A Review of Equivalence Relations

Definition: Let X be any set. A relation $\sim$ on X is called an **equivalence relation** if it satisfies the following three properties:

(i) Reflexive: $x \sim x$ for all $x \in X$
(ii) Symmetric: if $x \sim y$, then $y \sim x$ for all $x, y \in X$
(iii) Transitive: if $x \sim y$ and $y \sim z$, then $x \sim z$ for all $x, y, z \in X$

If $x \in X$, then $[x] = \{y: y \sim x\}$ is called the **equivalence class of** x

The importance of equivalence relations is due to the following result:

Proposition. Every element of X is in an equivalence class and any two equivalence classes are either equal or disjoint.

Proof.

First, for any $x \in X$, $x \sim x$, and so $x \in [x]$, proving the first statement. Next, assume the classes $[x]$, $[y]$ are not disjoint and choose $z \in [x] \cap [y]$. Hence $x \sim z$ and $z \sim y$, thus $x \sim y$. So, if $w \in [x]$, then $w \sim x$ and $x \sim y$ implies $w \sim y$. Thus $[x] \subset [y]$ and analogously $[y] \subset [x]$. This proves the second statement. ■

The proposition implies that an equivalence relation defined on a set breaks up a set into disjoint, "smaller pieces". These "smaller pieces" are usually called a **partition** of the set. An extreme amount of mathematics is carried out using equivalence relations. The first example is something you have been doing since elementary school.

Example 1: Let's assume that the integers $\mathbb{Z}$ are "god given" (actually, they're not, they too can be constructed via equivalence relations), but "god" did not give us fractions (i.e. man had to discover the rational numbers). To whit:

Let $S = \{(a, b): a, b \in \mathbb{Z}, b \neq 0\}$, i.e. the set of all ordered pairs of integers where the second component is not zero. We propose the following relation on this set:

Define $(a, b) \sim (c, d)$ iff $ad = bc$. We claim this is an equivalence relation. You check it's reflexive and symmetric, I'll check it's transitive:

Suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $ad = bc$ and $cf = de$. Note that $b, f \neq 0$ and so $adf = bcf$ and $bcf = bde$ implying that $adf = bde$. As we know, we have the cancelation property for integers and since $d \neq 0$ we conclude $af = be \rightarrow (a, b) \sim \sim (e, f)$. Consequently this is an equivalence relation. .
Of course, you'll recognize this equivalence relation is the relation which tells us when two fractions are equal. We usually abuse notation and write

$[(a,b)] = \frac{a}{b}$, and hence $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$. Now, you know that there are arithmetic operations that can be defined for fractions – addition and multiplication – and we end up getting what is called a field (a commutative ring in which every non zero element has a multiplicative inverse). We won't prove this now, however, in the class we will show this can always be done for any integral domain; by constructing the field of fractions of an integral domain (actually, one can even form "fractions" for rings where there are zero divisors and for certain non commutative rings, but we will only pursue the construction for integral domains).

Example 2: Again we will start with the integers, but define a completely different equivalence relation. Let $n > 1$ be an integers and for all $a, b \in \mathbb{Z}$ define $a \equiv bmodn$ if $n|(a-b)$, i.e. $a - b = nq, q \in \mathbb{Z}$ (we say $a - b$ is **divisible by** n). In this case we say a is **congruent to** b **modulo (mod) n.** Let's check this is an equivalence relation:

(i) $a \equiv amodn$ since $a - a = 0 = n \cdot 0$
(ii) If $a \equiv bmodn$, then $a - b = nq \rightarrow b - a = n(-q) \rightarrow b \equiv amodn$
(iii) If $a \equiv bmodn$ and $b \equiv cmodn$ then $a - b = nq$ and $b - c = nr$. Adding, we obtain $a - c = n(q + r) \rightarrow a \equiv cmodn$

Hence, congruence modulo gives an equivalence relation on the integers. What are the equivalence classes? The key to understanding this is the division algorithm. For any integer a, by the division algorithm we have $a = nq + r, 0 \leq r < n$ and hence $a \equiv rmodn$. Thus every integer is congruent to its remainder upon division by $rmodn$. Thus, we only get n equivalence classes, namely $[0], [1], [2], \ldots, [n-1]$. That is, every integers is in one, and only one, of these equivalence classes. This is not an isolated example, most of number theory and a large amount of abstract algebra is concerned with this equivalence relation. Hopefully, you'll recall from Math 360 that we let $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$ and we call this set the **integers mod n.** Like the preceding example, we can introduce addition and multiplication on this set which makes it a commutative ring.

