# Math 5111 (Algebra 1)

## Lecture $\#2 \sim$ September 14, 2020

More Polynomials and Rings:

- Factorization over $\mathbb{Q}$
- Polynomial Modular Arithmetic
- Rings, part 1

This material represents §1.2.4-1.3.4 from the course notes.

# Recap

Last time, I reviewed $\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$ and discussed some basic facts about the polynomials with coefficients in the field $F$.

Today we will finish up the remaining material we will need with polynomials (some results about factorization and irreducibility over $\mathbb{Q}$, and a discussion of polynomial modular arithmetic) and then introduce general rings.

# Factorization over $\mathbb{Q}$, I

It is more difficult to test whether a polynomial is irreducible in $\mathbb{Q}[x]$. A central idea is that we can reduce the problem of factoring in $\mathbb{Q}[x]$ to one of factoring in $\mathbb{Z}[x]$ by clearing denominators:

- Specifically, if $p$ is any polynomial in $\mathbb{Q}[x]$, we may multiply $p$ by the product of all the denominators of its coefficients (or their least common multiple) to obtain a polynomial in $\mathbb{Z}[x]$. Since every nonzero integer is invertible in $\mathbb{Q}$, the factorization of this new polynomial, with integer coefficients, will be essentially the same as that of the original polynomial.
- As an example, consider the problem of factoring $p(x) = 2x^3 + x^2 + \frac{2}{3}x + \frac{1}{3}$ in $\mathbb{Q}[x]$.
- Since 3 is an invertible constant in $\mathbb{Q}[x]$, we may equivalently ask about factoring $3p(x) = 6x^3 + 3x^2 + 2x + 1$ in $\mathbb{Z}[x]$.

# Factorization over $\mathbb{Q}$, II

It is not hard to test for rational roots:

**Proposition (Rational Root Test)**

*Suppose $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ is a polynomial in $\mathbb{Z}[x]$. Then any root $r/s$ (in lowest terms) must have $r | a_0$ and $s | a_n$.*

Proof:

- If $r/s$ is a root of $p(x)$, then $a_n (r/s)^n + a_{n-1} (r/s)^{n-1} + \cdots + a_0 = 0$. Clear denominators: $a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0$.
- Thus, by rearranging, we see that $a_n r^n = s(-a_{n-1} r^{n-1} - \cdots - a_0 s^{n-1})$, so $s$ divides $a_n r^n$. But since $s$ and $r$ are relatively prime, this means $s$ divides $a_n$.
- In a similar way, since $a_0 s^n = r(-a_n r^{n-1} - \cdots - a_1 s^{n-1})$, we see that $r$ divides $a_0 s^n$ hence $a_0$.

# Factorization over $\mathbb{Q}$, III

Example: Show that the polynomial $p(x) = x^3 + ax + 1$ is irreducible in $\mathbb{Q}[x]$ for any integer $a \neq 0, -2$.

- Since this polynomial has degree 3, we need only show that it has no roots in $\mathbb{Q}$.
- By the rational root test, the only possible rational roots are $\pm 1$, and since $p(1) = 2 + a$ and $p(-1) = a$, the conditions on $a$ imply that $p$ has no rational roots. Thus, $p$ is irreducible.

# Factorization over $\mathbb{Q}$, IV

As noted before, the general philosophy is that factorization of polynomials in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are essentially "the same", and this is ultimately true (though not quite so easy to state rigorously):

**Theorem (Gauss's Lemma)**

*If $p(x) \in \mathbb{Z}[x]$ has positive degree and is reducible in $\mathbb{Q}[x]$, then $p(x) = f(x)g(x)$ for some $f(x), g(x) \in \mathbb{Z}[x]$ of positive degree.*

In other words, if a polynomial with integer coefficients factors over the rational numbers, then it actually factors over the integers.

By inverting this, we see that if we want to factor over $\mathbb{Q}$, it is enough to look for factorizations over $\mathbb{Z}$.

# Factorization over $\mathbb{Q}$, V

Proof (outline):

- We say a polynomial in $\mathbb{Z}[x]$ is "primitive" if the gcd of its coefficients is equal to 1. Now observe:
  1. Over $\mathbb{Q}[x]$, any nonzero polynomial $a(x)$ is associate to a primitive polynomial in $\mathbb{Z}[x]$. (Write it down.)
  2. The product of two primitive polynomials is also primitive. (Induct on coefficients.)
- If $p(x) = f_0(x)g_0(x)$ factors in $\mathbb{Q}[x]$, then let $f, g$ be primitive associates of $f_0$, $g_0$.
- Moving units around gives $d \cdot p(x) = e \cdot f(x) \cdot g(x)$ for some relatively prime $d, e$.
- Since $f(x)g(x)$ is primitive, the only possibility is $d = \pm 1$. So we get a factorization of $p(x)$ over $\mathbb{Z}$.

# Factorization over $\mathbb{Q}$, VI

By reducing factorization over $\mathbb{Q}$ to a question over $\mathbb{Z}$, in principle we only have a computation of finite size to worry about (since there are only finitely many possible factorizations).

Of course, in practice one does not want to work through all the details of examining all possible factorizations by hand, since even for degree 4 this is quite tedious, as you'll see on the next slide....

# Factorization over $\mathbb{Q}$, VII

Example: Show $p = x^4 + x^3 - 2x^2 + x + 1$ is irreducible in $\mathbb{Q}[x]$.

- First, by the rational root test, the only possible roots of this polynomial are $\pm 1$, neither of which is a root.
- Thus, if $p(x)$ were reducible, it would factor as a product of two quadratics. By moving factors of $-1$ around (as needed) such a factorization would have the form $p(x) = (x^2 + ax + b)(x^2 + cx + d)$.
- By expanding and comparing coefficients, we see that $a + c = 1$, $b + ac + d = -2$, $ad + bc = 1$, and $bd = 1$.
- The last equation gives $(b, d) = (1, 1)$ or $(-1, -1)$.
- If $b = d = 1$ then we obtain the equations $a + c = 1$ and $ac = -4$, which has no integer solutions.
- If $b = d = -1$ then we obtain $a + c = 1$, $ac = 0$, and $a + c = -1$, which has no solutions at all!
- Therefore, $p(x)$ is irreducible, as claimed.

