$-automorphisms of $K$. The identity is one. How can we find the others? Say $\phi : K \to K$ is a $\mathbb{Q}$-automorphism. We know where each element of $\mathbb{Q}$ goes. If we also know where $\sqrt{5}$ and $i$ go, we’d be done, since $\phi$ must preserve both sums and products. Say $\phi$ sends $\sqrt{5}$ to $\alpha \in K$. What are the possible values of $\alpha$? Since $5 = \phi(5) = \phi(\sqrt{5}\sqrt{5}) = \phi(\sqrt{5})\phi(\sqrt{5}) = \alpha\alpha = \alpha^2$, we see that there are only two possible values for $\alpha$, either $\sqrt{5}$ or $-\sqrt{5}$. Similarly $\phi$ sends $i$ to $\pm i$. Thus there are four $\mathbb{Q}$-automorphisms of $K$: the identity, the map $\psi$ fixing $\mathbb{Q}(i)$ and sending $\sqrt{5}$ to $-\sqrt{5}$, the map $\psi'$ fixing $\mathbb{Q}(\sqrt{5})$ and sending $i$ to $-i$, and the composition $\psi \circ \psi'$ negating both $\sqrt{5}$ and $i$. Thus the Galois group is isomorphic to the Klein 4-group. The Galois group will tell us almost everything we want to know about the field extension, at least in the case of a so-called “Galois extension.” This is the beginning of a really beautiful story! 

### Wednesday March 14

In honor of $\pi$ day, we began the proof that the circle can’t be squared. That is, given a circle, it is impossible to construct, with compass and straightedge, a square with the same area. First, a definition: a collection $\mathcal{P}$ of points in $\mathbb{R}^2$ is said to be defined over $K$ (where $K$ is some subfield of $\mathbb{R}$) if both the $x$ and the $y$ coordinate of each $p \in \mathcal{P}$ is contained in $K$. We then proved a lemma: Let $p$ and $q$ be defined over $K$, then the line through $p$ and $q$ and the circle through $p$ with center $q$ are each given by equations with coefficients in $K$. For example, a (non-vertical) line through two points with rational coordinates is defined by an equation $y = mx + b$ where both $m$ and $b$ are rational. Likewise, a circle through a point with rational coordinates which has a center with rational coordinates is given $(x - a)^2 + (y - b)^2 = c$, where $a, b$, and $c$ are all rational. Using this lemma we proved the Key Proposition: If $\mathcal{P}$ is a collection of points defined over $K$ and $q = (\alpha, \beta) \in \mathbb{R}^2$ is constructed in one step from $\mathcal{P}$, then both $\alpha$ and $\beta$ satisfy a polynomial with coefficients in $K$ of degree two. We will do it next time carefully, but the point now is that the Key Proposition implies that the length of any constructible segment (starting with two points, which we declare to be $(0, 0)$ and $(1, 0)$) must have degree $2^n$ for some $n$. Squaring the (unit) circle would involve constructing a segment of length $\sqrt{\pi}$. [This is a proof modulo the fact that $\pi$ is transcendental; I won’t prove it; see Stewart.]

### Reading:

Continue reading the sections from Stewart already assigned, as well as Artin through the section on “constructions.”

### Monday March 12

We talked about “constructibility” of points, lines, circles, and “numbers” in the Greek style of mathematics. We start with two points $p_0$ and $p_1$. The line through
them is considered to be “constructed in one step,” as are the two circles, $C_1$ and $C_2$ with center at one of the points ($p_1$ or $p_2$) and passing through the other. The two intersection points of these two circles are now considered to be “constructed.” We inductively can construct more points (and lines, and circles) by adding in any points which are the intersection points of two already-constructed lines or circles. A number is said to be constructed if we can construct two points whose segment has that length. In this way, we showed in class that every natural number is constructed, as is $\frac{1}{2}, \sqrt{2}, \sqrt{3}$. We stated the fact (you will prove it in the homework) that all the positive rational numbers, as well as the square root of any such, are all constructible numbers. Fast-forwarding 1800 years, we come to the sixteenth century and the idea of coordinates. Corresponding to the successive addition of constructed points to the sets of points we have so far constructed

$$\{p_0, p_1\} = \mathcal{P}_0 \subset \mathcal{P}_1 = \mathcal{P}_0 \cup \{p_2\} \subset \cdots \subset \mathcal{P}_{i-1} = \{p_0, p_1, \ldots, p_i\} \subset \ldots$$

we have a tower of fields

$$K_0 \subset K_1 \subset \cdots \subset K_{i-1} \subset \ldots$$

where the field $K_i$ is defined to be the smallest subfield of $\mathbb{R}$ containing both the $x$ and $y$ coordinates of each point $p_0, p_1, \ldots, p_i$ in $\mathcal{P}_i$. That is, if $p_{i+1} = (\alpha, \beta)$ in coordinates, then $K_i = K_{i-1}(\alpha, \beta)$. It is convenient to choose coordinates so that $p_0 = (0, 0)$ and $p_1 = (1, 0)$. Then $K_0 = \mathbb{Q}$. We can construct the point $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ (as one of the two intersection points for the two circles constructed from $(0, 0)$ and $(1, 0)$). Letting $\mathcal{P}_1 = \{p_0, p_1, p_2\}$, we have that $K_1 = K_0\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) = \mathbb{Q}(\sqrt{3})$. We stated a lemma: if $\alpha$ is the $x$-coordinate (resp. $y$-coordinate) for $p_{i+1}$, then $\alpha$ satisfies a degree two polynomial over $K_{i-1}$. (Note: it need not be irreducible, so $\alpha$ might also satisfy a linear polynomial over $K_{i-1}$.

