......

# Summaries, March 12 and 15

## March 12

### Factoring.

When discussing factoring in a ring $R$, we always assume that that $R$ is a domain: $ab = 0$ only if $a = 0$ or $b = 0$. We also discuss only nonzero elements. So to avoid endless repetition ofthe word 'nonzero' we adopt the convention that we are always speaking of nonzero elements.

The basic terminology is as follows:

A *unit* is an element of $R$ that has a multiplicative inverse.

If $a$ and $b$ are elements of $R$, then $a$ *divides* $b$ if $b = ra$ for some $r$ in $R$.

Two elements $a$ and $b$ of $R$ are *associates* if $a$ divides $b$ and also $b$ divides $a$. This happens when $b = ua$ for some unit $u$.

A *proper factorization* of an element $a$ is an equation $a = bc$, where neither $b$ nor $c$ is a unit.

An element $a$ is *irreducible* if it is not a unit, and if it has no proper factorization.

A *prime element* $p$ is an elementvsuch that, whenever $p$ idvides a product $ab$, it divides one of the factors $a$ or $b$.

### Greatest Common Divisor.

First, the ring $\mathbb{Z}$ of integers. This ring is a principal ideal domain: Every ideal of $\mathbb{Z}$ is principal.

Let $a$ and $b$ be integers. The sum of the two principal ideals $a\mathbb{Z}$ and $b\mathbb{Z}$ is an ideal, so it has the form $d\mathbb{Z}$ for some integer $d$:

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

. The element $d$ is determined up to unit factor.

This displayed equation has the following consequences:

$d$ divides $a$ and $b$, because $a$ and $b$ are in $d\mathbb{Z}$.

(*) There are integers $r$ and $s$ such that $d = ra + sb$. This is true because $d$ is in the sum $a\mathbb{Z} + b\mathbb{Z}$.

It follows that, if an integer $e$ divides both $a$ and $b$, then $e$ divides $d$.

The conclusion marked with * is very powerful. One should always try to apply it.

One very important case is that $a$ and $b$ have no common divisors except units. In that case one says that their greatest common divisor is 1, and we can write $1 = ra + sb$ for suitable $r$ and $s$ in $R$.

**Proposition.** Let $R$ be a domain.
**(i)** A prime element of $R$ is irreducible.
**(ii)** If $R$ is a principal ideal domain, then an irreducible element of $R$ is a prime element.

**proof (i)** Let $p$ be a prime element. We must show that $p$ has no proper factorization. Sy that $p = ab$. Since $p$ is prime, 4=it divides one of the factors. Say that $p \,|\, a$, so $a = pq$ for some $q$. Then $p = ab = pqb$. Therefore $qb = 1$, $b$ is a unit, and the factorization wasn't proper.

**(ii)** For this proof, we restate the hypothesis that an element $q$ of $R$ is irreducible in terms of principal ideals. If $a$ is an element of $R$, we denote the principal ideal $Ra$ by $(a)$. If $a$ is a proper divisor of another element $q$, then $(q) < (a)$. The inclusion $(q) \subset (a)$ follows from the hypothesis that $a$ divides $q$, which shows that $q \in (a)$. And, if $(q) = (a)$, then $q$ and $a$ are associates, so the $a$ isn't a proper divisor of $q$. Therefore, an element $q$ is irreducible if and only if $(q) < (1)$ but there is no element $a$ such that $(q) < (a) < (1)$.

Suppose that an irreducible element $q$ divides a product $ab$: $\quad ab = qr$ for some $r$. Since $q$ is irreducible, it has no proper divisor. So if $q$ doesn't divide $a$, then $q$ and $a$ have no common divisors except units. Their greatest common divisor is 1, and therefore we can write $1 = ra + sq$ for some $r$ and $s$. Multiplying by $b$, $b = rab + sqb$. Here $q$ ivides the right side of this equation, and therefore $q$ divides $b$.

Unique Factorization Domains.

It is nearly true that a domain $R$ has unique factorization into irreducible elements if and only if every irreducible element is a prime element. The only thing missing is that one needs to know that factoring into irreducible elements is possible.