Addition: $[a] + [b] = [a + b]$
Multiplication $[a][b] = [a][b]$

You may recall that these operations are well-defined in the following sense (this needs to be proved for the fraction example, but we'll deal with that later).

Addition is well defined: That is if $[a] = [a']$ and $[b] = [b']$, then$[a + b] = [a' + b']$.
Multiplication is well defined: That is if $[a] = [a']$ and $[b] = [b']$, then $[ab] = [a'b']$.

I'll prove that multiplication is well defined, you should prove addition is:

$[a] = [a'] \rightarrow a - a' = nq$ and $[b] = [b'] \rightarrow b - b' = nr$. Hence, $ab - a'b = nqb$ and $a'b - a'b' = nra'$, and adding these last two equations yields

$ab - a'b' = n(qb + ra') \rightarrow ab \equiv a'b' mod n \rightarrow [ab] = [a'b']$. This shows multiplication is well defined. As you might recall, after these operations were checked to be well defined, we proceeded to show they satisfy many familiar arithmetic operations. That is $\mathbb{Z}_n$ is a commutative ring with additive identity element [0] and multiplicative identity [1]. What's interesting about these rings is sometimes they are fields – that is every non zero element has a multiplicative inverse and other times there are zero divisors, that is two non zero elements that multiply to zero. For example, in $\mathbb{Z}_6$, $[2][3] = [6] = [0]$. We will review these rings.

Example 3: Let $\mathbb{R}[x]$ denote that set of all polynomials with real coefficients. This is a ring, where the operations are the usual ones of addition and multiplication of polynomials. We introduce a relation on $\mathbb{R}[x]$ as follows: for $p(x), q(x) \in \mathbb{R}[x]$ define $p(x) \sim q(x)$ iff $p(x) - q(x) = f(x)(x^2 + 1)$, we could write this as $p(x) \equiv q(x)(mod)(x^2 + 1)$ and this is shown to be an equivalence relation just as we did in the last example. The set of all the equivalence classes in this example is written $\mathbb{R}[x] \,/\, (x^2 + 1)$. Both of these examples are special cases of a general type of equivalence relation, which yields quotient rings. As in the preceding example, we use the division algorithm for polynomials to give the form of a basic equivalence class. Suppose $f(x) \in \mathbb{R}[x]$, by the division algorithm for polynomials we have $f(x) = q(x)(x^2 + 1) + r(x)$, where $r(x) = 0$ or $degr(x) < 2$. In other words, an arbitrary element in $\mathbb{R}[x] \,/\, (x^2 + 1)$ looks like $[a + bx]$.

For example, by long division
$[x^3 + 1] = [-x + 1]$ (because $x^3 + 1 = x(x^2 + 1) + (-x + 1)$). We will see this is also a ring with the usual addition and multiplication of equivalence classes (just as above). Note, assuming we have shown the operations are well defined, we have $[x]^2 = [x^2] = [-1] = -[1]$, in other words the square of $[x]$ is negative one – this should remind you of the complex numbers. Also, from the above,
$[a + bx] = [a] + [b][x]$, where $[x]^2 = -[1]$. We will see that $\mathbb{R}[x] \,/\, (x^2 + 1)$ is ring isomorphic to the complex numbers.

The Field of Fractions of an Integral Domain

An important property that all integral domains posses is that they are contained in a field, all of whose elements are "quotients," of elements in the integral domain. This is, completely analogous to the integers sitting inside the rational numbers.

Theorem. If D is an integral domain, then there exists a field F and a monomorphism $i: D \to F$, such that every element of F is of the form $i(a)(i(b))^{-1}$, for $a, b \in D, b \neq 0$.

Proof.