As you might already see, this means that any constructible number has degree a power of 2 over $\mathbb{Q}$, so many numbers (have line segments) cannot be constructed! We will discuss the proof of this lemma and its implications next time. **READ:** Stewart Chapter 7 (third edition) or Chapter 5 (second edition) and also Artin Chapter 13 through 13.5.

**Friday March 9.** We took Quiz 5. We then continued discussing degree. We proved that if $F \subset E \subset K$ are fields, then $[K : F] = [K : E][E : F]$. We defined a field extension $F \subset K$ to be algebraic if every $\alpha \in K$ is algebraic over $F$. We proved that if $F \subset K$ has finite degree, then $K$ is necessarily algebraic over $F$. But the converse is false: Solly gave the example of adjoining all the $2^n$-th roots of 3 to $\mathbb{Q}$. This gives a tower of field extensions

$$\mathbb{Q} \subset \mathbb{Q}(3^{\frac{1}{2}}) \subset \mathbb{Q}(3^{\frac{1}{3}}) \subset \mathbb{Q}(3^{\frac{1}{4}}) \subset \cdots,$$

where each successive extension has degree 2. (Be sure you see why!)\(^2\) So the composite extension $\mathbb{Q}(3^{\frac{1}{2^n}})$ has degree $2^n$ over $\mathbb{Q}$. Taking the union of all gives an algebraic extension of $\mathbb{Q}$ of infinite degree. Another example would be the field $\mathbb{Q}$ of all algebraic numbers over $\mathbb{Q}$. On the other hand, this does not happen for “simple” extensions (ones obtained by

\(^2\) Actually, I think Solly gave us roots of 2, not 3, but I thought maybe this example would rule out any confusion as to “which 2” is contributing the degree.
adjoining one element): For $\alpha \in K$, we noted that that $F(\alpha)$ is algebraic over $F$ if and only if $[F(\alpha) : F] < \infty$. **Reading:** Stewart Chapters 3-6 (if you have the third edition) or Chapters 1-4 (if you have the second edition). Lots of this is review and a summary of what we have done; be sure to really understand it all. I am going to draw a quiz from the exercises in Stewart early next week, probably Monday.

**Wednesday March 7.** We began the next big item on the syllabus: Fields and Galois theory. We reviewed the notion of characteristic of a field, and gave lots of examples. We defined the degree of a field extension $F \subset K$ as the dimension of $K$ as a vector space over $F$ (the degree can be finite or infinite), and gave lots of examples. A particular $\alpha \in K$ is defined it to be algebraic over $F$ if it satisfies a polynomial with coefficients in $F$. In this case, there is a unique monic polynomial over $F$ satisfied by $\alpha$, which is usually called the minimal polynomial of $\alpha$ over $F$ (although Artin calls it the “irreducible polynomial” of $\alpha$ over $F$.). The degree of the minimal polynomial is precisely the degree of $F(\alpha)$ over $F$. If $\alpha$ is not algebraic over $F$, it is said to be transcendental over $F$. **Assignment:** READ Artin Chapter 13, Sections 1,2,3. Quiz Friday similar to practice problems (but much shorter) and possibly on the reading.

**Monday March 5.** We continued working on the proof of the Jordan Canonical Form, using the worksheets. Please download and make sure you can do both worksheets distributed the week before the break. There is also a new ”practice quiz” on the website, which tests you on the applications of the structure theorem for modules over a PID. You should do the worksheets first, after that the practice quiz problems should be easier. Friday in class, we will take 10 minutes to write a very short quiz with questions of this flavor.