To factor an element $z$, not a unit, one looks for a proper factor. If there is no such factor, then $z$ is irreducible. If there is, one has a proper factorization $z = ab$. Then one continues, looking for proper factors of $a$ and $b$, etc... It is usually clar tht this process can't be continued indefinitely.

Assume that very irreducible element is prime and that factoring is possible. We look at two factorizations of an element $z$ into irreducible elements, say $z = p_1 \cdots p_r$ and $z = q_1 \cdots q_n$. Since $p_1$ is irreducible, it is a prime element. Then since $p_1$ divids $z = q_1 \cdots q_n$, $p_1$ divides one of the factors $q_i$. Since $q_i$ is irreducible, it has no proper factor, so $p_1$ is an associate of $q_i$ : $q_i = up_1$ for some unit $u$. We cancel $p_1$ from both factorizations, moving the unit $u$ to another factor $q_j$. Then we use induction.

**Fatoring in the ring $\mathbb{Z}[x]$ of integer polynomials** (polynomials with integer coefficients)

The ring $\mathbb{Z}[x]$ isn't a principal ideal domain, but it does have unique factorization.

The main tools for studying this ring are:

the inclusion $\mathbb{Z}[x] \subset \mathbb{Q}[x]$, and

the homomorphisms $\mathbb{Z}[x] \overset{\psi_p}{\mathbb{F}}_p\ [x]$.

A polynomial $f() = a_n x^n + \cdots + a_0$ with rational coefficients $a_i$, an element of $\mathbb{Q}[x]$ is *primitive* if it has positive degree, $n > 0$, its leading coefficient $a_n$ is positive, it is an element of $\mathbb{Z}[x]$, i.e., the coefficients $a_i$ are integers, and the greatest common divisor of the coefficients $a_i$ is 1. For instance, $3x^2 + 5x + 8$ is a primitive polynomial.

**Lemma 1.** A polynomial $f(x)$ with integer coefficients nd positive leading coefficient is primitive if and only if it isn't in the kernel of $\psi_p$ for any prime $p$.

**Lemma 2.** Let $f(x)$ be a polynomial with rational coefficients, $f \in \mathbb{Q}[x]$. Then $f(x) = cf_0(x)$ with $c \in \mathbb{Q}$ and $f_0$ primitive. This expression for $f$ is unique. If $f$ has integer coefficients, then $c$ is an integer.

**Gauss Lemma.** The product $fg$ of primitive polynomials $f$ and $g$ is primitive.

**proof.** If $f$ and $g$ are primitive, then their images $\overline{f}$ and $\overline{g}$ in $\mathbb{F}_p[x]$ are not zero for any prime $p$. If so, then because $\mathbb{F}_p[x]$ is a domain, $\overline{f}\overline{g}$ isn't zero either. so $fg$ is primitive. $\square$

Isn't this a nice proof?

**Lemma 3.** Let $f_0$ and $g$ we polynomials in $\mathbb{Z}[x]$, with $f_0$ primitive. If $f_0$ divides $g$ in $\mathbb{Q}[x]$, sy $g = f_0 q$ then $q$ is in $\mathbb{Z}[x]$, and therefore $f_0$ divides $g$ in $\mathbb{Z}[x]$.

**proof** Say that $g = f_0 q$ in $\mathbb{Q}[x]$. Applying Lemma 2, we write $g = cg_0$ and $q = dq_0$ where $g_0$ and $q_0$ are primitive, $c \in \mathbb{Z}$, and $d \in bbq$. Then $cg_0 = df_0 q_0$, and $f_0 q_0$ is primitive. Since the expression $g = cg_0$ is unique, $c = d$ and $g_0 = f_0 q_0$. Then $d$ is an integer, and so $q = dq_+0$ is in $\mathbb{Z}[x]$. $\square$

**Proposition.** The irreducible elements of $\mathbb{Z}[x]$ with positive leading coefficient are: the prime integers $p$, and the primitive polynomials $f$ that are irreducible in $\mathbb{Q}[x]$. Moreover, these are prime elements of $\mathbb{Z}[x]$. Therefore $\mathbb{Z}[x]$ has unique factorization into irreducible (prime) elements.

