# Math 5111 (Algebra 1)

## Lecture #5 $\sim$ September 24, 2020

---

Properties of Subfields and Simple Extensions

- Properties of Subfields
- Simple Extensions

This material represents §2.2.2-2.2.3 from the course notes.

# Subfields and Field Extensions, I

As with other algebraic structures like vector spaces and rings, a natural first step in studying the structure of fields is to study subfields.

**Definition**

*If $F$ is a field, we say a subset $S$ of $F$ is a subfield if $S$ is itself a field under the same operations as $F$. If $F$ is a subfield of the field $K$, we say that $K$ is an extension field of $F$.*

Notation: We often write $K/F$ ("$K$ over $F$") to symbolize that $K$ is an extension field of $F$. (It is not the quotient of $K$ by $F$! That does not make sense in the land of rings, since $F$ is not an ideal of $K$.)

# Subfields and Field Extensions, II

Examples:

1. $\mathbb{Q}$ is a subfield of $\mathbb{R}$, which is a subfield of $\mathbb{C}$.
2. For any squarefree integer $D \neq 1$, $\mathbb{Q}(\sqrt{D})$ is a subfield of $\mathbb{C}$.
3. For any squarefree integer $D \neq 1$, $\mathbb{Q}(\sqrt{D})$ is an extension field of $\mathbb{Q}$.
4. $\mathbb{F}_2$ is a subfield of $\mathbb{F}_2[x]/(x^2 + x + 1)$, where we think of $\mathbb{F}_2$ as the constant polynomials. (Note $\mathbb{F}_2[x]/(x^2 + x + 1)$ is a field because $x^2 + x + 1$ is irreducible.)
5. If $p$ is an irreducible polynomial, $F[x]/p$ is an extension field of $F$. (This one is extremely important: in fact, it's the entire reason we discussed polynomials!)

# Subfields and Field Extensions, III

We can also exploit the structure of vector spaces to study the structure of fields. A fundamental observation is that if $K$ is an extension field of $F$, then $K$ is an $F$-vector space (under the addition and multiplication of $K$).

**Definition**

*If $K$ is an extension field of $F$, the degree $[K : F]$ (also called the relative degree or very occasionally the "index") is the dimension $\dim_F(K)$ of $K$ as an $F$-vector space. The extension $K/F$ is finite if it has finite degree; otherwise, the extension is infinite.*

In fact, defining the degree of a field extension was the entire reason we discussed vector spaces today.

# Subfields and Field Extensions, IV

Examples:

1. We have $[\mathbb{C} : \mathbb{R}] = 2$ since $\mathbb{C}/\mathbb{R}$ has a basis $\{1, i\}$.
2. We have $[\mathbb{Q}(\sqrt{D}) : \mathbb{Q}] = 2$, since $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ has a basis of 2 elements.
3. We have $[\mathbb{R} : \mathbb{Q}] = \infty$, since $\dim_{\mathbb{Q}}(\mathbb{R}) = \infty$.

The first two are finite extensions, while the third is infinite.

We will compute very many more extension degrees later.

# Subfields and Field Extensions, V

Like with subrings, it is not necessary to verify most of the field axioms to show that a subset is actually a subfield:

**Proposition (Subfield Criterion)**

*A subset $S$ of a field $F$ is a subfield if and only if $S$ contains 0 and 1, and is closed under subtraction and division. In other words, for any $a, b, c \in S$ with $c \neq 0$, we have $a - b \in S$ and $a \cdot c^{-1} \in S$.*

Equivalently, $S$ is a subfield if and only if it is a subring that contains 1 and is closed under multiplicative inverses.

The proof (in the notes, if you want to read the details) is just bookkeeping to verify that all of the field axioms hold.

# Subfields and Field Extensions, VI

Examples:

1. The set $S = \{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$ is not a subfield of $\mathbb{R}$, where $\sqrt[3]{2}$ denotes the real cube root of 2.

- This set is not closed under multiplication (so it is not even a subring): the element $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$ is not in the set, because we cannot write $\sqrt[3]{4} = a + b\sqrt[3]{2}$ for any rational numbers $a$ and $b$. This fact may seem obvious, but it is not so easy to prove directly!
- Here is one argument: if $\sqrt[3]{4} = a + b\sqrt[3]{2}$ then multiplying by $\sqrt[3]{2}$ yields $2 = a\sqrt[3]{2} + b\sqrt[3]{4}$ and plugging in for $\sqrt[3]{4}$ then yields $2 = a\sqrt[3]{2} + b(a + b\sqrt[3]{2}) = ab + (a + b^2)\sqrt[3]{2}$. Since $\sqrt[3]{2}$ is irrational and $a, b$ are rational, the coefficient of $\sqrt[3]{2}$ must be 0 so that $a = -b^2$. But this does not work since it yields $-a^3 = 2$, which is impossible if $a$ is rational.