Let $S = \{(a, b): a, b \in D, b \neq 0\}$. We define an equivalence relation $\sim$ on S as follows: $(a, b) \sim (c, d)$ iff $ad = bc$. It is easy to check the reflexive and symmetric properties. We check it is transitive: assume $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $ad = bc$ and $cf = de$. Then $adf = bcf$ and $bcf = bde$, implying that $adf = bde$ and due to cancelation in an integral domain we conclude that $af = be$, which yields $(a, b) \sim (e, f)$. We will denote the equivalence class of (a, b) by $[(a, b)]$. This class will play the role of the "fraction" $\frac{a}{b}$.

Let $F = \{[(a, b)]: a, b \in D, b \neq 0\}$. We must show F is the desired field. First, we must introduce addition and multiplication on F.

Addition: $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$
Multiplication: $[(a, b)][(c, d)] = [(ac, bd)]$

As usual, when working with equivalence relations, the key thing is to show these operations are well defined.

Addition is well defined: Assume $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$. This implies that $ab' = ba'$ and $cd' = dc'$. Multiplying the first equation by $dd'$and the second by bb' we obtain $ab'dd' = ba'dd'$ and $bb'cd' = bb'dc$'. Hence

$ab'dd' + bb'cd' = ba'dd' + bb'dc$', and so $(ad + bc)b'd' = bd(a'd' + b'c')$. This means $[(ad + bc, bd)] = [(a'd' + b'c', b'd')]$, that is
$[(a, b)] + [(c, d)] = [(a', b')] + [(c', d')]$, thus addition is well defined.

Multiplication is well defined: As an exercise show $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$ implies $[(ac, bd)] = [(a'c', b'd')]$, which gives multiplication is well defined.

To complete the proof that F is a field we would have to check all the axioms showing it is a commutative ring and every nonzero element is invertible. We will check a few axioms.

Additive identity: The additive identity of F is the class $[(0,1)]$: Using the definition of addition we get

$$[(a,b)] + [(0,1)] = [(a \cdot 1 + b \cdot 0, b \cdot 1)] = [(a,b)].$$

Also note that $[(0,1)] = [(0,b)]$ for any $b \neq 0$.

Additive Inverses: the additive inverse of $[(a,b)]$ is $[(-a,b)]$, that is $-[(a,b)] = [(-a,b)]$, since

$$[(a,b)] + [(-a,b)] = [(ab - ba, b^2)] = [(0,b^2)] = [(0,1)].$$

Multiplicative Identity: As an exercise check that $[(1,1)]$ is the multiplicative identity. Also note that $[(1,1)] = [(b,b)]$ for any $b \neq 0$.

Multiplicative inverses: Suppose $[(a,b)] \neq [(0,1)]$. Then $a \neq 0$ and hence

$$[(a,b)][(b,a)] = [(ab,ab)] = [(1,1)].$$

Thus $[(a,b)]^{-1} = [(b,a)]$ and we conclude F is a field.

Now, define a map $i: D \to F$ by $i(a) = [(a,1)]$. We check this is a one – to – one ring homomorphism.

$$i(a+b) = [(a+b,1)] = [(a,1)] + [(b,1)] = \ i(a) + i(b)$$

$$i(ab) = [(ab,1)] = [(a,1)][(b,1)] = i(a)i(b)$$

$$i(1) = [(1,1)].$$

So i is a ring homomorphism and $a \in keri \ iff \ i(a) = [(a,1)] = [(0,1)] \ iff \ a = 0$.

Thus, i is a ring monomorphism. Finally, if $[(a,b)] \in F$, then

$$[(a,b)] = [(a,1)][(1,b)] = \ i(a)\big(i(b)\big)^{-1}.$$

This shows that every element in F is a "quotient" of elements in the isomorphic "copy" of D in F. ■

Usually, we slightly abuse notation and assume D is literally contained in F, and we drop the equivalence class notation and just write ab^{-1} instead of $i(a)\big(i(b)\big)^{-1}$.

It can also be proven that F is unique "up to isomorphism" so that if there is a field K and a monomorphism $j: D \to K$ such that every element of K is of the form $j(a)(j(b))^{-1}$, for $a, b \in D, b \neq 0$, then F and K are isomorphic.

Definition. The field F constructed above is called the *field of fractions* of the integral domain D.