# Factorization over $\mathbb{Q}$, VIII

Because we do, in fact, want to be lazy in general whenever possible, we usually resort to using general irreducibility criteria. One of the easiest useful ones is as follows:

**Theorem (Eisenstein-Schönemann Criterion)**

*Let $q(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $\mathbb{Z}[x]$. If each coefficient $a_0, a_1, \ldots, a_{n-1}$ is divisible by a prime $p$, and $a_0$ is not divisible by $p^2$, then $q(x)$ is irreducible in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.*

Examples:

- By Eisenstein's criterion with $p = 3$, the polynomial $x^6 - 6x + 3$ is irreducible in $\mathbb{Z}[x]$.
- By Eisenstein's criterion with $p = 2$, the polynomial $x^n - 2$ is irreducible in $\mathbb{Z}[x]$ for any positive integer $n$.

# Factorization over $\mathbb{Q}$, IX

Proof:

- Suppose that $q(x) = b(x)c(x)$ were reducible in $\mathbb{Z}[x]$, with $b(x) = x^s + b_{s-1}x^{s-1} + \cdots + b_0$ and $c(x) = x^t + c_{t-1}x^{t-1} + \cdots + c_0$.
- Since $p$ divides $a_0 = b_0c_0$, $p$ divides at least one of these coefficients: without loss of generality, suppose $p|b_0$.
- Now let $b_i$ be the lowest-degree coefficient of $b(x)$ not divisible by $p$ (there must be one, since $b_s = 1$ is not divisible by $p$): then we have $a_i = b_0c_i + b_1c_{i-1} + \cdots + b_{i-1}c_1 + b_ic_0$.
- Since $p$ divides $a_i$ and also divides the terms $b_0c_i$, $b_1c_{i-1}$, ... , $b_{i-1}c_1$, it must divide $b_ic_0$. But since $p$ does not divide $b_i$, we see that $p$ divides $c_0$. But then $p$ divides both $b_0$ and $c_0$, meaning that $p^2$ divides $b_0c_0 = a_0$. This is a contradiction, so there cannot exist any such factorization of $q(x)$.
- Thus, $q(x)$ is irreducible in $\mathbb{Z}[x]$ hence $\mathbb{Q}[x]$ by Gauss.

# Factorization over $\mathbb{Q}$, X

By being sufficiently clever, one can also apply Eisenstein to polynomials it does not obviously apply to.

Example: Show that the polynomial $q(x) = x^4 + x^3 - 3x^2 + x + 7$ is irreducible in $\mathbb{Q}[x]$.

- Notice that $q(x-1) = x^4 - 3x^3 + 6x + 3$, and this polynomial is irreducible by Eisenstein's criterion with $p = 3$.
- It is then easy to see that any factorization of $q(x-1)$ would give a factorization of $q(x)$, and vice versa: therefore, the original polynomial $q(x)$ must also have been irreducible.

# Factorization over $\mathbb{Q}$, XI

We can also use calculations in $\mathbb{F}_p[x]$ to show that a polynomial is irreducible in $\mathbb{Z}[x]$.

- Specifically, if a polynomial factors in $\mathbb{Z}[x]$, then reducing the factorization modulo $p$ yields a factorization in $\mathbb{F}_p[x]$, as long as the degrees of the factors do not change.
- By taking the contrapositive of the observation above, we see that if $q(x)$ is irreducible in $\mathbb{F}_p[x]$ and has leading coefficient not divisible by $p$, then it must also be irreducible in $\mathbb{Z}[x]$ (and thus by Gauss's lemma, also in $\mathbb{Q}[x]$).

Example: Show $q = x^3 + 12x^2 + 27x + 345$ is irreducible in $\mathbb{Z}[x]$.

- Notice that $q(x) \equiv x^3 + x + 1$ modulo 2, and so $q$ has no roots modulo 2. Since $q$ has degree 3, this means $q$ is irreducible in $\mathbb{F}_2[x]$, and hence also in $\mathbb{Z}[x]$.

# Polynomial Modular Arithmetic, I

We now discuss polynomial modular arithmetic.

I will note that this is really just a special case of studying quotient rings (in this case, the quotients are by principal ideals). However, we will not really use many general facts about quotient rings, whereas we will frequently need to use polynomial modular arithmetic.

Thus, the goal here is to work everything out in explicit detail so that you are able to understand how all the computations work. (This will pay substantial dividends fairly soon.)

# Polynomial Modular Arithmetic, II

We start by defining congruence in the usual way:

**Definition**

*Let $F$ be a field. If $a, b, p \in F[x]$, we say that a is congruent to b modulo p, written $a \equiv b \pmod{p}$, if $p | (b - a)$.*

Examples:

- In $\mathbb{R}[x]$, it is true that $x^2 \equiv x$ modulo $x - 1$, because $x - 1$ divides $x^2 - x = x(x - 1)$.
- In $\mathbb{F}_2[x]$, it is true that $x^3 + x \equiv x + 1$ modulo $x^2 + x + 1$, as $(x^2 + x + 1)$ divides $(x^3 + x) - (x + 1) = (x + 1)(x^2 + x + 1)$.

# Polynomial Modular Arithmetic, III

The basic properties of modular congruences in $\mathbb{Z}$ extend to $F[x]$ with little or no change:

## Proposition (Modular Congruences)

*Let $F$ be a field. If $a, b, c, d, p \in F[x]$ and $p \neq 0$, then the following are true:*

1. $a \equiv a \pmod{p}$.
2. $a \equiv b \pmod{p}$ *if and only if* $b \equiv a \pmod{p}$.
3. *If* $a \equiv b \pmod{p}$ *and* $b \equiv c \pmod{p}$, *then* $a \equiv c \pmod{p}$.
4. *If* $a \equiv b \pmod{p}$ *and* $c \equiv d \pmod{p}$, *then* $a + c \equiv b + d \pmod{p}$.
5. *If* $a \equiv b \pmod{p}$ *and* $c \equiv d \pmod{p}$, *then* $ac \equiv bd \pmod{p}$.

Proof: Each of these is straightforward from the definition.

# Polynomial Modular Arithmetic, IV

Next, residue classes:

**Definition**

*If $a, r \in F[x]$, the residue class of a modulo r, denoted $\overline{a}$, is the set $S = \{a + dr \, : \, d \in F[x]\}$ of all elements in $F[x]$ congruent to a modulo r.*

Examples:

- The residue class of 1 modulo $x$ in $\mathbb{F}_2[x]$ is $\{1, 1 + x, 1 + x^2, 1 + x + x^2, 1 + x^3, \dots\}$.
- The residue class of 0 modulo $p$ in $F[x]$ is the set of multiples of $p$.