# Subfields and Field Extensions, VII

Examples:

2. The set $S = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$, denoted $\mathbb{Q}[\sqrt[3]{2}]$.

We use square brackets, like with the polynomial ring $F[x]$, because $\mathbb{Q}[\sqrt[3]{2}]$ is the collection of polynomials in $\sqrt[3]{2}$.

- It is a straightforward calculation to see that $S$ is closed under addition, additive inverses, and multiplication (so it is a subring). It is less clear why every nonzero element in $S$ possesses a multiplicative inverse.
- In fact, one may verify that $\dfrac{1}{a + b\sqrt[3]{2} + c\sqrt[3]{4}} = \dfrac{(a^2 - 2bc) + (2c^2 - ab)\sqrt[3]{2} + (b^2 - ac)\sqrt[3]{4}}{a^3 + 2b^3 + 4c^3 - 6abc}$, and that the denominator is never zero for $a, b, c \in \mathbb{Q}$ except when $a = b = c = 0$.

# Subfields and Field Extensions, VIII

Examples:

2. The set $S = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$, denoted $\mathbb{Q}[\sqrt[3]{2}]$.

- Explicitly: since every term in the denominator $a^3 + 2b^3 + 4c^3 - 6abc$ has degree 3, by multiplying through by a common denominator we may assume that $a, b, c$ are relatively prime integers. Then $a$ must be even since the other terms all have even coefficients; cancelling the common factor of 2 then shows $b$ must be even, and then cancelling again shows $c$ must be even: contradiction.
- Using a similar calculation, we can show that the set $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ is $\mathbb{Q}$-linearly independent and is therefore a basis for $\mathbb{Q}[\sqrt[3]{2}]$. Thus, we see that $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$.

# Subfields and Field Extensions, IX

Examples:

3. The set $S = \{a + b\sqrt{2} + c\sqrt{3} : a, b, c \in \mathbb{Q}\}$ is not a field.

- This set is not closed under multiplication, since $\sqrt{6} = \sqrt{2} \cdot \sqrt{3}$ is not in $S$. Like in the other examples, this is not so easy to prove directly.
- Here is one argument: if $\sqrt{6} = a + b\sqrt{2} + c\sqrt{3}$ then rearranging yields $\sqrt{6} - c\sqrt{3} = a + b\sqrt{2}$. Squaring both sides yields $(6 + 3c^2) - 6c\sqrt{2} = (a^2 + 2b^2) + 2ab\sqrt{2}$. Since $\sqrt{2}$ is irrational this requires $2ab = -6c$ and $6 + 3c^2 = a^2 + 2b^2$. Solving the first equation for $c$ yields $c = -ab/3$, and then plugging into the second equation yields $18 + a^2b^2 = 3a^2 + 6b^2$. But this can be rearranged and factored as $(a^2 - 6)(b^2 - 3) = 0$, which has no rational solutions for $a, b$.

# Subfields and Field Extensions, X

Examples:

3. The set $S = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$ forms a field, denoted $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.
   - As with $\mathbb{Q}[\sqrt[3]{2}]$, it is easy to see that $S$ is a subring: the hard part is the existence of multiplicative inverses.
   - One can "rationalize denominators" repeatedly to compute multiplicative inverses in $S$: explicitly, the multiplicative inverse of $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ can be computed to be

$$\frac{(a^3-2ab^2-3ac^2+6bcd-6ad^2)+(-2a^2b+2b^3-3bc^2+6acd-6bd^2)\sqrt{2}+(-a^2c-2b^2c+3c^3+4abd-6cd^2)\sqrt{3}+(2abc-a^2d+2}{a^4-4a^2b^2-6a^2c^2-12a^2d^2+48abcd+4b^4-12b^2c^2-24b^2d^2+9c^4-36c^2d^2+36d^4}$$

     and one can similarly show that the denominator is never zero unless $a = b = c = d = 0$.
   - Using a similar calculation, we can show that the set $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is $\mathbb{Q}$-linearly independent and is therefore a basis for $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Thus, we see that $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}] = 4$.

# Subfields and Field Extensions, XI

Okay, so.... those last few examples really were awful.

- Even though it may seem fairly obvious that those sets really ought to be fields once we closed them under multiplication, actually establishing the existence of multiplicative inverses was deliriously unpleasant.
- It also seems very unlikely that we would be able to extend these computations to examples that are even a little bit more complicated than those ones.
- What we will do now is develop other ("better") techniques for studying subfields and field extensions that are less reliant on explicit calculations.