**Friday February 24.** We began discussing the proof of the Jordan Canonical form. The point is given an $F$- vector space $V$ with a given linear transformation $T : V \to V$, we can define on it a unique $F[t]$ module structure in which $t$ acts by $T$. *This is a difficult conceptual idea:* keep reading Artin 12.6 and reviewing your notes until it sticks. We can therefore think of the “functor”

$$\{F[t] - \text{modules}\} \to \{F - \text{vector spaces with fixed linear transformation}\}$$

sending an $F[t]$-module $M$ to the pair $(M_F, T)$ (where $M_F$ is the $F$-vector space which is the same abelian group as $M$ and whose $F$-action is just the action of the constant polynomials in $F[t]$, and where $T$ is given by multiplication by $t$) as an “equivalence of categories.” That is, to study a linear transformation $T : V \to V$ is precisely the same as studying $V$ as an $F[t]$-module. Perhaps it seems like a more complicated way to think of things, but now we can make use of the ring structure of $F[t]$ and module theory! Indeed, the proof of both Jordan Canonical form and rational canonical form comes down to the following: given a square matrix $A$ representing a linear transformation $T : V \to V$, we interpret this as an $F[t]$-module. Using the structure theorem for modules over a PID, we write $V$ as a direct sum of cyclic modules (with $d_i|d_{i+1}$ over $F[t]$). When we reinterpret each of these as a $F$-vector space, and choose a nice basis, the transformation $T$ will be in rational canonical form. For
Jordan form, we use the “prime power” version of the structure theorem, noting that the only prime (= irreducible) elements of \( \mathbb{C}[t] \) are of the form \((t - \lambda)\). This time we also choose a different basis in which to write \( T \) to get the Jordan form. Students are supposed to figure this out mainly for themselves, using the Worksheet on Jordan Form II. Please download it and complete it. **Assignment:** Finish both worksheets on Jordan form, preferably with a friend. Get Stewarts book on Galois theory! Read the early sections and prefaces, including historical introduction and/or life of Galois (depending on whether you have the second or third edition) and Chapters 1 and 2 (second edition) or Chapter 1, 2 and 3 (third edition). Finally, and most importantly **Have a good break!**

**Wednesday February 22:** Guest Lecturer! The famous Professor Stephen Debacker lectured on the \( p \)-adic numbers.

**Monday February 20.** We did a worksheet, whose purpose was to gain familiarity with Jordan form, and also (on the back) the minimal polynomial. **Assignment:** Finish worksheet. Be sure you understand with the minimal polynomial is.

**Friday February 17.** We discussed the classification of finitely generated abelian groups. Every finitely generated abelian group is a direct sum of cyclic groups, hence isomorphic to \( \mathbb{Z}^r \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_t} \) for some \( r \) and some \( n_i \). The rank \( r \) is uniquely determined but the \( n_i \) are not. However, there is a unique such presentation with \( n_i \) dividing \( n_{i+1} \) for each \( i \). There is also a unique presentation with the \( n_i \) being prime powers (up to order), as can be derived from the previous statement using the Chinese Remainder theorem. We then started talking about Jordan form. The point is that every \( n \times n \) matrix over \( \mathbb{C} \) is similar to one in Jordan form (unique up to the order of the Jordan blocks). Jordan form is a block form, where each Jordan block has some \( \lambda \) on the diagonal, 1’s above the diagonal, and zeros elsewhere. More on this soon. **Assignment:** Read Sections 1 and 2.1 of the wikipedia article on “Jordan Normal Form” and Artin 12.7.

**Wednesday February 15.** We defined generators and relations for an \( R \) module. If \( \{m_1, \ldots, m_n\} \) are generators for \( M \), then a relation on them is an \( n \)-tuple \((r_1, \ldots, r_n)\) such that \( \sum^n_{i=1} r_i m_i = 0 \). We showed that the relations form a submodule of \( R^n \), sometimes called the module of “first syzygies” of the \( m_i \). We defined \( M \) to be **finitely presented** if it admits a finite set of generators whose module of relations is also finitely generated. It is a fact (Proposition 5.17 in Artin 12.5) that every submodule of a finitely generated module over a Noetherian ring is finitely generated: in particular, every module over a Noetherian ring (in particular, over a PID) is finitely presented. We showed that a finitely presented module over any ring is isomorphic to the cokernel of some matrix, called a presenting matrix for \( M \). This is especially powerful over a PID, because by the “diagonalization theorem” proved last time, we can choose bases of the source and target so as to make the matrix diagonal—and cokernels of diagonal matrices are easy to understand! Using these ideas we proved the fundamental structure theorem for modules over a PID: Every finitely generated module over a PID is isomorphic to \( R' \oplus R/(d_1) \oplus \cdots \oplus R/(d_t) \) where \( d_i | d_{i+1} \). Furthermore, the
Monday February 13. We discussed the *first and third isomorphism theorems* for rings, which the test revealed is not yet so solid. One way to think of it is this: if $\phi : R \to S$ is a *surjective* ring homomorphism, then $\phi$ induces an isomorphism $R/\ker \phi \cong S$. Specifically, the isomorphism (call it $\overline{\phi}$) sends the class $r$ to $\phi(r)$. Identifying (renaming the elements of) $R/\ker \phi$ with $S$ (via $\overline{\phi}$, we can study all the (ring theoretic) business of $S$ as if it is the quotient ring $R/\ker \phi$ (or vice versa). For example, the ideals of $S$ “can be identified” with the ideals of $R$ containing $\ker \phi$. The map that does the identification, of course, is $\phi$, because this is the map that induces the isomorphism $\overline{\phi} : R/\ker \phi \to S$. So, when we are identifying $S$ with $R/\ker \phi$, we are also identifying $\phi$ with the canonical quotient map from $R$ to $R/\ker \phi$. Now, the third isomorphism (or correspondence) theorem gives a bijection between the ideals of $R$ containing $\ker \phi$ and the ideals of $S$. Again, the bijection sends an ideal $I \subset R$ containing $\ker \phi$ to $\phi(I)$ in $S$. In this case, the map $\phi$ also induces an isomorphism. In particular, it is immediate that $I$ is prime (respectively, maximal) if and only if $\phi(I)$ is. **Run through these ideas until they make sense!**