To check that a set F is the field of fractions of an integral domain we have to check two things:

1. F is a field containing D
2. Every element of $F$is of the form $ab^{-1}$for $a, b \in D, b \neq 0$.

Examples.

1. Clearly, the rational numbers $\mathbb{Q}$ is the field of fractions of the integers $\mathbb{Z}$.
2. $\mathbb{Q}(\sqrt{2})$ is the field of fractions of the integral domain $\mathbb{Z}[\sqrt{2}]$.
3. Consider the ring $\mathbb{R}[x]$ of all polynomials with real coefficients. This is an integral domain and so must have a field of fractions. We denote its field of fractions by $\mathbb{R}(x)$ and formally it is defined by

$$\mathbb{R}(x) = \left\{ \frac{p(x)}{q(x)} : p(x), q(x) \in \mathbb{R}[x] \right\}$$

More generally, for any field F, the field of fractions of $F[x]$ is

$$F(x) = \left\{ \frac{p(x)}{q(x)} : p(x), q(x) \in F[x] \right\}$$

$F(x)$ is called the *field of rational functions.*

The Greatest Common Divisor Exists in UFDs

Definition. Let R be an integral domain and suppose $a, b \in R$ are non zero, non units. An element $d \in R$ is called a greatest common divisor (GCD) of a and b if:

1. $d|a$ and $d|b$
2. if $d' \in R$ with $d'|a$ and $d'|b$, then $d'|d$

We write $d = \gcd(a, b)$.

Exercise: Prove if d and d' are both gcds for a and b, then they must be associates (i.e., $b = ua, u \in U(R)$)

If R is a PID, there is a quick way to show GCDs and that they can be expressed as linear combinations. Here's the exercise.

Exercise: Suppose R is a PID and let $a, b \in R$, non zero, non units. Consider (a, b), the ideal generated by a and b. Since R is a PID there exists some $d \in R$ with $(a, b) = (d)$. Show $d = \gcd(a, b)$.

We will show that GCDs exist in UFDs:

Proposition. Suppose R is a UFD and $a, b \in R$ are non zero, non units. Then a and b have a GCD.

Proof.

Let $a = {p_1}^{m_1}{p_2}^{m_2} \cdots {p_k}^{m_k}$ and $b = {p_1}^{n_1}{p_2}^{n_2} \cdots {p_k}^{n_k}$ be the factorization into irreducible elements.

Let $d = {p_1}^{\min(m_1, n_1)}{p_2}^{\min(m_2, n_2)} \cdots {p_k}^{\min(m_k, n_k)}$. It is clear that $d|a$ and $d|b$.

Furthermore if $d'|a$ and $d'|b$, then $a = d'r, b = d's, r, s' \in R$. Hence, if we factor all of these elements into products of irreducibles, we see that the irreducibles involved in d' must come from the $p_i's$ and the power of p_i can be no more than $\min(m_i, n_i)$, from which it follows that $d'|b$, then $d'|d$. ■

Unfortunately, we cannot conclude that the greatest common divisor of two elements in a UFD can be expressed as a linear combination, as it can in a PID. Here's an example.

Exercise: We will soon see that $\mathbb{Z}[x]$ is a UFD, we already know that it is not a PID. Show that in $\mathbb{Z}[x]$,
1. $\gcd(6x, 10x^2) = 2x$ and
2. $2x$ is not a linear combination of $6x$ and $10x^2$

An Introduction to Extension Fields

Definition. Suppose E, F are fields. We say E is an *extension field* of F if $F \subset E$.

Example .

1. The complex numbers $\mathbb{C}$ is an extension field of the real numbers $\mathbb{R}$.
2. $\mathbb{Q}(\sqrt{2})$ is an extension field of $\mathbb{Q}$.
3. If F is any field and $f(x) \in F[x]$ is irreducible, then we have seen that $F[x]/(f(x))$ is a field. Define a map $i: F \to F[x]/(f(x))$ by $i(a) = a + (f(x))$. Check that i is a monomorphism (i.e., a one – to – one ring homomorphism). In this way we see that $F[x]/(f(x))$ is an extension field of F.