# Properties of Subfields, I

As an immediate corollary of the subfield criterion, we see that the intersection of subfields is also a subfield:

**Proposition (Intersection of Subfields)**

*If $F$ is a field, then the intersection of any nonempty collection of subfields of $F$ is also a subfield of $F$.*

Proof:

- Let $S = \bigcap_{i \in I} F_i$ where the $F_i$ are subfields of $F$. Then by the subfield criterion, $0, 1 \in F_i$ for all $i \in I$, so $S$ contains 0 and 1.
- Furthermore, for any $a, b, c \in S$ with $c \neq 0$, we have $a, b, c \in F_i$ for all $i$. Thus, $a - b \in F_i$ and $a \cdot c^{-1} \in F_i$ for all $i$ by the subfield criterion, and therefore $a - b \in S$ and $a \cdot c^{-1} \in S$, so $S$ is a subfield.

# Properties of Subfields, II

Like with vector spaces and span, if we have a subset $S$ of a field, we would like to understand the structure of the subfield of $F$ "generated by" the elements of $S$.

- If $F$ is a field and $S$ is a subset of $F$, a natural choice is to define "the subfield generated by $S$" to be the smallest subfield of $F$ containing $S$.
- *A priori*, it is not obvious that there is such a smallest subfield. However, since the intersection of any nonempty collection of subfields is also a subfield, per the above proposition, and since $S$ is always contained in at least one subfield (namely $F$ itself), we can equivalently define the subfield $E \subseteq F$ generated by $S$ to be the intersection of all subfields containing $S$.

# Properties of Subfields, III

**Definition**

*If $F$ is a field and $S$ is a subset of $F$, we define the subfield of $F$ generated by $S$ to be the intersection of all subfields of $F$ containing $S$.*

- Although this definition is clearly well-posed, we have not really described what the elements in this subfield $E$ actually are.
- If $x_1, x_2, \ldots, x_n \in S$, then since $E$ is closed under addition and multiplication and contains 1, we see that any polynomial with integer coefficients in $x_1, x_2, \ldots, x_n$ must be in $S$ as well. And since $E$ is closed under division, it must in fact contain any "rational function" (i.e., quotient of one polynomial by another) of $x_1, x_2, \ldots, x_n$.

# Properties of Subfields, IV

**Definition**

*If $F$ is a field and $S$ is a subset of $F$, we define the subfield of $F$ generated by $S$ to be the intersection of all subfields of $F$ containing $S$.*

- On the other hand, one can verify that the collection of all rational functions in elements of $S$ with coefficients from $F$ actually is a field.
- This follows by the simple observation that the sum, product, additive inverse, and multiplicative inverse of nonzero rational functions are also rational functions.
- Therefore, this collection of rational functions is the desired field.

# Properties of Subfields, V

We will frequently be interested in extensions of subfields.

**Definition**

*If $F$ is a field, $S$ is a subset of $F$, and $E$ is a subfield of $F$, we define $E(S)$, the extension of $E$ by the set $S$, to be the smallest subfield containing $E$ and $S$.*

Example:

- The field $\mathbb{Q}(\sqrt{2})$, inside $\mathbb{C}$, is the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and $\sqrt{2}$.
- This field must necessarily contain all elements of the form $a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$. But as we saw last class, the set $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is itself a field, so it is exactly $\mathbb{Q}(\sqrt{2})$.

# Properties of Subfields, VI

Another useful case is the subfield generated by 1:

**Definition**

*If $F$ is a field, the prime subfield of $F$ is the subfield generated by 1. (It is sometimes written $F'$.)*

- Any subfield of $F$ contains 1, so the subfield generated by 1 will be the "smallest" subfield of $F$, and will be contained in every other subfield of $F$.
- The structure of the prime subfield will depend on the characteristic of $F$:

**Proposition (Prime Subfield)**

*If $F$ has characteristic $p > 0$, then the prime subfield of $F$ is (isomorphic to) $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and if $F$ has characteristic 0, then the prime subfield of $F$ is (isomorphic to) $\mathbb{Q}$.*

# Properties of Subfields, VII

Proof:

- Let $E$ be the prime subfield of $F$.
- If $F$ has characteristic $p > 0$, consider the map $\varphi : \mathbb{Z} \to E$ defined by $\varphi(\overline{a}) = a1_F$.
- It is easy to see that $\varphi(a + b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ and that $\varphi$ is surjective.
- Furthermore, by the assumption on the characteristic (since $p1_F = 0$ in a field of characteristic $p$), we see that $\ker(\varphi) = p\mathbb{Z}$.
- Therefore, by the first isomorphism theorem, we obtain an isomorphism of $\mathbb{Z}/\ker(\varphi)$ with $\mathrm{im}(\varphi) = E$.
- Thus, $E$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, as claimed.