We then continued with the diagonalization theorem for matrices over a PID. One consequence: if $W \to V$ is a map of finitely generated free abelian groups, then there are bases for $W$ and $V$ such that the corresponding matrix is *diagonal* (with $d_i$ dividing $d_{i+1}$ if we like). We saw in examples that it is much easier to understand the kernel, image and cokernel of a diagonal matrix. This is important, because we will show that *every finitely generated module over a Noetherian ring* $R$ is the cokernel of a map between free $R$-modules. **Assignment: Read 12.5.**

Friday February 10. We proved the theorem (stated last time) on diagonalization of matrices over any Euclidean Domain. We also looked at some examples, over $\mathbb{Z}$ and over $\mathbb{F}[x]$. **Assignment: Read 12.5.**

Wednesday February 8. We took a quiz (Quiz 3), on sections 1 and 2 of Chapter 12. We then discussed “diagonalization” of matrices over a ring $R$. We recalled that, over a field, any $m \times n$ matrix can be brought into “diagonal” form by a series of elementary row and column operations: the result is an $r \times r$ identity matrix in the upper left and zeros elsewhere. By contrast, over $\mathbb{Z}$, we *can not hope* to achieve 1’s on the diagonal. For example, even the matrix $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ can not be brought to the identity matrix (over $\mathbb{Z}$) since we can not multiply by $\frac{1}{2}$. Can we maybe get every matrix over a ring at least diagonal after some elementary row and column operations? We then discussed the three different types of elementary (*invertible!*) row and column operations. Type I is “replace $R_i$ by $R_i + cR_j$” where $c$ is any element of $R$; this is invertible since it can be undone by replacing (the new) $R_i$ by $R_i - cR_j$. It can also be interpreted as left multiplication by the elementary matrix $E_{ij}(c)$, the matrix obtained from the identity matrix by putting a $c$ in
the \((ij)\)th spot; its inverse is \(E_{ij}(-c)\). Type II switches rows \(i\) and \(j\); this is left multiplication by \(E_{ij}\) obtained by switching rows \(i\) and \(j\) of the identity matrix. Type III multiplies row \(i\) by a \textsc{unit} \(\lambda\) in \(R\). It is represented by \(E_{ii}(\lambda)\) obtained from the identity by exactly that operation. These are the elementary row operations—all are invertible. The elementary column ops are defined analogously, and correspond to \textsc{right} multiplication by the corresponding elementary matrices. Note: this is very much like the case we studied in 296 for fields, but in type III, it is important to say “multiplication by some \textsc{unit}” rather than “multiplication by some \textsc{non-zero}” element.

Can we bring every matrix over a ring to diagonal form by a series of these row and column operations? The answer is \textsc{NO}, as the matrix
\[
\begin{pmatrix}
x & y \\
z & w
\end{pmatrix}
\]
over the polynomial ring \(\mathbb{C}[x, y, z, w]\) shows us. However, over \(\mathbb{Z}\) or over \(\mathbb{F}[x]\) or indeed over any \(\text{PID}\) we can diagonalize by row and column ops. \textbf{Theorem:} Let \(R\) be a \(\text{PID}\) and let \(A\) be an \(m \times n\) matrix over \(R\). Then, after a sequence of invertible row and column operations, the matrix can be brought to the form where all entries are zero except \(d_{11}, d_{22}, \ldots, d_{rr}\) and furthermore, \(d_{ii}\) divides \(d_{i+1,i+1}\) for all \(i\). We began the proof of this theorem, \textit{only in the special case where \(R\) is a \textsc{Euclidean domain}}, using induction on the dimension of the matrix and the size of the “smallest” entry of the matrix. \textbf{Assignment:} Remember Exam I is due tomorrow. Also, re-read Chapter 12 Section 4. Also, if you are not happy with your quiz, you may turn it again by \textsc{monday} instead. I will average the scores. The median was 8/10. Many misconceptions were revealed by this quiz (to me) so be sure to understand what you got wrong (or guessed).