# Polynomial Modular Arithmetic, IV

Here are a few fundamental properties of residue classes:

**Proposition (Properties of Residue Classes)**

*Let $F$ be a field and suppose $p \in F[x]$ is nonzero. Then*

1. *If $a, b \in F[x]$, then $a \equiv b \pmod{p}$ if and only if $\overline{a} = \overline{b}$.*
2. *Two residue classes modulo $p$ are either disjoint or identical.*
3. *The residue classes modulo $p$ are precisely those of the form $\overline{r}$ where $\deg(r) < \deg(p)$.*

Proofs: These are the same as in $\mathbb{Z}$.

- (1) follows from the definition, and (2) follows from (1).
- (3) follows from the division algorithm: for any $a$ there exists a unique $r$ with $\deg(r) < \deg(p)$ such that $a = qm + r$ with $q \in F[x]$. Then $a \equiv r \pmod{p}$, and (3) follows from (2) and uniqueness of remainders.

# Polynomial Modular Arithmetic, V

If $F$ is an infinite field, then if $\deg(p) > 0$, there will always be infinitely many residue classes in $F[x]$ modulo $p(x)$.

- However, when $F$ is a finite field of cardinality $\#F$, then the residue classes are each represented by a unique polynomial in $F[x]$ of degree less than $\deg(p)$.
- Such a polynomial has exactly $\deg(p)$ coefficients (for the terms of degree 0, 1, ... , $\deg(p) - 1$), and each coefficient has $\#F$ possible choices: thus, there are precisely $(\#F)^{\deg(p)}$ residue classes modulo $p(x)$.
- <u>Example</u>: There are $2^2 = 4$ residue classes in $\mathbb{F}_2[x]$ modulo $x^2$, and they are $\overline{0}$, $\overline{1}$, $\overline{x}$, and $\overline{x+1}$.
- <u>Example</u>: There are $5^3 = 125$ residue classes in $\mathbb{F}_5[x]$ modulo $x^3 + 2x + 1$, and they are of the form $\overline{a + bx + cx^2}$ for $a, b, c \in \mathbb{F}_5$.

# Polynomial Modular Arithmetic, VI

## Definition

*If $F$ is a field and $p \in F[x]$ is nonzero, the set of residue classes modulo $p$ is denoted as $F[x]/p$ (read as "$F[x]$ modulo $p$").*

Like in $\mathbb{Z}/m\mathbb{Z}$, we have natural addition and multiplication operations in $F[x]/p$:

## Definition

*The addition operation in $\mathbb{Z}/m\mathbb{Z}$ is defined as $\overline{a} + \overline{b} = \overline{a+b}$, and the multiplication operation is defined as $\overline{a} \cdot \overline{b} = \overline{ab}$.*

# Polynomial Modular Arithmetic, VII

## Definition

*The addition operation in $\mathbb{Z}/m\mathbb{Z}$ is defined as $\overline{a} + \overline{b} = \overline{a+b}$, and the multiplication operation is defined as $\overline{a} \cdot \overline{b} = \overline{ab}$.*

- Just as in $\mathbb{Z}/m\mathbb{Z}$, we need to verify that these operations are well-defined; that is, if we choose different elements $a' \in \overline{a}$ and $b' \in \overline{b}$, the residue class of $a' + b'$ is the same as that of $a + b$, and similarly for the product.
- To see this, if $a' \in \overline{a}$ then $a' \equiv a \pmod{p}$, and similarly if $b' \in \overline{b}$ then $b' \equiv b \pmod{p}$.
- Then $a' + b' \equiv a + b \pmod{p}$, so $\overline{a' + b'} = \overline{a + b}$ by the properties of residue classes.
- Likewise, $a'b' \equiv ab \pmod{p}$, so $\overline{a'b'} = \overline{ab}$.
- Thus, the operations are well-defined.

# Polynomial Modular Arithmetic, VIII

## Proposition (Basic Arithmetic in $F[x]/p$)

*Let $F$ be a field and $p \in F[x]$ be nonzero. Then the following properties hold for residue classes in $F[x]/p$ :*

1. *$+$ is associative: $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$ for any $\overline{a}$, $\overline{b}$, and $\overline{c}$.*
2. *$+$ is commutative: $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ for any $\overline{a}$ and $\overline{b}$.*
3. *$\overline{0}$ is an additive identity: $\overline{a} + \overline{0} = \overline{a}$ for any $\overline{a}$.*
4. *Every $\overline{a}$ has an additive inverse $-\overline{a}$ satisfying $\overline{a} + (-\overline{a}) = \overline{0}$.*
5. *$\cdot$ is associative: $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$ for any $\overline{a}$, $\overline{b}$, and $\overline{c}$.*
6. *$\cdot$ is commutative: $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$ for any $\overline{a}$ and $\overline{b}$.*
7. *$\cdot$ distributes over $+$: $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$ for any $\overline{a}$, $\overline{b}$, $\overline{c}$.*
8. *$\overline{1}$ is a multiplicative identity: $\overline{1} \cdot \overline{a} = \overline{a}$ for any $\overline{a}$.*

Proof: All of these follow immediately from the corresponding properties of arithmetic in $F[x]$.

# Polynomial Modular Arithmetic, IX

Example: Here are tables for $\mathbb{F}_2[x]/p$ with $p = x^2 + x + 1$:

| $+$ | $0$ | $1$ | $x$ | $x+1$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $x$ | $x+1$ |
| $1$ | $1$ | $0$ | $x+1$ | $x$ |
| $x$ | $x$ | $x+1$ | $0$ | $1$ |
| $x+1$ | $x+1$ | $x$ | $1$ | $0$ |

| $\cdot$ | $0$ | $1$ | $x$ | $x+1$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $x$ | $x+1$ |
| $x$ | $0$ | $x$ | $x+1$ | $1$ |
| $x+1$ | $0$ | $x+1$ | $1$ | $x$ |

For example, $x + (x+1) = 2x + 1 = 1$ since $2 = 0$, and also $x \cdot (x+1) = x^2 + x \equiv (x+1) + x = 1$ since $x^2 \equiv x + 1$.