# Properties of Subfields, VIII

Proof (continued):

- If $F$ has characteristic 0, then instead consider the map $\varphi : \mathbb{Q} \to E$ defined by $\varphi(a/b) = (a1_F) \cdot (b1_F)^{-1}$.
- This map is well-defined by the assumption that $b1_F \neq 0_F$ whenever $b \neq 0$.
- As before, it is straightforward to see that $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$.
- Likewise, $\varphi$ has an inverse map defined by $\varphi^{-1}[(a1_F) \cdot (b1_F)^{-1}] = a/b$.
- Thus, $\varphi$ is a ring isomorphism and so $E$ is isomorphic to $\mathbb{Q}$, again as claimed.

# Properties of Subfields, IX

As we noted above, every subfield of $F$ contains the prime subfield of $F$, which is to say, every subfield of $F$ is an extension field of the prime subfield.

- We can therefore always denote the subfield of $F$ generated by $S$ as $E(S)$, where $E$ is the prime subfield of $F$.
- The round parentheses are intended to indicate that we are closing under field operations, in contrast to square brackets where we only close under ring operations.

# Properties of Subfields, X

For example, compare the following two things:

1. The set of rational functions in $\sqrt[3]{2}$ with rational coefficients is denoted $\mathbb{Q}(\sqrt[3]{2})$. This is the subfield of $\mathbb{R}$ generated by $\sqrt[3]{2}$.
2. The set of polynomials in $\sqrt[3]{2}$ with rational coefficients is denoted $\mathbb{Q}[\sqrt[3]{2}]$.

- As it happens, these two sets turn out to be the same, because $\mathbb{Q}[\sqrt[3]{2}]$ is actually a field, but as we discussed, this is not a trivial statement to establish (at least, not the way we did it!).
- Furthermore, as we will see, there exist real numbers $\alpha$ with the property that $\mathbb{Q}(\alpha) \neq \mathbb{Q}[\alpha]$: for example, this situation arises when $\alpha$ is the transcendental number $\pi$.

# Simple Extensions, I

In fact, let's revisit the example of the field $F = \mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \,:\, a, b, c \in \mathbb{Q}\}$ to examine the structure a bit more closely:

- For shorthand, write $\overline{x} = \sqrt[3]{2}$: then every element of $F$ has the form $a + b\overline{x} + c\overline{x}^2$.
- Addition is performed in the obvious way: $(a+b\overline{x}+c\overline{x}^2)+(d+e\overline{x}+f\overline{x}^2) = (a+d)+(b+e)\overline{x}+(c+f)\overline{x}^2$.
- For multiplication, we can use the distributive law to compute $(a + b\overline{x} + c\overline{x}^2) \cdot (d + e\overline{x} + f\overline{x}^2) =$ $ad + (ae + bd)\overline{x} + (af + be + cd)\overline{x}^2 + (bf + ce)\overline{x}^3 + cf\overline{x}^4$.
- Since $\overline{x}^3 = (\sqrt[3]{2})^3 = 2$, we see $(a + b\overline{x} + c\overline{x}^2) \cdot (d + e\overline{x} + f\overline{x}^2) =$ $(ad + 2bf + 2ce) + (ae + bd + 2cf)\overline{x} + (af + be + cd)\overline{x}^2$.

So now here's the question: does this look at all familiar?

# Simple Extensions, II

In fact (with the sort-of-cheating replacement of $\sqrt[3]{2}$ by $x$), we can see that the arithmetic has exactly the same description as the arithmetic in the polynomial quotient ring $\mathbb{Q}[x]/(x^3 - 2)$.

- This situation of "these rings look exactly the same" is merely reflecting the fact that the map $\varphi : \mathbb{Q}[x]/(x^3 - 2) \to \mathbb{Q}[\sqrt[3]{2}]$ sending $\overline{x} \mapsto \sqrt[3]{2}$ is a ring homomorphism.
- You can ponder how to use the first isomorphism theorem to construct this map $\varphi$, rather than having to do it directly.
- Furthermore, since $\varphi$ is clearly a bijection, the rings $\mathbb{Q}[\sqrt[3]{2}]$ and $\mathbb{Q}[x]/(x^3 - 2)$ are isomorphic.
- Finally, because the polynomial $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ (either because it has degree 3 and no rational roots, or by Eisenstein with $p = 2$), we know that $\mathbb{Q}[x]/(x^3 - 2)$ is a field.
- Therefore, $\mathbb{Q}[\sqrt[3]{2}]$ is a field as well, since it is ring-isomorphic to a field.