\textbf{Monday February 6.} Some students bravely attempted to summarize the main ideas from Friday’s worksheet at the board. They did a decent job; still, we will need to work on this skill. \textbf{Be Prepared:} I’d like to get everyone up at the board at least once. We then stated the \textbf{Theorem on the Structure of finitely generated modules over a \textsc{PID}:} If \(M\) is a finitely generated module over a \(\text{PID}\), then \(M\) is isomorphic to \(R^n \oplus R/(f_1) \oplus \cdots \oplus R/(f_r)\) for some unique \(n\) and some unique (up to unit multiple) non-unit elements \(f_i\) satisfying \(f_i | f_{i+1}\). One of the main applications is the classification of finitely generated abelian groups. Joe V. pointed out that if the group is finite, the \(n\) will necessarily be zero. In particular, here is a \textsc{PhD} qualifying exam question: \textit{Classify all \textsc{abelian} groups of order 720.} Since \(720 = 2^43^25\), we need to just analyze the possible lists of integers successively dividing each other whose product is 720. These are \{720\}, \{2, 360\}, \{3, 240\}, \{4, 180\}, \{6, 120\}, \{12, 60\}, \{2, 2, 180\}, \{2, 6, 60\}, \{2, 4, 90\}, \{2, 2, 90\}. These correspond, respectively, to the ten isomorphism classes \(\mathbb{Z}_{720}, \mathbb{Z}_2 \times \mathbb{Z}_{360}, \text{etc}.\) These are all the \textsc{abelian} groups of order 720, up to isomorphism, as guaranteed by our \textbf{Theorem.} We’ll be proving this \textbf{Theorem} over the next few days. \textbf{Assignment:} Solidify your understanding of the first three sections of Chapter 12, and read the new section, 12.4. We will have a quiz to make sure you know the basic definitions and examples associated with modules. As you are working on Exam 1, be sure that you check for the most recent versions. On two occasions, erroneous versions have been replaced. \textbf{Be sure to correct these in the tex file too!}
**Friday February 3.** We discussed the fact that a module over $\mathbb{Z}$ is exactly the same thing as an abelian group. Of course, given any $\mathbb{Z}$-module, it is first and foremost an abelian group, but also conversely: given any abelian group $M$, a positive $n \in \mathbb{Z}$ always acts on $x \in M$ by $n \cdot x = x + x + \cdots + x$ ($n$ times). This is the only way to define a $\mathbb{Z}$ module structure on $M$—this is an easy consequence of the axioms of a module; you should check it! A subgroup is the same as a $\mathbb{Z}$-submodule, and a homomorphism of groups turns out to be the same as a $\mathbb{Z}$-module homomorphism. So the category of $\mathbb{Z}$-modules is equivalent to the category of abelian groups. There is no difference. We then did a **Worksheet on Free Modules.** The point was to discover that free modules are “vector-space like” in many ways: they have bases, and each element can be written uniquely as $R$-linear combination of the basis element. The finitely generated free modules have a “rank” (like dimension) and all free modules of the same rank $n$ are isomorphic to $R^n$. Also, like with vector spaces, maps between free modules are given by matrices after fixing a basis. One difference: an $n \times n$ matrix defines an isomorphism if and only if its determinant is a **unit** in $R$; being non-zero is not sufficient (unless $R$ is a field, of course, in case “unit” and “non-zero” are synonymous). **Assignment:** Complete the worksheet. Be prepared to explain it to the class. Read 12.2, 12.3. Work on Exam I. You may not work together on it; nor may you consult other texts or the internet. There is modest bonus for texing your exam.

**Wednesday February 1.** We defined an $R$-module. Informally, an $R$-module is an abelian group $(M, +)$ together with an action (called scalar multiplication) of $R$ which respects both the group structure in $M$ and the ring structure in $R$. We also defined an $R$-module homomorphism in the usual way as a map of sets which preserves all the structures. We saw that if $R$ happens to be a field, then an $R$-module is nothing more than a vector space, and an $R$-module homomorphism is nothing more than a linear mapping. We gave tons of examples. The trivial module $\{0\}$ is one stupid example. The ring $R$ itself, viewed as the abelian group $(R, +)$ is another, with scalar multiplication the usual multiplication in $R$. Every ideal $I \subset R$ is also an $R$-module in the same way: it is a submodule of the $R$-module $R$. The abelian group $R^n$ of all $n \times 1$ column matrices with entries in $R$ is an $R$-module, with the addition and scalar multiplication defined entry-wise. For any two $R$-modules $M$ and $N$, we saw that there is a naturally defined $R$-module structure called the direct sum $M \oplus N$ on the set of all pairs $(m, n)$ of elements $m \in M$ and $n \in N$; again addition and scalar multiplication are defined component-wise. In this way, we saw that the direct sum of $n$-copies of the $R$-module $R$ with itself is isomorphic to $R^n$. A more exotic example of an $R$ module is $R/I$. Here the addition is the “usual” addition of cosets in $R/I$ and the scalar multiplication is given by $r \cdot [s + I] = [rs + I]$. We defined what it means for a module $M$ to be generated by some subset $S$ of $M$, and found generators in all the examples. For an example of a non-finitely generated module, we consider the $\mathbb{Z}$-module $\mathbb{Q}$. **Assignment:** Read 12.1, 12.2 in Artin about modules, and 11.4 and 11.5 on factorization.
Monday January 30. We proved that $\mathbb{Z}[X]$ is a UFD. In a sense, this follows from the fact that larger ring $\mathbb{Q}[X]$ is a UFD (which we know because it is a Euclidean domain; anyway you proved it on the first homework set). The difficulty to be dealt with is that—because there are fewer units in $\mathbb{Z}[X]$—a polynomial $f \in \mathbb{Z}[X]$ can be irreducible viewed in $\mathbb{Q}[X]$ but not in $\mathbb{Z}[X]$; consider $2x - 4$. To deal with this, we introduced the notion of a primitive polynomial: a polynomial $f \in \mathbb{Z}[X]$ is primitive if its coefficients have no non-unit common divisors. We then showed the following Lemma: any polynomial in $\mathbb{Q}[X]$ can be written (essentially uniquely) as $cp_0$ where $c \in \mathbb{Q}$ and $p_0$ is a primitive integer polynomial, and that if $f$ happens to have integer coefficients, then the constant $c$ is an integer. Another important point is that a non-constant primitive integer polynomial is irreducible in $\mathbb{Z}[X]$ if and only if it is irreducible in $\mathbb{Q}[X]$. This follows easily from (the previous lemma and) Gauss’s Lemma: the product of primitive polynomial is primitive. From this, it was not hard to show that every polynomial in $\mathbb{Z}[X]$ factors (unique up to reordering and multiplication by $\pm 1$) as $p_1 \cdots p_r q_1(x) \cdots q_s(x)$ where $p_i$ are prime integers and the $q_i$ are primitive polynomials. This completes the proof of the unique factorization in $\mathbb{Z}[X]$. Assignment: Read 11.3.