Rapid Review of Vector Spaces:

Recall that an abelian group V, under addition, is a *vector space* over a field F, if there is a scalar multiplication $F \times V \to V$, $(\alpha, v) \to \alpha v$ such that following axioms hold for all $u, v \in V, \alpha, \beta \in F$

1. $\alpha(u + v) = \alpha u + \alpha v$
2. $(\alpha + \beta)u = \alpha u + \beta u$
3. $(\alpha\beta)u = \alpha(\beta u)$
4. $1 \cdot u = u$

Often, in linear algebra courses (and books), F is taken to be the real numbers or the complex numbers. However, this is not necessary for the majority of things you learned in linear algebra. The key ideas in linear algebra are linear independence, basis and dimension. The material you need to know from linear algebra is summarized in the following definition. Read it over and make sure you understand these ideas.

Definitions. Let V be a vector space. A set of vectors $\{v_1, v_2, \dots, v_n\}$ is said to be *linearly independent* if $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0_V$ (the zero vector), then $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$ (the zero scalar). If the set is not linearly independent (that is, it is possible to have a linear combination equal to the zero vector, with non zero scalars), then we say the set is *linearly dependent.* An infinite set of vectors is linearly independent, if any finite subset is linearly independent. The set of vectors $\{v_1, v_2, \dots, v_n\}$ is said to *span* V if given any u$\in V$, $u = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$, for some scalars $\alpha_i \in F$. A linearly independent, spanning set is called a *basis* for V. A major result in linear algebra is that two bases (even infinite ones) have the same number of vectors. The number of vectors in a basis is called the *dimension* of the vector space. A principal result in linear algebra (which gets used a lot in field theory is): if $dim V = n$, then any set containing more than n vectors must be linearly dependent. The proofs of these results work over any scalar field. We will assume all

linear algebra results. They should have been proven in Math 262, if you have taken Math 462, you should be more familiar with this material. If not, no worries, you just have to know the results.

Important Remark!! If $F \subset E$(that is E is an extension field of F), then we can view E as a vector space over F. The addition is just the addition in E, and the scalar multiplication is just the multiplication in E. The 4 scalar axioms above are due to the fact that a field is a ring. Here we are viewing the "vectors" as the elements in E, and the scalars are the elements in F. This simple remark is the basis of all modern field theory and needs to be understood. We let $[E: F]$ denote the dimension of E as a vector space over F.

Examples.

1. $[\mathbb{C}: \mathbb{R}] = 2$, with basis $\{1, i\}$.
2. $\left[\mathbb{Q}(\sqrt{2}): \mathbb{Q}\right] = 2$, with basis $\left\{1, \sqrt{2}\right\}$.
3. $\left[\mathbb{Q}\left(2^{\frac{1}{3}}\right): \mathbb{Q}\right] = 3$, with basis $\left\{1, 2^{\frac{1}{3}}, 2^{\frac{2}{3}}\right\}$.
4. For any field F, $[F; F] = 1$, with basis $\{1\}$.
5. Let $\mathbb{R}(x)$ be the field of rational functions (that is the field of fractions of the polynomial ring $\mathbb{R}[x]$). Then $[\mathbb{R}(x): \mathbb{R}] = \infty$ since the set $\{1, x, x^2, \dots\}$ is an infinite linearly independent set over $\mathbb{R}$

We will be primarily concerned with finite dimensional field extensions, such as those in examples 1 – 4 above.

Definition. An extension field E of F is called a *finite extension,* if $[E: F] < \infty$.

Definition. Suppose E is an extension field of F. We say $u \in E$ is *algebraic over F* if there exists a non zero polynomial $f(x) \in F[x]$ such that $f(u) = 0$.

Examples.

1. i is algebraic over $\mathbb{R}$ since it is the root of $x^2 + 1$.
2. $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since it is the root of $x^2 - 2$.
3. Show that $u = \sqrt{2} + \sqrt{3}$ is algebraic over $\mathbb{Q}$:

$\left(u - \sqrt{2}\right)^2 = 3$ implies $u^2 - 2u\sqrt{2} + 2 = 3$, which gives $u^2 - 1 = 2u\sqrt{2}$ and squaring both sides yields $u^4 - 2u^2 + 1 = 8u^2$, so $u^4 - 10u^2 + 1 = 0$. Hence, u is a root of the rational polynomial $x^4 - 10x^2 + 1$.