# Simple Extensions, III

We can generalize the analysis in the example to the class of field extensions generated by a single element:

**Definition**

*If $K/F$ is a field extension, we say that $K$ is a simple extension if $K = F(\alpha)$ for some $\alpha \in K$: in other words, if $K$ is generated over $F$ by the single element $\alpha$.*

Examples:

- $\mathbb{C}$ is a simple extension of $\mathbb{R}$, generated by the element $i$. (In fact, $\mathbb{C}$ is generated over $\mathbb{R}$ by any non-real complex number.)
- $\mathbb{Q}(\sqrt{2})$ is a simple extension of $\mathbb{Q}$, generated by $\sqrt{2}$.
- The rational function field $F(x)$ is a simple extension of $F$, generated by the element $x$.

# Simple Extensions, IV

It is not always obvious whether a given extension has a single generator.

- Even if we construct the extension using several different generators, it is possible that some combination of them might generate the extension by itself.
- Later, we will be able to characterize simple extensions, and it turns out that many (perhaps "most") extensions are simple.

# Simple Extensions, V

Example: Show that the field $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is a simple extension of $\mathbb{Q}$ generated by the element $\alpha = \sqrt{2} + \sqrt{3}$.

# Simple Extensions, V

Example: Show that the field $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is a simple extension of $\mathbb{Q}$ generated by the element $\alpha = \sqrt{2} + \sqrt{3}$.

- We can see that $\alpha^2 = 5 + 2\sqrt{6}$ and $\alpha^3 = 11\sqrt{2} + 9\sqrt{3}$.
- It is then easy to see that we can write $\sqrt{6} = \frac{1}{2}(\alpha^2 - 5)$, $\sqrt{2} = \frac{1}{2}(\alpha^3 - 9\alpha)$, and $\sqrt{3} = \frac{1}{2}(11\alpha - \alpha^3)$.
- This means every element in the field is a rational function (in fact, a polynomial) with rational coefficients in $\alpha$, meaning that $\alpha$ is a generator for the field.

# Simple Extensions, VI

The structure of the simple extension $K = F(\alpha)$ will depend on the nature of the element $\alpha$: specifically, on whether $\alpha$ is the root of some polynomial with coefficients in $F$.

**Definition**

*If $K/F$ is a field extension, we say that the element $\alpha \in K$ is algebraic over $F$ if $\alpha$ is the root of some nonzero polynomial $p \in F[x]$. Otherwise, if $\alpha$ is not a root of any nonzero polynomial in $F[x]$, we say $\alpha$ is transcendental over $F$.*

# Simple Extensions, VII

Examples:

1. The elements $\sqrt{2}$, $\sqrt[3]{2}$, $i$, and $2 - 3i$ of $\mathbb{C}$ are algebraic over $\mathbb{Q}$, since they are roots of the polynomials $x^2 - 2$, $x^6 - 4$, $x^4 - 1$, and $(x - 2)^2 + 9$ respectively.
2. The elements $e$ and $\pi$ of $\mathbb{R}$ are transcendental over $\mathbb{Q}$ (neither of these facts is easy to prove, and we will not prove them!).
3. The element $t$ in the field of rational functions $F(t)$ is transcendental over $F$, since it does not satisfy any polynomial with coefficients in $F$. (This fact is implicit in the definition of the polynomial ring $F[t]$.)
4. If $p$ is any irreducible polynomial over $F$, then the element $\overline{x}$ in the polynomial quotient ring $K = F[x]/p$ is algebraic over $F$, because $p(\overline{x}) = 0$ in $K$.

# Minimal Polynomials, I

By definition, an algebraic element over $F$ is by definition a root of some nonzero polynomial in $F[x]$.

- Indeed, it may be a root of many different polynomials: for example, $\sqrt{2}$ is a root of $x^2 - 2$, $x^3 + x^2 - 2x - 2$, and $x^4 - 4$.

However, all of these polynomials are multiples of an essentially unique monic polynomial:

**Proposition (Minimal Polynomials)**

*If $K/F$ is a field extension and $\alpha \in K$ is algebraic over $F$ and nonzero, then there exists a unique monic irreducible polynomial $m \in F[x]$ such that $m(\alpha) = 0$. This polynomial is called the minimal polynomial of $\alpha$ over $F$, and is the monic polynomial of smallest positive degree having $\alpha$ as a root; furthermore, any other polynomial having $\alpha$ as a root is divisible by $m$.*

# Minimal Polynomials, II

Proof:

- If $\alpha$ is algebraic, consider the set of all nonzero polynomials in $F[x]$ having $\alpha$ as a root.
- By hypothesis, $S$ is nonempty, so by the well-ordering axiom, $S$ contains a polynomial of minimal positive degree.
- It is easy to see that if $m(\alpha) = 0$, then any $F$-multiple of $m$ also has $\alpha$ as a root, so we may divide $m$ by its leading coefficient to make $m$ monic.
- We claim that $m$ is irreducible: if $m$ had a factorization $m = pq$ with $0 < \deg p, \deg q < \deg m$, then by evaluating both sides at $\alpha$ we would see $0 = m(\alpha) = p(\alpha)q(\alpha)$.
- Since $K$ is a field, this implies $p(\alpha) = 0$ or $q(\alpha) = 0$ so that one of $p, q$ has $\alpha$ as a root and is therefore in $S$.
- But this is a contradiction, since $m$ was assumed to be an element of minimal degree in $S$: thus, $m$ is irreducible.