Friday January 27. We defined Euclidean domain, which is a domain in which we can “divide with remainder” so that the remainder is strictly “smaller” than the divisor. More precisely, $R$ is a Euclidean domain if it admits a a “size function” $\sigma : R \setminus 0 \to \mathbb{Z}_{\geq 0}$ satisfying the following ”division algorithm”: for any $f \in R$ and any non-zero $d \in R$, we can write

$$f = qd + r$$

where $\sigma(d) > \sigma(r)$. The integers are of course the original Euclidean domain, studied by Euclid himself: here the size function is the usual absolute value. Polynomials over a field are a Euclidean domain, where the size is the degree. We then showed that (using the “same proof” you did in 295 for $\mathbb{Z}$ and in 512 for $\mathbb{F}[x]$) that every Euclidean domain is a PID, and hence a UFD. This is the main way mathematicians can check the UFD property, which is hard in general! We then defined the greatest common divisor of two elements in a domain, and remarked that they do not always exist! However, they do exist in any UFD: if $f$ and $g$ are non-zero elements in a UFD, factor each uniquely (up to order and unit multiple) into irreducibles; then just compare, and take the product of the factors they have in common (including multiplicities). Do this for 36 and 48 to make sure you understand. In practice, this is hard because it is difficult to factor into irreducibles, or even to tell whether or not a given element is irreducible (even in $\mathbb{Z}!$). In a PID, we showed that the gcd of $f$ and $g$ is simply the generator of the ideal $(f, g)$. Even better, in a Euclidean domain, there is the Euclidean Algorithm for finding this generator! Student then did a class worksheet in which they discovered the Euclidean algorithm. Make sure you know it! Assignment: You will be held accountable for knowing the Euclidean algorithm, including how to prove it. Also, continue reading: 11.3 is the new section.

Wednesday January 25. We proved that every principal ideal domain is a unique factorization domain, following Artin, 11.2. The points were this. First, to show that every
element in a domain has some factorization into irreducibles turns out to be the same as saying that every ascending chain of principal ideals terminates. We then used a slick argument to show that every PID has the ascending chain condition on (principal) ideals; the point of that argument was that the union of a chain of ideals is always an ideal. Second, to show that the factorization (in some domain $R$) is unique turned out to be the same as saying that every irreducible element in $R$ is prime. So it remains only to show that in a PID, every irreducible is prime; this will be on Homework set 4. Caution: The difference between “prime” and “irreducible” is subtle! Be sure you understand it. The reason it is hard is that in a UFD, prime and irreducible ARE equivalent and nearly all your intuition comes from your experience with UFDs such as $\mathbb{Z}$, $\mathbb{R}[x]$ and even more exotic rings like $\mathbb{R}[x, y, z]$ or $\mathbb{Z}[x]$. Intuition is a grand thing, but as a mathematician, you know it needs to be backed up with precise reasoning! You will play with some non UFDs in the homework, to remedy your lack of familiarity with these more exotic beasts. Quiz Friday.