Definition. Suppose E is an extension field of F. We say E is an *algebraic extension* of F if every element of E is algebraic over F.

The next result provides a convenient method for showing a given extension is algebraic.

Proposition 1. If $[E:F] = n < \infty$, that is, E is a finite extension of F, then E is an *algebraic extension* of F.

Proof.

Let $u \in E$ be arbitrary. Since $[E:F] = n$, we know that the elements $1, u, u^2, \dots, u^n$ must be linearly dependent over F. This means that there are scalars $a_0, a_1, \dots, a_n \in F$, not all 0, such that $a_0 + a_1u + \cdots + a_nu^n = 0$. Hence u is algebraic over F, being the root of the nonzero polynomial $a_0 + a_1x + \cdots + a_nx^n$. ■

This result can be remembered as **FINITE ⇒ ALGEBRAIC**

We give an example later on (or next semester) showing that the reverse implication is false.

Proposition 2. Suppose $F \subset E$ is a field extension and let $u \in E$ be an algebraic element. Then there exists a unique monic, irreducible polynomial $m_u(x) \in F[x]$ having u as a root. Furthermore, if $degm_u(x) = n$, then $1, u, u^2, \dots, u^{n-1}$is an $F - basis$ for $F(u)$ over F (recall $F(u) \cong F[x] \,/\, \big(m_u(x)\big)$), where $F(u)$ is the subring of E generated by u. That is, $F(u) = \{a_0 + a_1u + \cdots + a_{n-1}u^{n-1} : a_i \in F\}$ and so $[F(u):F] = n = \ degm_u(x)$.

Proof.

Recall the substitution homomorphism $\mu_u : F[x] \to F[u]$, where $F[u] = im\mu_u = \{a_0 + a_1u + \cdots + a_nu^m : a_i \in F, m\ varies\}$. By the FHT, $F[x]/ker\mu_u \cong F[u]$. Furthermore, we know that $ker\mu_u = (m_u(x))$, where $m_u(x)$ is the unique monic polynomial, of smallest degree, having u as a root. As we have noted, $m_u(x)$ must be irreducible, otherwise we would have a polynomial of smaller degree having u as a root. Hence $F[u]$ is a field and we write it with the parentheses, i.e. $F(u)$. Hence $F(u)$ is an extension field of F and so it is an $F -$ vector space. We must now prove that $1, u, u^2, \dots, u^{n-1}$is a vector space basis for $F(u)$ over F.

Spanning: Let $a_0 + a_1u + \cdots + a_mu^m \in F(u)$ and set $f(x) = a_0 + a_1x + \cdots + a_mx^m$. By the division algorithm, there exists $q(x), r(x) \in F[x]$ such that

$f(x) = q(x)m_u(x) + r(x)$, where $r(x) = 0$ or $degr(x) < n = degm_u(x)$. So $r(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$. Now, substituting in $x = u$ (using $m_u(u) = 0$) yields

$$a_0 + a_1u + \cdots + a_nu^m = f(u) = b_0 + b_1u + \cdots + b_{n-1}u^{n-1}$$

and hence $F(u)$ is spanned by $1, u, u^2, \dots, u^{n-1}$ over F.

Independence: Suppose $c_0 + c_1u + \cdots + c_{n-1}u^{n-1} = 0$, with some $c_i \neq 0$. Then

$g(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$is a non zero polynomial in $F[x]$, of degree less than $n = deg m_u(x)$, contradicting the minimality of n.

Hence $1, u, u^2, \dots, u^{n-1}$is a vector space basis of $F(u)$ over F and $[F(u): F] = n$ ■

Notation: We will use $irr(u, F)$ to represent the minimal polynomial of u over F. So $irr(u, F) = m_u(x)$.

The next result gives us a method for determining $irr(u, F)$.

Proposition 3. If $f(x) \in F[x]$ is an irreducible monic polynomial and $f(u) = 0$, then $f(x) = irr(u, F)$.

Proof.