# Minimal Polynomials, III

Proof (continued):

- For the divisibility property, suppose that $b$ is a polynomial with $\alpha$ as a root.
- Then applying the division algorithm to $b$ and $m$ shows that $b = qm + r$ for some $q, r$ with $\deg r < \deg m$.
- Evaluating both sides at $\alpha$ and rearranging then yields $r(\alpha) = b(\alpha) - q(\alpha)m(\alpha) = 0$, so since $\deg r < \deg m$ we must have $r = 0$ by the minimality of $m$. Thus, $m|b$ as claimed.
- For the uniqueness of $m$, if there were another such polynomial $m'$, then by the above we would have $m'|m$ and $m|m'$ so that $m$ and $m'$ are associates. But since both $m$ and $m'$ are monic, they are equal.

# Minimal Polynomials, IV

Examples:

1. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$: it has $\sqrt{2}$ as a root and is irreducible.
2. The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$: it has $\sqrt[3]{2}$ as a root and is irreducible.
3. The minimal polynomial of $2 + i$ over $\mathbb{R}$ is $(x-2)^2 + 1$: it has $2 + i$ as a root and is irreducible.

We will compute many more examples as we continue with our discussion.

# Simple Extensions, VIII

The nature of the simple extension $F(\alpha)$ will depend on whether $\alpha$ is algebraic or transcendental over $F$:

**Theorem (Simple Extensions)**

*Suppose $K/F$ is a simple extension with $K = F(\alpha)$. If $\alpha$ is algebraic over $F$ with minimal polynomial $m(x)$ then $K$ is isomorphic to the field $F[x]/m(x)$, while if $\alpha$ is transcendental over $F$ then $K$ is isomorphic to the field $F(t)$ of rational functions in $t$.*

The idea of the proof is simply to show that the map associating $\overline{x}$ (or $t$, as appropriate) with $\alpha$ is a well-defined ring isomorphism.

# Simple Extensions, IX

Proof:

- First suppose $\alpha$ is algebraic over $F$ with minimal polynomial $m(x)$. Consider the map $\psi : F[x] \to K$ mapping $p(x)$ to $p(\alpha)$.
- Then $\psi(p+q) = (p+q)(\alpha) = p(\alpha) + q(\alpha) = \psi(p) + \psi(q)$; similarly $\psi(pq) = \psi(p)\psi(q)$, so $\psi$ is a ring homomorphism.
- Furthermore, $\ker(\psi)$ is the set of polynomials having $\alpha$ as a root, which is simply the ideal $(m)$ of multiples of $m$, by our discussion of the minimal polynomial.
- Therefore, by the first isomorphism theorem, we obtain an isomorphism $\varphi : F[x]/\ker(\psi) \cong \mathrm{im}(\psi)$.
- But $F[x]/m(x)$ is a field since $m$ is irreducible, so the image of $\varphi$ is a subfield of $K$ containing $\alpha$ and $F$.
- Therefore, by definition of $F(\alpha)$, this means it must actually be $F(\alpha) = K$, and thus $K = F(\alpha)$ is isomorphic to $F[x]/(m(x))$ as claimed.

# Simple Extensions, X

Proof (continued):

- If $\alpha$ is transcendental over $F$, the argument is similar, except we instead use the map $\varphi : F(t) \to K$ sending $\dfrac{p(t)}{q(t)}$ to $\dfrac{p(\alpha)}{q(\alpha)}$.
- This map is well defined because $q(\alpha) \neq 0$ whenever $q$ is not the zero polynomial by the assumption that $\alpha$ is transcendental.
- It is easy to see that $\varphi$ respects addition and multiplication, and is injective (the latter because $\alpha$ is transcendental).
- Surjectivity follows by a similar argument as before: $F(t)$ is isomorphic as a ring to the image of $\varphi$, and since $F(t)$ is a field, we conclude that the image of $\varphi$ is a subfield of $K$ containing $\alpha$ and $F$, hence is equal to $K = F(\alpha)$.