# Polynomial Modular Arithmetic, X

Here is the multiplication table for $\mathbb{F}_3[x]/r$ with $r = x^2 + 1$:

| $\cdot$ | $0$ | $1$ | $2$ | $x$ | $x+1$ | $x+2$ | $2x$ | $2x+1$ | $2x+2$ |
|---|---|---|---|---|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $2$ | $x$ | $x+1$ | $x+2$ | $2x$ | $2x+1$ | $2x+2$ |
| $2$ | $0$ | $2$ | $1$ | $2x$ | $2x+2$ | $2x+1$ | $x$ | $x+2$ | $x+1$ |
| $x$ | $0$ | $x$ | $2x$ | $2$ | $x+2$ | $2x+2$ | $1$ | $x+1$ | $2x+1$ |
| $x+1$ | $0$ | $x+1$ | $2x+2$ | $x+2$ | $2x$ | $1$ | $2x+1$ | $2$ | $x$ |
| $x+2$ | $0$ | $x+2$ | $2x+1$ | $2x+2$ | $1$ | $x$ | $x+1$ | $2x$ | $2$ |
| $2x$ | $0$ | $2x$ | $x$ | $1$ | $2x+1$ | $x+1$ | $2x+2$ | $2x+1$ | $x+2$ |
| $2x+1$ | $0$ | $2x+1$ | $x+2$ | $x+1$ | $2$ | $2x$ | $2x+2$ | $x$ | $1$ |
| $2x+2$ | $0$ | $2x+2$ | $x+1$ | $2x+1$ | $x$ | $2$ | $x+2$ | $1$ | $2x$ |

Notice that $\mathbb{F}_3[x]/r$ is a field, since every nonzero residue class is invertible. As we will show in a moment, this is because $p(x) = x^2 + 1$ is irreducible in $\mathbb{F}_3[x]$ (it has degree 2 but no roots).

# Polynomial Modular Arithmetic, XI

In analogy with the situation in $\mathbb{Z}/m\mathbb{Z}$, we can characterize the invertible elements in $F[x]/p$:

**Theorem (Invertible Elements in $F[x]/p$)**

*Let $F$ be a field and $p \in F[x]$ be nonzero. Then the residue class $\overline{r}$ in $F[x]/p$ has a multiplicative inverse if and only if $r$ and $p$ are relatively prime.*

Like with integers, we say two polynomials are relatively prime if 1 is a greatest common divisor.

# Polynomial Modular Arithmetic, XII

Proof:

- First suppose that $r$ and $p$ are relatively prime.
- Then by the Euclidean algorithm, we can write $1 = c_r r + c_p p$ for some polynomials $c_r, c_p$. Then $\overline{c_r} \cdot \overline{r} = \overline{1}$, meaning that $\overline{r}$ is invertible in $F[x]/p$.
- Conversely, suppose that $\overline{r}$ is invertible in $F[x]/p$ with multiplicative inverse $\overline{c_r}$.
- Then $\overline{c_r} \cdot \overline{r} = \overline{1}$ so that $c_r r \equiv 1 \pmod{p}$, meaning that there exists some polynomial $c_p$ with $c_r r + c_p p = 1$.
- But any common divisor of $r$ and $p$ must then divide $c_r r + c_p p = 1$, and thus we see that $r$ and $p$ are relatively prime.

We can use the argument here to compute multiplicative inverses when they exist. (This will be a useful computational tool later!)

# Polynomial Modular Arithmetic, XIII

Example: Find the inverse of $x^2+2$ in $\mathbb{F}_5[x]$ mod $x^3+1$.

- First we apply the Euclidean algorithm in $\mathbb{F}_5[x]$:

$$\begin{aligned} x^3+1 &= x\cdot(x^2+2)+(3x+1) \\ x^2+2 &= (2x+1)\cdot(3x+1)+1 \\ 3x+1 &= (3x+1)\cdot 1 \end{aligned}$$

  and so the gcd of $x^2+2$ and $x^3+1$ is 1.

- By back-solving, we obtain

$$\begin{aligned} 3x+1 &= (x^3+1)-x\cdot(x^2+2) \\ 1 &= (x^2+2)-(2x+1)(3x+1) \\ &= (2x^2+x+1)(x^2+2)-(2x+1)(x^3+1) \end{aligned}$$

  and thus by reducing modulo $x^3+1$, we see that the multiplicative inverse of $x^2+2$ is $2x^2+x+1$.

# Polynomial Modular Arithmetic, XIV

In analogy with the fact that $\mathbb{Z}/m\mathbb{Z}$ is a field precisely when $m$ is prime, we also see that $F[x]/p$ is a field precisely when $p$ is irreducible:

**Corollary**

*Let $F$ be a field and $p \in F[x]$ have positive degree. Then $F[x]/p$ is a field if and only if $p$ is irreducible.*

Proof:

- By the previous theorem, we see that if $p$ is irreducible then every nonzero residue class modulo $p$ is invertible. Furthermore, if $\deg(p) > 0$, then $\overline{1} \neq \overline{0}$, so $F[x]/p$ is a field.
- Inversely, if $p$ is reducible, then (again as above) there are non-invertible residue classes in $F[x]/p$, such as the irreducible factors of $p$.

# Polynomial Modular Arithmetic, XV

By finding irreducible polynomials in $\mathbb{F}_p[x]$, we can use the corollary above to construct additional finite fields. (After we develop more tools, we will be able to say much about finite fields.)

Example: Construct a finite field with 27 elements.

- Since $27 = 3^3$, we can construct a finite field with 27 elements as $\mathbb{F}_3[x]/p$ where $p$ is an irreducible polynomial of degree 3.
- One possible choice is the polynomial $p(x) = x^3 + 2x + 1$: it has no roots, since $p(0) = p(1) = p(2) = 1$, so (since it has degree 3) it is irreducible.
- Therefore, $\mathbb{F}_3[x]/p$ is a field with $3^3 = 27$ elements, as required.

# Rings, I

We now broaden our discussion from polynomials to general rings.