Monday January 23. We discussed some common misconceptions, the most serious of which is the ridiculous notion that $\mathbb{Z}_3$ is a subring of $\mathbb{Z}_{12}$. It is not even a subset! Quotient rings are a difficult conceptual ideal; please come talk to me and others to solidify it! We then defined a Unique Factorization Domain. To do so, we needed to define the notions of a unit in a ring, a (proper) divisor of an element in a ring, an irreducible element, and associate elements. Be sure you can state all these definitions, and also prove the ideal-theoretic characterizations of them. Then, we defined a domain $R$ to be a UFD if it has the property that every non-zero non-unit element can be factored as a product of irreducible elements, unique in the following sense: if $p_1 \ldots p_m = q_1 \ldots q_n$ are two factorizations into irreducibles, then $n = m$ and after reordering, each $q_i$ is an associate of $p_i$. We have already shown that $\mathbb{Z}$ and $\mathbb{F}[x]$ are unique factorization domains. Today we showed that $\mathbb{Z}[\sqrt{-5}]$ is NOT, since $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$ are two essentially distinct factorizations into irreducibles. [To do so, we used the field norm function from Homework Set 1; be sure you can complete the details.] Assignment: Read Artin 11.1 and 11.2. Expect a quiz soon on UFD stuff. Continue reading 11.7 and 11.8.

Friday January 20. We continued discussing the field of fractions of a domain, and also considered what happens in a non-domain, when we adjoin the multiplicative inverse of a zero divisor. In particular, we studied the ring “$\mathbb{Z}_6[\frac{1}{2}]$”, by which we mean formally the quotient ring $\mathbb{Z}_6[X]/(2X - 1)$. Since $2x = 1$ in this ring, we saw that (multiplying by 3), in fact $0 = 3$, and so that $x = 2$. The map $\mathbb{Z}_6 \to \mathbb{Z}_6[\frac{1}{2}]$ is not injective, indeed, it is the “mod 3” map. To formally show that $\mathbb{Z}_6[X]/(2X - 1) \cong \mathbb{Z}_3$ we used a sequence of (first and third) isomorphism theorems: $\mathbb{Z}_6[X]/(2X - 1) \cong \mathbb{Z}[X]/(6, 2X - 1) = \mathbb{Z}[X]/(3, X - 2) \cong \mathbb{Z}_3[X]/(X - 2) \cong \mathbb{Z}_3$. Assignment: Please read Artin 10.5 and 10.6. These give a lot of insight into manipulating quotient rings which is a difficult conceptual idea. Also, over the next week, please read also 10.7 and 10.8. We will only discuss these sections briefly in class but they will be a major part of the homework this week and in the future. Read.
**Wednesday January 18.** We took a quiz on the correspondence theorem, and then went over it. If you feel you did badly, work out the correspondence theorem explicitly in an analogous case (of your choice) in \( \mathbb{F}[x] \) instead of \( \mathbb{Z} \). If you get it to me before I grade the quiz I will grade it instead. We then defined domain and discussed the cancellation property for domains. We then defined and constructed the fraction field \( F \) of any domain \( R \). This is a field whose elements are “fractions” \( \frac{a}{b} \), of elements in \( R \), which put more precisely is an equivalence class of pairs of elements \( (a, b) \) in \( R \) with \( b \neq 0 \). The equivalence relation is the one you know from grade school of course: \( \frac{a}{b} = \frac{c}{d} \) if and only if \( ad = bc \). The set of all these fractions, together with the “usual” rules for addition and multiplication, form the **field of fractions** of the domain \( R \). This is a field “containing” \( R \) in a natural way (technically, we mean there is an injective ring homomorphism \( R \to F \), of course, the one sending \( r \to \frac{r}{1} \) and it is has the property that it must be “contained in” any field “containing” \( R \). **Assignment:** Read Artin 10.6. Think about things that go wrong when we “adjoin multiplicative inverses” in non-domains. Be prepared to have at least one thing that goes wrong to report in class.

**Friday January 13.** Nick and Alex explained the main concepts from the worksheet. We then discussed the intuition of quotient rings, including more examples of the first isomorphism theorem, and the idea of “adjoining an element” to any ring. The quotient ring

\[
\mathbb{Z}[X]/(X^2 - 2)
\]

can be thought of as “like” the polynomial ring \( \mathbb{Z}[x] \) but in which \( X^2 \) is identified with 2. This means that \( X \) is essentially \( \sqrt{2} \) (or \( -\sqrt{2} \); there is no canonical way to do this.) Formally, we can use the first isomorphism theorem to see that \( \mathbb{Z}[X]/(X^2 - 2) \cong \mathbb{Z}[\sqrt{2}] \). Here \( \mathbb{Z}[\sqrt{2}] \) is the subring of \( \mathbb{C} \) generated by \( \sqrt{2} \)—that is, the smallest subring of \( \mathbb{C} \) containing \( \sqrt{2} \), which is the subring of \( \mathbb{C} \) consisting of elements of the form \( a + b\sqrt{2} \) where \( a, b \) are integers. Interestingly, this allows us to “abstractly adjoin” elements to any ring: for example, in the field \( \mathbb{Z}_3 \), the element 2 has no square root. But we can construct the ring \( \mathbb{Z}_3[X]/(X^2 - 2) \), which is a ring containing \( \mathbb{Z}_3 \) and also the class of \( X \), which has the property that its square is 2. So, we might choose to write the class of \( X \) as \( \sqrt{2} \), keeping in mind that the meaning of the symbol \( \sqrt{2} \) is **not** the one from high school: this is not a real number!\(^3\) By abstractly adjoining the roots of every polynomial to a field, we will later use this idea to construct an “algebraic closure” of any field!