**proof** Let $f$ be an irreducible element of $\mathbb{Z}[x]$. Let's suppose that $f$ isn't a constant. When we write $f = cf_0$, we must have $c = \pm 1$. Otherwise $f$ isn't irreducible. So $f = \pm f_0$. We may assume that $f = f_0$ is primitive.

To show that $f_0$ is a prime element of$\mathbb{Z}[x]$, we suppose that $f_0$ divides a product $gh$ in $\mathbb{Z}[x]$. We write $g = cg_0$ and $h = dh_0$ with $g_0, h_0$ primitive. Then since $f_0$ is assumed irreducible in the principal ideal domain $\mathbb{Q}[x]$, $f_0$ divides one of the factors, say $f_0$ divides $g_0$, in $\mathbb{Q}[x]$. By Lemma 3, $f_0$ divides $g_0$ in $\mathbb{Z}[x]$. $\square$

**March 15**

**Gauss Primes.**

We have seen that the ring $\mathbb{Z}[i]$of Gauss integers is a principal ideal domain and therefore a unique factorization domain. Here we describe the irreducible (or prime) elements of $\mathbb{Z}[i]$. They are called the *Gauss primes*.

A prime integer may be an irreducible element of $\mathbb{Z}[x]$, a Gauss prime, or not. The prime 3 is irreducible, as is seen by looking for a proper divisor. The only Gauss integers $\alpha$ with absolute value $< 3$ are associates of $1+i$. They don't divide 3. Instead, $(i+i)(i-i) = 2$. So 2 is not a Gauss prime. Similarly, $5 = (2+i)(2-i)$. The factors $1 \pm i$ and $2 \pm i$ are Gauss primes.

**Lemma 1.** Let $p$ be a prime different from 2, and let $G$ be the multiplicative group of nonzero elements of the field $\mathbb{F}_p$ of integers modulo $p$, which has order $p - 1$.
**(i)** $G$ contains an element of order 4 if and only if $p \equiv 1$ modulo 4.
**(ii)** The residue $\overline{a}$ of an integer $a$ in $G$ is an element of order 4 if and only if $a^2 \equiv -1$ modulo $p$. If so, then $\overline{a}^2 = -1$.

**proof (i)** We inspect the homomorphism $G \xrightarrow{\varphi} G$ defined by $\varphi(\overline{a}) = \overline{a}^2$. Its kernel is $\{\pm 1\}$ and its image $H$ has order $(p-1)/2$. This subgroup contains 1, and the elements $\overline{a}$ distinct from $\pm 1$ can be paired with their inverses. So $H$ contains $-1$ if and only if its order is even, $(p-1)/2 = 2n$. This is true if and only if $p - 1 = 4n$ and therefore $p \equiv 1$ modulo 4. $\square$

**Lemma 2.** An integer prime $p$ is either a Gauss prime or a product a product $\overline{\pi}\pi$ of a Gauss prime and its conjugate.

**proof** If $\alpha = a + bi$ is a Gauss integer ($a, b \in \mathbb{Z}$), then $\overline{\alpha}\alpha = a^2 + b^2$ is an integer.

We factor $p$ into Gauss primes in the ring $\mathbb{Z}[i]$, say $p = \pi_1 \cdots \pi_k$. Then $p^2 = \overline{p}p$ is the product of the integers $(\overline{\pi}_1\pi_1), ..., (\overline{\pi}_k\pi_k)$. Since $\mathbb{Z}$ is a unique factorization domain, $k \leq 2$. If $k = 2$, then $p = \overline{\pi}_1\overline{\pi}_1$, and if $k = 1$, then $p$ is an associate of $\pi$, and is a Gauss prime. $\square$

The next theorem describes the Gauss primes.

**Theorem.** Let $p$ be an odd prime integer. The following are equvalent:

**1.** There is a Gauss prime $\pi$ such that $p = \overline{\pi}\pi$.

**2.** $p$ is the sum of two integer squares: $p = a^2 + b^2$.

**3.** $p$ is congruent 1 modulo 4: $p = 5, 13, 17, ....$

**4.** The residue of $-1$ modulo $p$ is a square.

**proof 1. $\Leftrightarrow$ 2.**This is rather trivial. If $p = \overline{\pi}\pi$ and $\pi = a + bi$, then $\overline{\pi}\pi = (a - bi)(a + bi) = a^2 + b^2$.