## Definition

*A ring is any set $R$ having two (closed) binary operations $+$ and $\cdot$ that satisfy the six axioms [R1]-[R6]:*

**[R1]** $+$ *is associative:* $a + (b + c) = (a + b) + c$ *for all* $a, b, c$ *in* $R$.

**[R2]** $+$ *is commutative:* $a + b = b + a$ *for all* $a, b$ *in* $R$.

**[R3]** *There is an additive identity 0 with* $a + 0 = a$ *for all* $a$ *in* $R$.

**[R4]** *Every* $a \in R$ *has an additive inverse* $-a$ *with* $a + (-a) = 0$.

**[R5]** $\cdot$ *is associative:* $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for all* $a, b, c$ *in* $R$.

**[R6]** $\cdot$ *distributes over* $+$: $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(a + b) \cdot c = a \cdot c + b \cdot c$ *for all* $a, b, c$ *in* $R$.

# Rings, II

Certain rings will also possess additional nice properties:

### Definition

*If a ring satisfies axiom [R7], we say it is a commutative ring.*

**[R7]** $\cdot$ *is commutative:* $a \cdot b = b \cdot a$ *for all* $a, b$ *in* $R$.

### Definition

*If a ring satisfies axiom [R8], we say it is a ring with identity.*

**[R8]** *There is a multiplicative identity* $1 \neq 0$ *with* $1 \cdot a = a = a \cdot 1$ *for all* $a$ *in* $R$.

### Definition

*If a ring with identity further satisfies the axiom [D], it is called a division ring. A commutative division ring is called a field.*

**[D]** *Every nonzero* $a$ *in* $R$ *has a multiplicative inverse* $a^{-1}$ *satisfying* $a \cdot a^{-1} = 1 = a^{-1} \cdot a$.

# Rings, III

If not specified, all operations are the obvious ones.

1. The integers $\mathbb{Z}$ are a commutative ring with identity.
2. The even integers are a commutative ring without identity.
   - The properties [R1]-[R7] all follow from their counterparts in $\mathbb{Z}$: [R3] follows because 0 is an even integer, and [R4] follows because $n$ is an even integer if and only if $-n$ is an even integer.
   - This ring does not have a multiplicative identity because there is no solution to $2n = 2$ inside the set of even integers.
3. The set of odd integers is not a ring.
   - The problem is that, although multiplication of two odd integers does return an odd integer, the sum of two odd integers is not odd: thus, the operation $+$ is not defined on the set of odd integers.

# Rings, IV

4. The set $\mathbb{Z}/m\mathbb{Z}$ of residue classes modulo $m$ form a commutative ring with identity.
   - Furthermore, if $p$ is a prime, we know that all of the nonzero residue classes modulo $p$ are invertible, meaning that $\mathbb{Z}/p\mathbb{Z}$ is a field.
   - Indeed, the only residue classes that are invertible modulo $m$ are those relatively prime to $m$, so if $m$ is not prime, then $\mathbb{Z}/m\mathbb{Z}$ is not a field.
5. The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are all examples of fields.
   - The elements of $\mathbb{C}$ are of the form $a + bi$, where $a$ and $b$ are real numbers and $i^2 = -1$, with operations $(a + bi) + (c + di) = (a + c) + (b + d)i$ and $(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$.

# Rings, V

6. If $F$ is a field, the set $F[x]$ of polynomials in $x$ with coefficients from $F$ forms a commutative ring with identity.
    - More generally, if $R$ is any ring, we can consider the ring $R[x]$ of polynomials with coefficients from $R$ (we have already implicitly done this when discussing polynomials with integer coefficients).
    - Warning: When $R$ is not commutative or has zero divisors, the polynomial ring $R[x]$ can have unintuitive properties.
7. The set of complex numbers of the form $a + bi$ where $a, b \in \mathbb{Z}$ are a commutative ring with identity.
    - This ring is denoted $\mathbb{Z}[i]$ (read as: "$\mathbb{Z}$ adjoin $i$") and is also often called the Gaussian integers.
    - [R1]-[R8] all follow from their counterparts in $\mathbb{C}$.

# Rings, VI

8. The set of real numbers of the form $a + b\sqrt{2}$ where $a, b \in \mathbb{Z}$ are a commutative ring with identity.
   - This ring is denoted $\mathbb{Z}[\sqrt{2}]$. The addition and multiplication are defined in a similar way as for the complex numbers and Gaussian integers: $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$, and $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2}$.
9. More generally, the complex numbers of the form $a + b\sqrt{D}$ for an arbitrary $D \in \mathbb{Z}$, is a commutative ring with identity.
   - This ring is denoted $\mathbb{Z}[\sqrt{D}]$.

# Rings, VI

10. If $S$ is any set and $A$ is any ring, the collection $R$ of functions $f : S \to A$, with operations $(f+g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x)g(x)$, forms a ring.
    - Thus, for example, if $A$ is the set of real numbers, with $f(x) = x^2$ and $g(x) = 3x^2$, then $(f+g)(x) = 4x^2$ and $(fg)(x) = 3x^4$.
    - Ultimately, each of the properties [R1]-[R6] follows from the corresponding property of $A$. The additive identity is the "identically-zero function" $0_S$ that is 0 on each element of $S$, and the additive inverse $-f$ of $f$ is defined as $(-f)(x) = -f(x)$ for each $x$ in $S$.
    - If $A$ is commutative, then it is easy to see that $R$ will also be commutative. Likewise, if $A$ has a 1, then the "identically-1 function" $1_S$ that is 1 on each element of $S$, is a multiplicative identity in $R$.

# Rings, VII

11. If $F$ is a field and $n \geq 2$, then the set of $n \times n$ matrices $M_{n\times n}(F)$ with entries from $F$, forms a noncommutative ring with identity.
    - The operations are the usual addition and multiplication of matrices. The zero element is the zero matrix while the multiplicative identity is the identity matrix $I_n$.
12. If $V$ is a vector space of dimension larger than 1, the set $\mathcal{L}(V, V)$ of linear transformations from $V$ to $V$ is a noncommutative ring with 1 under the operations of function addition and function composition: $(S+T)(\mathbf{v}) = S\mathbf{v} + T\mathbf{v}$ and $(ST)\mathbf{v} = S(T\mathbf{v})$.
    - After choosing a basis, this is really the same example as above.

# Rings, VIII

13. The set $\mathbb{H}$ of real quaternions $a + bi + cj + dk$, for real numbers $a, b, c, d$ and "imaginary units" $i, j, k$ satisfying the relations $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, and $ki = -ik = j$, form a noncommutative ring with identity.