# Simple Extensions, XI

Using the description of simple extensions we can easily compute the extension degree, and characterize when $F(\alpha) = F[\alpha]$:

**Corollary (Simple Extension Degrees)**

*Suppose $K/F$ is a simple extension with $K = F(\alpha)$. If $\alpha$ is algebraic over $F$ with minimal polynomial $m(x)$ then $[F(\alpha) : F] = \deg m$, and $F(\alpha)$ is spanned (as an $F$-vector space) by $\{1, \alpha, \alpha^2, \ldots, \alpha^{\deg m - 1}\}$, while if $\alpha$ is transcendental over $F$ then $[F(\alpha) : F] = \infty$. Furthermore, $F(\alpha) = F[\alpha]$ if and only if $\alpha$ is algebraic over $F$.*

# Simple Extensions, XII

Proof:

- First suppose $\alpha$ is algebraic over $F$ with minimal polynomial $m(x)$, where $\deg m = n$.
- As we just showed, $K$ is isomorphic to $F[x]/m(x)$.
- From our discussion of residue classes in $F[x]/m(x)$, we know (via an application of the division algorithm) that every residue class can be written uniquely in the form $b_0 + b_1\overline{x} + \cdots + b_{n-1}\overline{x}^{n-1}$ for unique elements $b_i \in F$.
- Equivalently, this says that the set $\{1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{n-1}\}$ is an $F$-basis for $F[x]/m(x)$.
- Applying the isomorphism between $K$ and $F[x]/m(x)$ shows that the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is an $F$-basis for $F(\alpha)$.
- Therefore, we have $[F(\alpha) : F] = n$.
- Furthermore, we see immediately that $F(\alpha) = F[\alpha]$ here.

# Simple Extensions, XIII

Proof (continued):

- Now suppose $\alpha$ is transcendental over $F$.
- Then the set $\{1, \alpha, \alpha^2, \dots\}$ is linearly independent over $F$, as any nontrivial linear dependence $c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$ would imply that $\alpha$ is the root of some nonzero polynomial in $F[x]$, but this cannot occur because $\alpha$ is transcendental.
- Since $K$ contains an infinite $F$-linearly independent set we see $[K : F] = \infty$.
- Furthermore, $F(\alpha)$ contains elements that are not polynomials in $\alpha$ (namely, any rational function that is not a polynomial).
- For a specific example, we cannot have $\alpha^{-1} = p(\alpha)$ since this would imply $1 - \alpha p(\alpha) = 0$ so that $\alpha$ would be a root of a nonzero polynomial, impossible.
- Therefore, $\alpha^{-1} \in F(\alpha)$ is not in $F[\alpha]$, so $F(\alpha) \neq F[\alpha]$ here.

# Simple Extensions, IX

These results allow us to do calculations in simple extensions very pleasantly: all we need to do is find the minimal polynomial of the generator.

Example: Show that the field $\mathbb{Q}(\sqrt[8]{2})$ has degree 8 over $\mathbb{Q}$ and find a basis.

# Simple Extensions, IX

These results allow us to do calculations in simple extensions very pleasantly: all we need to do is find the minimal polynomial of the generator.

Example: Show that the field $\mathbb{Q}(\sqrt[8]{2})$ has degree 8 over $\mathbb{Q}$ and find a basis.

- Observe that $\sqrt[8]{2}$ is a root of the polynomial $x^8 - 2$ over $\mathbb{Q}$, and this polynomial is irreducible by Eisenstein's criterion with $p = 2$.
- Therefore, $x^8 - 2$ is the minimal polynomial of $\sqrt[8]{2}$.
- Thus, by our results on simple extensions we see that $[\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}] = 8$ and that the set $\{1, 2^{1/8}, 2^{2/8}, \ldots, 2^{7/8}\}$ is a basis.

# Simple Extensions, X

Example: Show that the field $\mathbb{Q}(\sqrt{3+\sqrt{21}})$ has degree 4 over $\mathbb{Q}$ and find a basis.

# Simple Extensions, X

Example: Show that the field $\mathbb{Q}(\sqrt{3+\sqrt{21}})$ has degree 4 over $\mathbb{Q}$ and find a basis.

- If we let $\alpha = \sqrt{3+\sqrt{21}}$, then $\alpha^2 = 3+\sqrt{21}$.
- Squaring gives $(\alpha^2-3)^2 = 21$, so that $\alpha^4 - 6\alpha^2 - 12 = 0$.
- However, the polynomial $q(x) = x^4 - 6x^2 - 12$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with $p = 3$.
- Therefore, $q$ must be the minimal polynomial of $\alpha$.
- Thus, by our results, we see that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and that the set $\{1, \alpha, \alpha^2, \alpha^3\}$ is a basis.