**1. $\Leftrightarrow$ 4.** This is the most interesting part of the theorem because, a priori, these two conditions don't seem related.

We show that a prime integer $p$ is a Gauss prime if and only if the residue of $-1$ is not a square in the field $\mathbb{F}_p$ of integers modulo $p$. The ring $\mathbb{Z}[i]$ of Gauss integers can be obtained from the ring of integers $\mathbb{Z}$ by adjoining an element $i$ with the relation $i^2 + 1 = 0$. So as explained last time, $\mathbb{Z}[i]$ is isomorphic to the quotient ring $\mathbb{Z}[x]/Q$ of the integer polynomial ring, where $Q$ is the principal ideal of $\mathbb{Z}[x]$ generated by $x^2 + 1$.

Next, $p$ is a Gauss prime if and only if it generates a prime ideal of the ring $\mathbb{Z}[i]$ of Gauss integers. Let $\overline{R}$ denote the quotient ring $\mathbb{Z}[i]/p\mathbb{Z}[i]$.

The ring $\overline{R}$ has finite order $p^2$. Its elements are the residues of the cosets that contain $n$ or $ni$, with $n = 0, ., ..., p-1$. If $p$ generates a prime ideal, then $\overline{R}$ is a domain. A finite domain is a field. So if $p$ generates a prime ideal of $\mathbb{Z}[i]$, then $\overline{R}$ is a field.

Now, $\overline{R}$ is obtained from the integer polynomial ring $\mathbb{Z}[x]$ by killing $x^2 + 1$, and then killing $p$. It is the quotient $\mathbb{Z}[x]/I$, where $I$ is the ideal generated by the two elements $x^2 + 1$ and $p$. Moreover, we can just as well start by killing $p$ in $\mathbb{Z}[x]$ first, then killing the residue of $x^2 + 1$. Killing $p$ in $\mathbb{Z}[x]$ produces the ring $\mathbb{F}_p[x]$ of polynomials with coefficients modulo $p$.

The two procedures of killing elements in succession are summed up in this diagram:

$$\begin{tikzcd}
\mathbb{Z}[x] \arrow[r, "a"] \arrow[d, "b"'] & \mathbb{Z}[i] \arrow[d, "c'"] \\
\mathbb{F}_p[x] \arrow[r, "a'"] & \overline{R}
\end{tikzcd}$$

where $b$ and $b'$ stand for for killing $p$ in $bbz[x]$ and in $\mathbb{Z}[i]$, and $a$ and $a'$ stand for killing $x^2+1$ in $\mathbb{Z}[x]$ and in $\mathbb{F}_p[x]$.

Therefore $\overline{R}$ is a field if and only if $p$ is an irreducible element of $\mathbb{Z}[i]$, and also if and only if $x^2+1$ is an irreducible element of $\mathbb{F}_p[x]$. And, $x^2+1$ is irreducible in $\mathbb{F}_p$ if and only if it has no root, which means that $-1$ is not a square in $\mathbb{F}_p$. This shows that **1.** and **4.** are equivalent.

**3.** $\Leftrightarrow$ **4.**: Let $G$ be the group of $p-1$ nonzero elements in $\mathbb{F}_p$, as before. We consider the homomorphism $G \xrightarrow{sq} G$ that sends an element $\alpha$ to $\alpha^2$. Its kernel is $\{\pm 1\}$, so its image $H$ has order $(p-1)/2$. In $H$ we can pair the elements that aren't equal to $\pm 1$ with their inverses. So the number of such elements is even. We also have the identity element 1. So, if the order $|H|$ of $H$ is odd, $-1$ cannot be in $H$, while if $|H|$ is even, $-1$ must be in $H$. And, if $-1$ is in $H$, there is an element $\alpha$ in $G$ whose square is $-1$. Then $-1$ is a square in $\mathbb{F}_p$. Since the order of $H$ is $(p-1)/2$, this happens if and only if $p \equiv 1$ modulo $4$. Therefore **3.** and **4.** are equivalent. This completes the proof of the theorem. $\square$

**Factoring Polynomials.**

We consider the problem of factoring a given polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

with rational coefficients.