    - This ring was first characterized by William Rowan Hamilton in 1843 (whence $\mathbb{H}$), and is one of the first examples of a noncommutative ring.
    - Addition works componentwise, so that $(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k$.
    - Multiplication is defined using the distributive law and the relations listed above, taking care to keep the terms in the proper order when multiplying. (The real number coefficients commute with $i$, $j$, and $k$.)

# Rings, IX

13. More about quaternions.

- Thus, for example, we have

$$\begin{aligned}(1+i-k)\cdot(2+3i+j) &= (1+i-k)\cdot 2+(1+i-k)\cdot 3i+(1+i-k)\cdot j\\ &= (2+2i-2k)+(3i-3-3j)+(j+k+i)\\ &= -1+6i-2j-k.\end{aligned}$$

- In fact, the real quaternions are a division ring: since $(a+bi+cj+dk)(a-bi-cj-dk)=a^2+b^2+c^2+d^2$, the nonzero quaternion $a+bi+cj+dk$ has a multiplicative inverse $\dfrac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$.
- The quaternions are related to 3-dimensional geometry (via cross products) and the units $\{\pm 1, \pm i, \pm j, \pm k\}$ also form the quaternion group $Q_8$.

# Rings, X

If we have a set with an addition operation, we can make it into a ring in a trivial way.

14. If $S$ is $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$, with $+$ taken to be normal addition, and $\cdot$ defined so that $a \cdot b = 0$ for every $a$ and $b$, then $S$ is a commutative ring.
    - All of the multiplicative axioms immediately reduce to the true statement $0 = 0$. Of course, this ring has no multiplicative identity.
15. The set $R = \{0\}$, with operations $0 + 0 = 0$ and $0 \cdot 0 = 0$, is a commutative ring.
    - All of the axioms follow trivially. In fact, this ring even has a multiplicative identity! (But it is not a ring with 1 because we require $1 \neq 0$.)
    - This ring is known as the trivial ring, and is the only ring where $1 = 0$.

# Basic Ring Properties, I

Here are a few basic properties of ring arithmetic:

- As in $\mathbb{Z}$, we define the binary operation of subtraction by setting $a - b = a + (-b)$. We also often use implicit multiplication, and drop the $\cdot$ notation.
- We can define scaling of a ring element $a$ by a positive integer as repeated addition: $na = \underbrace{a + a + a + \cdots + a}_{n \text{ terms}}$. By associativity of addition, this notation is well-defined. In a ring with 1, this notation coincides with the product of ring elements $n \cdot a$, but (as we would desire) it is true that $n \cdot a = na$.
- We can also define exponentiation of a ring element $a$ as $a^k = \underbrace{a \cdot a \cdot a \cdot \cdots \cdot a}_{k \text{ terms}}$, for any positive integer $k$. By associativity of multiplication, this notation is well-defined.

# Basic Ring Properties, II

## Proposition (Basic Arithmetic)

*Let $R$ be any ring. For any $a, b, c \in R$, the following hold:*

1. *The additive identity 0 is unique, as is the multiplicative identity 1 (if $R$ has a 1).*
2. *Addition has a cancellation law: if $a + b = a + c$ then $b = c$.*
3. *Additive inverses are unique.*
4. $0 \cdot a = 0 = a \cdot 0$, $-(-a) = a$, $(-1) \cdot a = -a = a \cdot (-1)$.
5. $-(a + b) = (-a) + (-b)$.
6. $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$, *and* $(-a) \cdot (-b) = a \cdot b$.
7. *For any positive integers $m$ and $n$ and any $a \in R$, $ma + na = (m + n)a$, $m(na) = (mn)a$, $a^{m+n} = a^m a^n$, and $a^{mn} = (a^m)^n$.*

Proofs: Straightforward from the ring axioms.

# Basic Ring Properties, III

An important property of $\mathbb{Z}$ that does *not* hold in general rings is the statement that $ab = 0$ implies $a = 0$ or $b = 0$. We already remarked on this during our discussion of $\mathbb{Z}/m\mathbb{Z}$ and $F[x]/p$.

## Definition

*In a ring $R$, we say that an element $a$ is a zero divisor if $a \neq 0$ and there exists a nonzero $b \in R$ such that $ab = 0$ or $ba = 0$. (Note in particular that 0 is not a zero divisor!)*

Examples:

- In $\mathbb{Z}/24\mathbb{Z}$, we have $\overline{3} \cdot \overline{8} = \overline{0}$ so $\overline{3}$ and $\overline{8}$ are zero divisors.
- In $\mathbb{F}_5[x]/(x^2 + x)$, we have the equality $\overline{x+1} \cdot \overline{x} = \overline{x^2 + x} = \overline{0}$, so $\overline{x+1}$ and $\overline{x}$ are zero divisors in $\mathbb{F}_5[x]/(x^2 + x)$.
- More generally, any polynomial not relatively prime to the modulus will be a zero divisor in $\mathbb{Z}/m\mathbb{Z}$ or $F[x]/p$.

# Basic Ring Properties, IV

In the opposite direction, it is also possible for a general ring to contain many elements that have multiplicative inverses (unlike in $\mathbb{Z}$, where the only elements with multiplicative inverses are $\pm 1$).

**Definition**

*In a ring $R$ with $1 \neq 0$, we say that an element $a$ is a unit if there exists a $b \in R$ such that $ab = 1 = ba$. The set of units in $R$ is denoted $R^\times$.*

Example:

- In $\mathbb{F}_5[x]/(x^2+x)$, we have $\overline{x+2} \cdot \overline{2x+3} = \overline{2x^2+7x+6} = \overline{1}$. Thus, $\overline{x+2}$ and $\overline{2x+3}$ are units in $\mathbb{F}_5[x]/(x^2+x)$.
- More generally, the units in $\mathbb{Z}/m\mathbb{Z}$ or $F[x]/p$ are the elements relatively prime to the modulus.

We remark that the set of units $R^\times$ is a group under multiplication.