We know that the kernel of $\mu_u: F[x] \to F[u]$ is generated by $irr(u, F)$ and $f(u) = 0$ implies $f(x) \in ker\mu_u$, that is $f(x) \in \big(irr(u, F)\big)$. Hence $f(x) = irr(u, F)g(x)$, for some $g(x) \in F[x]$. But $f(x)$ irreducible implies $f(x) = c\ irr(u, F)$, for some $c \in F$. However, since both $f(x)$ and $irr(u, F)$ are monic, $c = 1$ and $f(x) = irr(u, F)$. ■

Examples.

1. $irr(i, \mathbb{R}) = x^2 + 1$. Thus $[\mathbb{R}(i): \mathbb{R}] = 2$, with basis $1, i$. Of course, this is no big surprise, as we know $\mathbb{R}(i) = \mathbb{C}$.
2. By Eisenstein's Criterion (EC), we know that for any natural number n, $x^n - 2$ is irreducible over $\mathbb{Q}$ and has the real root $u = 2^{\frac{1}{n}}$. Thus $x^n - 2 = irr\left(2^{\frac{1}{n}}, \mathbb{Q}\right)$ and $\left[\mathbb{Q}\left(2^{\frac{1}{n}}\right): \mathbb{Q}\right] = n$, and $\mathbb{Q}\left(2^{\frac{1}{n}}\right)$ has $\mathbb{Q}-$ basis $1, 2^{\frac{1}{n}}, 2^{\frac{2}{n}}, \dots, 2^{\frac{n-1}{n}}$. Hence $\mathbb{Q}\left(2^{\frac{1}{n}}\right) = \left\{a_0 + a_1 2^{\frac{1}{n}} + a_2 2^{\frac{2}{n}} + \cdots + a_{n-1}2^{\frac{n-1}{n}}: a_i \in \mathbb{Q}\right\}$.
3. From an example above, we know that $u = \sqrt{2} + \sqrt{3}$ is algebraic over $\mathbb{Q}$ and is the root of the polynomial $f(x) = x^4 - 10x^2 + 1$. As an **Exercise,** show this polynomial is irreducible over $\mathbb{Q}$. Thus $irr\left(\sqrt{2} + \sqrt{3}: \mathbb{Q}\right) = x^4 - 10x^2 + 1$ and this gives $\left[\mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right): \mathbb{Q}\right] = 4$, with basis $1, u, u^2, u^3$.
4. Let $\omega \neq 1$ denote a root of $x^p - 1$, for some prime p. Thus ω is a root of the cyclotomic polynomial $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$, which we proved is irreducible over $\mathbb{Q}$ (using EC). Thus $[\mathbb{Q}(\omega): \mathbb{Q}] = p - 1$, with basis $1, \omega, \omega^2, \dots, \omega^{p-1}$. ω is called a *primitive p^{th}root of unity.*

The next result shows that given any non constant polynomial over a field F, we can find an extension field containing a root of the polynomial. This is an existence proof, in the sense that the proof does not give an explicit algorithm for finding a root.

Theorem 4(Kronecker's Theorem). Suppose $f(x) \in F[x]$ is a non constant polynomial. Then there exists an extension field K of F, which contains a root of $f(x)$.

Proof.

Since $F[x]$ is a UFD, we know that $f(x)$ must have an irreducible factor $p(x)$. Since $f(x)$ is a multiple of $p(x)$, a root of $p(x)$ is a root of $f(x)$.
As we know, $K = F[x] \,/\, (p(x))$ is an extension field of F (basically, we view $a \in F$ as $\overline{a} = a + (p(x)) \in K$ - this is analogous to viewing $n \in \mathbb{Z}$ as $\frac{n}{1} \in \mathbb{Q}$). If $p(x) + a_1 x + \cdots + a_n x^n$, then we claim that $\overline{x} = x + \big(p(x)\big) \in K$ is a root of $p(x)$. Actually, we will show $\overline{x}$ is a root of $\overline{a_0} + \overline{a_1} x + \cdots + \overline{a_n} x^n$ (the isomorphic image of $p(x)$ in K). To this end, we have $p(\overline{x}) = \overline{a_0} + \overline{a_0}\,\overline{x} + + \cdots + \overline{a_n}\,\overline{x}^n =$ (because barring is a homomorphism) $\overline{a_0 + a_1 x + \cdots + a_n x^n} = \overline{p(x)} = p(x) + \big(p(x)\big) = \overline{0}$, proving the result. ■

Hence, given any irreducible polynomial, over a field F, we can always assume it has a root in some extension field of F.