First, we may as well clear the denominators. So we can suppose that $f$ has integer coefficients. The cost of doing this is that, whereas with rational coefficients we aan assume that $f$ is *monic*, i.e., that $a_n = 1$, we can't do this if we want integer coefficients. However, if a polynomial

$$g(x) = b_r x^r + \cdots + b_0$$

divides $f$ in $\mathbb{Q}[x]$, then if we make it primitive, the quotient will have integer coefficients too. This was discussed before. So at the cost of working with nonmonic polynomials, we can stay with integers.

(Recall that $g$ is primitive if $b_i$ are integers for all $i$, they have no common divisor, and $b_r$ is positive.)

The simplest case is that $g$ has degree 1, $g = b_1 x + b_0$. Then if $g$ divides $f$, $b_1$ divides $a_n$ and $b_0$ divides $a_0$. Since $a_n$ and $a_0$ have finitely many intger divisors, there are finitely many linear polynomials to check for dividing $f$. Of course we prefer not to do such a check.

It is harder to decide if $f$ has a divisor $g$ of degree 2.

**Reduction modulo $p$**

The homomorphism $\mathbb{Z}[x] \xrightarrow{\pi} \mathbb{F}_p[x]$, $p$ a prime integer, is a useful tool for studying divisibility. We denote the image $\pi(f)$ by $\overline{f}$ as usual:

$$\overline{f}(x) = \overline{a}_n x^n + \cdots + \overline{a}_0$$

If $f$ factors, $f = gh$, then $\overline{f} = \overline{g}\overline{h}$, and provided that $p$ doesn't divide the leading coefficient $a_n$ of $f$, $\overline{g}$ and $\overline{h}$ will have the same degrees as $g$ and $h$, respectively. So if we factor $\overline{f}$, we will, among other things, know the degrees of possible factors of $f$. This is helpful because there are finitely many polynomials of a given degree in $\mathbb{F}_p[x]$, so factoring of $\overline{f}$ can be done in finitely many steps.

The simplest application is to show that a polynomial $f$ is irreducible. If we suspect that $f$ is irreducible, we can reduce modulo som prime $p$. If $\overline{f}$ turns out to be irreducible, then we will have proved that $f$ is irreducible.

Let's take the prime $p = 2$. There are two rules making computation modulo 2 particularly simple. Let $R$ be a ring $R$ of characteristi 2, i.e., in which $1+1=0$. Then, first, if $a$ is in $R$, then, then $a+a = a(1+1) = 0$, so $a = -a$. This means that we can bring an element $a$ that a;ppears on one side of any equation to the other side without changing it. Second, if $a$ and $b$ are in $R$, then $(a+b)^2 = a^2 + b^2$ becauseth cross term $2ab$ is zero.

OK: Let's list the irrducible polynomials in $\mathbb{F}_2[x]$. First, in degree 1 there are two polynmials $x$ and $x+1$, and obviously, both are irreducible. We use the "sieve method" to find the irrducible polynomials of degree 2. The polynomials of degree 2 are:

$$x^2, x^2+x, x^2+1, x^2+x+1$$

The first two have 0 as root, and not irreducible. The third one $x^2+1$ has root 1, also not irreducible. The last one, $x^2+x+1$ doesn't have 0 or 1 as root. it is the only irreducible polynomial of degree 2.

We see here two necessary conditions that a polynomial must satisfy in order to be irreducible: The constant coefficient must be 1. If it is 0, then 0 is a root, and there must be an odd number of monomials with coefficient 1. If the number of those monomials is even, then 1 is a root.

Any reducible polynomial of degree 5 or less must have a linear factor or an irreducible quadratic factor. If it is made up of an odd number of monomials including 1 and is irreducible, it must be divisible by $x^2+x+1$. And it isn't hard to check divibility by that polynomial.