# Basic Ring Properties, V

Examples:

1. In $\mathbb{Z}$, there are no zero divisors, and the units are $\pm 1$.
2. In $\mathbb{Z}/m\mathbb{Z}$, the units are the residue classes relatively prime to $m$, while the zero divisors are the nonzero classes having a nontrivial common divisor with $m$. In particular, every nonzero residue is either a unit or a zero divisor.
3. In a field, every nonzero element is a unit. Indeed, a commutative ring with 1 is a field precisely when every nonzero element is a unit.
4. In the ring $\mathbb{Z}[\sqrt{2}]$, the integers 1 and $-1$ are units, but the element $\sqrt{2}+1$ is also a unit, because $(\sqrt{2}+1)\cdot(\sqrt{2}-1) = 1$. Note that $\mathbb{Z}[\sqrt{2}]$ is not a field, however, because $\sqrt{2}$ is not a unit.

# Basic Ring Properties, VI

Here are a few basic properties of units and zero divisors:

**Proposition (Units and Zero Divisors)**

*Let $R$ be a ring with $1 \neq 0$.*

1. *The multiplicative inverse of a unit is unique.*
2. *The product of two units is a unit, as is the multiplicative inverse of a unit.*
3. *A unit can never be a zero divisor in $R$.*

Proofs:

1. The multiplicative inverse of a unit is unique.
    - If $a$ is a unit with $ab = 1 = ba$ and also $ac = 1 = ca$, then $b = b(ac) = (ba)c = c$.

# Basic Ring Properties, VII

Proofs (continued):

2. The product of two units is a unit, as is the multiplicative inverse of a unit.
   - If $a$ is a unit with $ab = 1 = ba$, then by definition $b$ is also a unit.
   - If $c$ is another unit with $cd = 1 = dc$, then $(ac)(db) = a(cd)b = a1b = ab = 1$ and likewise $(db)(ac) = 1$ as well, so the inverse of $ac$ is $db$.
3. A unit can never be a zero divisor in $R$.
   - Suppose $a$ is a unit and $xa = 0$ for some $x \neq 0$.
   - Then by assumption, there is a $b$ such that $ab = 1$, so then $x = x(ab) = (xa)b = 0b = 0$, contradicting the assumption that $x \neq 0$.
   - In the same way, if $ax = 0$ for some $x \neq 0$, then if $ba = 1$ then $x = (ba)x = b(ax) = b0 = 0$, again a contradiction.

# Basic Ring Properties, VIII

We give a special name to the class of commutative rings having no zero divisors, attesting to their similarity to $\mathbb{Z}$:

**Definition**

*A commutative ring with* $1 \neq 0$ *having no zero divisors is called an* *integral domain* *(or often, just a "domain"). Equivalently,* $R$ *is an integral domain if* $R$ *is commutative with* $1 \neq 0$*, and where* $ab = 0$ *implies* $a = 0$ *or* $b = 0$*.*

Examples:

- The integers are an integral domain, as is any field.
- More generally, any ring that is a subset of a field (such as the Gaussian integers $\mathbb{Z}[i]$) is an integral domain.
- In fact, the converse is also true: any integral domain $R$ arises naturally as a subset of its field of fractions $F$, which is constructed from $R$ in the same way $\mathbb{Q}$ is constructed from $\mathbb{Z}$.

# Basic Ring Properties, IX

Integral domains possess various fundamental properties:

**Proposition (Cancellation in Domains)**

*Suppose $R$ is an integral domain. Then multiplication in $R$ has a cancellation law: if $a \neq 0$ and $ab = ac$, $b = c$.*

Proof:

- Suppose that $ab = ac$: then $a(b - c) = 0$, so since $R$ is a domain we either have $a = 0$ or $b - c = 0$. Thus, if $a \neq 0$, we have $b - c = 0$ so that $b = c$.

# Basic Ring Properties, IX

**Corollary**

*If $R$ is a finite integral domain, then $R$ is a field.*

Proof:

- Let $a$ be any nonzero element of $R$, and consider the set $\{a, a^2, a^3, \dots, a^n, \dots\}$. Since $R$ is finite, two of the elements of this set must be equal: say $a^j = a^{j+k}$ for some positive integers $j$ and $k$.
- Then $a^j = a^{j+k}$ implies $a^j(a^k - 1) = 0$, and then since $a \neq 0$, we see $a^j \neq 0$. Thus, $a^k - 1 = 0$, so that $a \cdot a^{k-1} = 1$, meaning that $a^{k-1}$ is the multiplicative inverse of $a$.

# Subrings, I

Next, subsets of rings that themselves are rings:

**Definition**

*If $R$ is a ring, we say a subset $S$ of $R$ is a subring if it also possesses the structure of a ring, under the same operations as $R$.*

Most of the ring axioms are inherited from $R$, and we can condense the other verifications as follows:

**Proposition (Subring Criterion)**

*A subset $S$ of $R$ is a subring if only if $S$ contains the zero element of $R$ and, for any $a, b \in S$, the elements $a - b$ and $ab$ are also in $S$.*

Proof: Straightforward from the definition.

Using the subring criterion, we can construct more rings.

# Subrings, II

Examples:

1. $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$, which is a subring of $\mathbb{C}$, which is a subring of $\mathbb{H}$.
2. The trivial ring $\{0\}$ is a subring of any ring.
3. The multiples of $n$, denoted $n\mathbb{Z}$ are a subring of $\mathbb{Z}$. Indeed, these are all the subrings of $\mathbb{Z}$, as follows by the division algorithm and well-ordering principle.
4. The set of rational numbers having denominator equal to a power of 2 (i.e., that are of the form $n/2^k$ for an integer $n$ and nonnegative integer $k$), forms a subring of $\mathbb{Q}$.
5. The set of upper-triangular $n \times n$ matrices is a subring of $M_{n\times n}(F)$.
6. The set of differentiable real-valued functions is a subring of the ring of continuous real-valued functions, which is in turn a subring of the ring of all real-valued functions.

# Cartesian Products

We can also construct new rings using Cartesian products.

**Proposition (Cartesian Products of Rings)**

*If $A$ and $B$ are rings, then the Cartesian product $A \times B$ is also a ring, with operations performed componentwise:*
$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$ *and*
$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$.

Proof: Straightforward from the definition.

- This ring $A \times B$ is called the direct product. We can also generalize this definition to direct products and direct sums over arbitrary indexing sets.
- Note that if $A$ and $B$ are commutative, then so is $A \times B$; likewise, if $A$ and $B$ have a 1, then $(1_A, 1_B)$ is the multiplicative identity in $A \times B$.