We also discussed the “substitution principle,” which in one special case at least says that to give a ring homomorphism \( \mathbb{Z}[X] \to R \) where \( R \) is any ring, is the same as specifying any one element \( r \) in \( R \) to be the image of \( X \). Since ring homomorphisms preserve multiplication and addition, if we know \( X \) maps to \( r \), then we also know \( X^2 \) maps to \( r^2 \), \( X + X^2 \) maps to \( r + r^2 \) and indeed any polynomial \( g(X) \) must be sent to \( g(r) \). There are no restrictions whatsoever on \( r \): all choices of \( r \) give a valid ring homomorphism. However, it is much harder if we want to define a ring homomorphism from a quotient ring \( \phi : \mathbb{Z}[X]/I \to R \). Of course, the image of (the class of) \( X \) still determines the image of every polynomial (class), but the map sending \( x \) to \( r \) is well-defined if and only if \( g(r) = 0 \) for all \( g \in I \). For example,

\(^3\)For that matter, the symbol 2 is not as in high school either in this example.
there are only two possible choices of ring maps \( \mathbb{Z}[X]/(X^2 - 2) \to \mathbb{C} \). The class of \( X \) must be sent to a complex number satisfying \( X^2 - 2 = 0 \), which is to say, \( X \) can be sent to \( \sqrt{2} \) or \( -\sqrt{2} \). No other choice can give a well-defined ring map. **Assignment:** Read Artin 4.4 and 4.5 on quotients and adjoining elements. There will be a quiz Wednesday on the reading.

**Wednesday January 11.** We discussed the following example: if \( X \) is a topological space, and \( Y \subset X \) is a subspace, then there is a natural ring homomorphism \( C^0(X) \to C^0(Y) \) given by restricting a (real-valued) continuous function on \( X \) to \( Y \). The kernel is the ideal \( I \) of all continuous functions on \( X \) that vanish on \( Y \). If this map is surjective (which depends on the specifics of \( Y \) and \( X \)), the first isomorphism theorem for rings tells us that \( C^0(X)/I \cong C^0(Y) \). For example, if \( Y \) is a closed interval in \( \mathbb{R} \), then \( C^0(\mathbb{R})/I \cong C^0([a, b]) \).

**Question:** is it always surjective for \( Y \) closed in \( X \)?) If \( Y \) is an open interval in \( \mathbb{R} \), the restriction map is never surjective. We then did a class worksheet to familiarize you with thinking about quotient rings. We studied specific examples of quotients of a polynomial ring in one variable over a field. **Assignment:** Finish the worksheet. Be prepared to explain the results to the class. Also, read Artin 10.5. There could be a quiz anytime.

**Monday January 9.** We discussed quotient rings. For any ideal \( I \) in a ring \( R \), we already know that the set of (additive) cosets \( R/I \) has the structure of an abelian group under the naturally induced addition on cosets. (This is because \( I \subset R \) is a normal subgroup of the underlying additive group of \( R \); we just take the natural quotient group structure as in Math 512.) So the question is: can we put a natural multiplication on \( R/I \) so that \( R/I \) becomes a ring? The answer is YES: we defined \([r + I][s + I] \) to be \([rs + I] \), and then carefully checked that this is well-defined. (Check it carefully yourself: if \( R \) is non-commutative, then the ideal \( I \) must be a two-sided ideal in order to make the multiplication well-defined!) It was then easy to verify that the natural map \( R \to R/I \) sending each \( r \in R \) to its coset \( r + I \) is a surjective ring homomorphism whose kernel is \( I \). Similarly, there is a first isomorphism theorem for rings: if \( \phi : R \to S \) is a surjective homomorphism of rings, then there is an induced isomorphism \( \overline{\phi} : R/(\ker \phi) \to S \). Of course, we already know that there is an isomorphism of the underlying groups; the only new point is that the isomorphism also respects the multiplication. As an example, we used this theorem to show that \( \mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C} \). **Assignment:** Read 10.4.

**Friday January 6.** We took an exceptionally silly 5-minute quiz just to make sure folks are reading. We then defined the following concepts from the reading: kernel, ideal, generators for an ideal, principal ideal. We gave a few more examples of ideals and homomorphisms. We proved that in both \( \mathbb{Z} \) and in \( F[X] \), where \( F \) is a field, every ideal is principal, i.e. generated by one element. The proofs in these two cases are essentially the same: the point is the division algorithm. **Make sure you can reproduce this proof in either ring!** Reading: Artin, 10.4.
**Wednesday January 4.** We defined rings and ring homomorphisms and gave lots of examples. Read Artin Chapter 10, first 3 sections. The first two are essentially review. Expect a quiz friday on the reading.