One way to can make that check easily is to look at the quotient ring $K = \mathbb{F}_2[x]/I$, where $I$ is the principal ideal generated by $g = x^2+x+1$. Since $g$ has degree 2, the residues of $0, 1, x, x^2$ form a basis for $K$, which is therefore a vector space of dimension 4 over the field $\mathbb{F}_2$. Let's use the same notation $0, 1, x, x^2$ forthe residues. Since the residue of $x^2+x+1$ is zero, $x^2 = x+1$ in $K$. Since $g$ is irreducible, $K$ is a finite domain, and therefore a field. The multiplicative group $K^\times$ of nonzeo elements of $K$ has order 3. It is a cyclic group. generated by any element different from 1, for example by $x$ (more precisely, its residue). Then the powers of $x$ run through the group $K^\times$:

$$1, x, x^2 = x+1, x^3 = 1, x^4 = x, x^5 = x+1, ...$$

Now to check whether a polynmial such as $f = x^5 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, we look at its residue $\overline{f}$ in $\mathbb{F}_2[x]/I$. Working modulo $g$, we substitute the values of the powers, obtaining $\overline{f} = (x{+}1) + 1 + (x{+}1) + x + 1$. We cancel pairs of $x$s and pairs of 1s, and are left with $x$. Therefore $\overline{f}$ isn't zero and $f$ isn't divisible by $x^2+x+1$. Since it has an odd number of terms and 1 appears, $f$ is an irreducible element of $\mathbb{F}_2[x]$. Of course, there are otherways to do this.

**the Eisenstein Criterion**

It is easiest to understand this by going through an example. Let $f = x^5 + 3x^3 - 6x^2 + 3$. Reducing modulo 3, we get the polynomial $\overline{f} = x^5$ in $\mathbb{F}_3[x]$. Now suppose that $f$ were reducible, say $f = gh$, where $g = x^2 + b_1x + b_0$ and $h = x^3 + \cdots + c_0$. Then in $\mathbb{F}_5[x]$, we will have $\overline{f} = \overline{g}\overline{h}$, and since $\overline{f} = x^6$, $\overline{g} = x^2$ and $\overline{h} = x^3$. Therefore the coefficients $b_1, b_0$, and $c_2, c_1, c_0$ are all divisible by 3. The constant term of $f$ is the product $b_0c_0$. So it must be divisible by $3^2$. Since the constant term is 3, this is a contradiction. So we can't have $f = gh$.

The principle at work here is the Eisenstein Criterion: Let $f(x) = a_nx^2 + \cdots + a_0$ be an integer polynomial and let $p$ be a prime integer. Suppose that

- $p$ doesn't divide $a_n$,
- $p$ divides all other coefficients $a_{n-1}, ..., a_0$, and
- $p^2$ doesn't divide $a_0$.

Then $f$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

The proof is the same as the one given in the example.

The Eisenstein Criterion doesn't apply often, but it is very useful when it does apply. Its most important application is to prove that the *cyclotomic polynomial* $\phi(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible when $p$ is a prime. (When $p$ is not a prime, this polynomial won't be irreducible.) The cyclotomic polynomial is the result of dividing $x^p - 1$ by $x - 1$:

$$x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1) = (x-1)\phi(x)$$

To prove that $\phi(x)$ is irreducible, we substitute $x = y+1$ into this equation:

$$(y+1)^p - 1 = y\phi(y+1)$$

If $\phi(x)$ factors, so does $\phi(y+1)$. So it suffices to prove that $\phi(y+1)$ is irreducible. We expand the left side of the equation:

$$(y+1)^p - 1 = \big(y^p + \binom{p}{1} y^{p-1} + \cdots \binom{p}{p-1} y + 1\big) - 1$$

Dividing both sides of the equation by $y$,

$$y^{p-1} + \binom{p}{1} y^{p-2} + \cdots \binom{p}{p-1} = \phi(y+1)$$

Now, $\binom{p}{i}$ is divisible by $p$ for every $i = 1, ..., p-1$. The reason is that $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. In this fraction, the numerator is divisible by $p$ but the denominator is not. The hypotheses of the Eisenstein Criterion are satisfied, so $\phi(y+1)$ and $\phi(x)$ are irreducible.