# Ideals, I

Our next task is to generalize the idea of modular arithmetic into general rings.

- In $\mathbb{Z}$ and $F[x]$, we defined modular congruences using divisibility, but let us take a broader approach: if $I$ is a subset of $R$ (whose properties we intend to characterize in a moment) let us say that two elements $a, b \in R$ are "congruent modulo $I$" if $a - b \in I$.
- We would like "congruence modulo $I$" to be an equivalence relation: this requires $a \equiv a \pmod{I}$, $a \equiv b \pmod{I}$ implies $b \equiv a \pmod{I}$, and $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$ implies $a \equiv c \pmod{I}$.
- It is easy to see that these three conditions require $0 \in I$, that $I$ be closed under additive inverses, and that $I$ be closed under addition. (Thus, $I$ is in fact closed under subtraction.)

# Ideals, II

We also want congruences to respect addition and multiplication.

- If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then we want $a + c \equiv b + d \pmod{I}$ and $ac \equiv bd \pmod{I}$.
- In terms of ring elements, this is equivalent to the following: if $b = a + r$ and $d = c + s$ for some $r, s \in I$, then we want $(b + d) - (a + c) = r + s$ to be in $I$, and we also want $bd - ac = (a + r)(c + s) - ac = as + rc + rs$ to be in $I$.
- The first condition clearly follows from the requirement that $I$ is closed under addition. It is a bit less obvious how to handle the second condition, but one immediate implication follows by setting $a = c = 0$: namely, that $rs \in I$.
- Thus, $I$ must be closed under $\cdot$, so it must be a subring.
- But more is needed: since $0 \in I$, we can set $r = 0$ to see that $as \in I$, and we can also set $s = 0$ to see that $rc \in I$.

# Ideals, III

- So in fact, $I$ must be closed under (left and right) multiplication by *arbitrary* elements of $R$, in addition to being a subring. It is then easy to see that this condition is also sufficient to ensure that $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$ imply $a + c \equiv b + d \pmod{I}$ and $ac \equiv bd \pmod{I}$.
- Our last task is to define residue classes and then the ring operations: we define the residue class $\overline{a}$ (modulo $I$) to be the set of ring elements $b$ congruent to $a$ modulo $I$, which is to say, $\overline{a} = \{a + r \,:\, r \in I\}$.
- Then we take the operations on residue classes to be $\overline{a} + \overline{b} = \overline{a + b}$ and $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$, and by properties of congruences, these operations will be well-defined and the collection of residue classes will form a ring.

# Ideals, IV

Now we just have to run through the discussion more formally:

**Definition**

*A subset $I$ of a ring $R$ that is closed under arbitrary left and right multiplication by elements of $R$ is called an ideal of $R$ (or, for emphasis, a two-sided ideal).*

- Explicitly, $I$ is an ideal if $I$ contains 0 and for any $x, y \in I$ and any $r \in R$, the elements $x - y$, $rx$, and $xr$ are all in $I$.
- There are one-sided notions of ideals as well: a left ideal is closed under arbitrary left multiplication, while a right ideal is closed under arbitrary right multiplication.
- If $R$ is commutative, then left ideals, right ideals, and two-sided ideals are the same.

# Ideals, V

Examples:

1. The subrings $n\mathbb{Z}$ are ideals of $\mathbb{Z}$, since they are clearly closed under arbitrary multiplication by elements of $\mathbb{Z}$.
2. If $R = F[x]$ and $p$ is any polynomial, the subring $pR$ of multiples of $p$ is an ideal of $F[x]$, since it is closed under arbitrary multiplication by polynomials in $F[x]$.
3. The subring $\mathbb{Z}$ of $\mathbb{Q}$ is not an ideal of $\mathbb{Q}$, since it is not closed under arbitrary multiplication by elements of $\mathbb{Q}$, since for example if we take $r = \frac{1}{3} \in \mathbb{Q}$ and $x = 4 \in \mathbb{Z}$, the element $rx = \frac{4}{3}$ is not in $\mathbb{Z}$.
4. For any ring $R$, the subrings $\{0\}$ and $R$ are ideals of $R$. We refer to $\{0\}$ as the trivial ideal (or the "zero ideal") and refer to any ideal $I \neq R$ as a proper ideal (since it is a proper subset of $R$).

# Ideals, V

Examples:

5. In the ring $R = \mathbb{Z}[x]$, the set $S$ of polynomials with even constant term is an ideal of $R$. It is not hard to see that $0 \in S$, that $S$ is closed under subtraction, and that the product of any polynomial with an element of $S$ also has even constant term, so $S$ is closed under arbitrary $R$-multiplication.
6. The set $S = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ of "even" residue classes is an ideal of $\mathbb{Z}/8\mathbb{Z}$. It is not hard to verify that this set is closed under subtraction and arbitrary $R$-multiplication.
7. The set $S = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ is not an ideal of $\mathbb{Z}/7\mathbb{Z}$ since it is not closed under addition. (The problem is that 7 is odd.)
8. The set $S = \{(2a, 3a) : a \in \mathbb{Z}\}$ is not an ideal of $\mathbb{Z} \times \mathbb{Z}$: although it is a subring, it is not closed under arbitrary $R$-multiplication since for example $(1, 2) \cdot (2, 3) = (2, 6)$ is not in $S$, even though $(2, 3)$ is.

# Ideals, VI

## Proposition (Principal Ideals)

*If $R$ is a commutative ring with 1, the set $(a) = \{ra : r \in R\}$ of all $R$-multiples of $a$ forms a (two-sided) ideal of $R$, known as the principal ideal generated by $a$.*

Proof:

- Since $0a = 0$ we see $0 \in (a)$. Furthermore, since $ra - sa = (r - s)a$ we see that $(a)$ is closed under subtraction.
- Furthermore, if $t \in R$ then we have $t(ra) = (tr)a$, so since $R$ is commutative, $(a)$ is closed under multiplication by arbitrary elements of $R$. Thus, $(a)$ is an ideal.

We will remark that in any Euclidean domain (like $\mathbb{Z}$ or $F[x]$), every ideal is principal (an element of minimum norm will generate the ideal).

# Summary

We discussed polynomial modular arithmetic.

We discussed rings, examples of rings, basic properties of rings, subrings, and ideals.

Next lecture: Quotient rings, isomorphisms, homomorphisms, the isomorphism theorems.