Example. Let's return to a familiar example, but looking at it from this point of view. As we know $f(x) = x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$. Let u be a root in some extension field. Hence, Proposition 3, we know that $f(x) = irr(u, \mathbb{Z}_3)$, and by Proposition 2, $[\mathbb{Z}_3(u) : \mathbb{Z}_3] = 2$ and $1, u$, is a basis for $\mathbb{Z}_3(u)$ over $\mathbb{Z}_3$. This means that every element in $\mathbb{Z}_3(u)$ can be written uniquely in the form $a + bu$, where $a, b \in \mathbb{Z}_3$. Hence, $|\mathbb{Z}_3(u)| = 9$. This is no big surprise, because we know that $\mathbb{Z}_3(u) \cong \mathbb{Z}_3[x]/(x^2 + 1)$, and in HW 2 you showed this field had 9 elements. Let's return to the problem that you did for HW. Find $(2 + u)^{-1}$in $\mathbb{Z}_3(u)$. We solve it in the usual manner: let

$(2 + u)^{-1} = a + bu \to 1 = (2 + u)(a + bu) = (2a - b) + (a + 2b)u$ (here we are using the fact that in $\mathbb{Z}_3(u)$, $u^2 = -1$. Since $1, u$, is a basis for $\mathbb{Z}_3(u)$ over $\mathbb{Z}_3$, we can equate coefficients and this yields

$$\begin{aligned} 2a - b &= 1 \\ a + 2b &= 0 \end{aligned}$$

Solving this system over $\mathbb{Z}_3$, we get $a = b = 1$. Thus $(2 + u)^{-1} = 1 + u$. Another interesting point is that the other root of $f(x) = x^2 + 1$ is $-u = 2u$ and so $\mathbb{Z}_3(u)$ contains all the roots of $f(x)$. So we can factor $f(x)$ completely in $\mathbb{Z}_3(u)$ as $f(x) = (x - u)(x + u)$.

Let's look at another similar example:

Example. Note that $g(x) = x^3 - x + 1$ is irreducible in $\mathbb{Z}_3[x]$ (why?). Let u be a root in some extension. Hence $g(x) = irr(u, \mathbb{Z}_3)$, and by Proposition 2, $[\mathbb{Z}_3(u): \mathbb{Z}_3] = 3$ and $1, u, u^2$ is a basis for $\mathbb{Z}_3(u)$ over $\mathbb{Z}_3$. We claim that the other roots of $g(x)$ are $u + 1$ and $u + 2$. Let's check this, using the binomial theorem $mod 3$:

$g(u + 1) = (u + 1)^3 - (u + 1) + 1 = u^3 + 1 - u - 1 + 1 = u^3 - u + 1 = 0$ and
$g(u + 2) = (u + 2)^3 - (u + 2) + 1 = u^3 + 8 - u - 2 + 1 = u^3 - u + 1 = 0.$

So we see that $\mathbb{Z}_3(u)$ contains all the roots of $g(x)$. Also note that that every element in $\mathbb{Z}_3(u)$ can be written uniquely in the form $a + bu + cu^2$, where $a, b, c \in \mathbb{Z}_3$. Consequently $|\mathbb{Z}_3(u)| = 27$. If you want (it's probably worthwhile), make up a few problems for yourself finding inverses of elements in $\mathbb{Z}_3(u)$ (remember, the key to doing the computation is the fact that, in this field, $u^3 = u - 1$.

In the above two examples, $\mathbb{Z}_3(u)$ is a special case of a type of field that has nice properties.

Definition. Let $f(x)$ be a non constant polynomial over a field F. An extension field E of F is called a *splitting field* of $f(x)$ if it is the smallest extension field of F containing all the roots of $f(x)$. Equivalently, E can be generated a field by the roots of $f(x)$.

Example. From the above two examples, we see that $\mathbb{Z}_3(u)$ is a splitting field for the polynomials $f(x) = x^2 + 1$ and $g(x) = x^3 - x + 1$, respectively. Of course, u is different in both examples.

Splitting fields play a major role in Galois theory and are studied in greater detail in Math 560.