# Simple Extensions, XI

We can also see that if $\alpha$ and $\beta$ have the same minimal polynomial over $F$, then the extension fields $F(\alpha)$ and $F(\beta)$ are isomorphic:

**Corollary (Algebraic Equivalence)**

*If $\alpha$ and $\beta$ are two elements in $K/F$ with equal minimal polynomials, then the fields $F(\alpha)$ and $F(\beta)$ are isomorphic as fields. Explicitly, there is an isomorphism $\varphi : F(\alpha) \to F(\beta)$ that fixes $F$ (i.e., sends every element in $F$ to itself) and sends $\alpha$ to $\beta$.*

Proof:

- Both fields are isomorphic to $F[x]/m(x)$ where $m$ is the common minimal polynomial.
- Thus $F(\alpha)$ is isomorphic to $F(\beta)$ since the composition of isomorphisms is an isomorphism. This composition sends $\alpha$ to $\beta$ and fixes every element of $F$, also as claimed.

# Simple Extensions, XII

Example: If $\alpha = \sqrt{2}$ and $\beta = -\sqrt{2}$, then $\alpha$ and $\beta$ both have the minimal polynomial $x^2 - 2$ over $\mathbb{Q}$, so $F(\alpha)$ is isomorphic to $F(\beta)$.

- Explicitly, the isomorphism maps $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ to the element $a + b(-\sqrt{2}) \in \mathbb{Q}(-\sqrt{2})$.
- In fact, these fields are equal (as subfields of $\mathbb{R}$ or of $\mathbb{C}$) because $\sqrt{2} \in \mathbb{Q}(-\sqrt{2})$ and $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.
- Thus, we may alternatively view this isomorphism as a map from $\mathbb{Q}(\sqrt{2})$ to itself, acting via $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$.

In this example, $F(\alpha)$ is actually equal to $F(\beta)$ as a set. This is not necessarily the case in general, as the next example will show.

# Simple Extensions, XIII

Example: If $\alpha = \sqrt[3]{2}$ is the real cube root of 2, and $\beta = e^{2\pi i/3}\sqrt[3]{2}$ is a nonreal cube root of 2, then $\alpha$ and $\beta$ both have the minimal polynomial $x^3 - 2$ over $\mathbb{Q}$, and so $F(\alpha)$ is isomorphic to $F(\beta)$.

- As an explicit complex number, notice that $e^{2\pi i/3} = (-1 + i\sqrt{3})/2$ , and the cube of this number is indeed 1 (one may either note that $e^{2\pi i} = 1$, or simply cube it explicitly). Thus, $\beta^3 = 2$ as claimed.
- However, as subfields of $\mathbb{C}$, $F(\alpha)$ is not equal to $F(\beta)$, because $F(\alpha)$ is a subfield of $\mathbb{R}$ while $F(\beta)$ is not.
- Nonetheless, these two fields have precisely the same algebraic structure, which is the same as the structure of the field $\mathbb{Q}[x]/(x^3 - 2)$.

# Simple Extensions, XIV

In particular, you should take a moment to re-evaluate what exactly you think "the cube root of 2" actually is.

# Simple Extensions, XIV

In particular, you should take a moment to re-evaluate what exactly you think "the cube root of 2" actually is.

- One perspective (the analytic one) is that it is the unique real number $\sqrt[3]{2} \approx 1.25992$ whose cube is equal to 2: such a number certainly exists by the intermediate value theorem, and is unique by the mean value theorem.
- The other perspective (the algebraic one) is that "a cube root of 2" is merely "a number whose cube equals 2". There is no uniquely special cube root of 2, and (depending on what field you are in) there may be 3 such numbers, 1 such number, or none at all.
- Specifically, in $\mathbb{F}_5$, there is one cube root of 2 (namely, 3), whereas in $\mathbb{F}_7$ the number 2 has no cube root at all, and in $\mathbb{F}_{31}$ there are three cube roots of 2 (namely, 4, 7, and 20).

# Simple Extensions, XV

The observation in this last example may seem minor, but it is actually very important.

We will often encounter situations where fields are isomorphic but not equal, and this question of whether two fields are merely *isomorphic* or actually *equal* is connected to a number of subtle issues, which we will of course deliberate upon very carefully!

# Simple Extensions, XVI

Another way to interpret all of this is to view the different roots of the minimal polynomial as being "algebraically indistinguishable", in the sense that the resulting extension fields have the same algebraic structure.

- This does not mean that the fields are the same, since we may sometimes be able to distinguish these fields in some other ("non-algebraic") way.
- In the example with $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(e^{2\pi i/3}\sqrt[3]{2})$, we used information about the field $\mathbb{R}$ (which involves using additional analytic/topological operations (i.e., the use of limits and continuity), rather than intrinsic algebraic properties of the field $\mathbb{Q}$) to distinguish these two fields.

# Summary

We discussed some useful properties of subfields and field extensions.

We discussed simple extensions and their relationship to polynomial quotient rings.

Next lecture: Algebraic extensions.