Corollaries of the Factor Theorem

Throughout today’s class, $F$ is a field.

Recall that the Factor Theorem says that for all $f \in F[x]$ and all $a \in F$,

$$f(a) = 0 \iff (x - a) \mid f.$$  

**Corollary.** A nonzero polynomial $f \in F[x]$ of degree $n$ can have at most $n$ zeroes in $F$.

**Proof.** Let $a_1, \ldots, a_r$ be the (distinct) zeroes of $f$ in $F$. We need to show that $r \leq n$. We will use induction on $n$.

**Base Case.** If $n = 0$ then $f$ is a constant polynomial $c \neq 0$, so $f$ has no zeroes.

**Inductive Step.** Assume $n > 0$. If $r = 0$ then $r \leq n$ and we’re done. Otherwise $a_1$ is a zero of $f$, so $(x - a_1) \mid f$, say $f = (x - a_1)g$. Here $g \in F[x]$, $\deg g = (\deg f) - 1 = n - 1$, and $g$ has zeroes $a_2, \ldots, a_r$ (and also possibly $a_1$). (This is because $0 = f(a_1) = (a_i - a_1)g(a_i)$ and $a_i - a_1 \neq 0$ for all $i > 1$.) Therefore, by the inductive hypothesis, $r - 1 \leq (\text{number of zeroes of } g) \leq n - 1$, which gives $r \leq n$. □

**Corollary.** If $G$ is a finite subgroup of $F^*$, then $G$ is cyclic.

**Proof.** Let $n = |G|$ and suppose that $G$ is not cyclic. Then there is an $m < n$ such that $g^m = 1$ for all $g \in G$ (exercise). But then $f(x) = x^m - 1$ has $n > m$ zeroes, namely all elements of $G$. This is a contradiction. □

**Corollary.** If $F$ is a finite field (for example, $\mathbb{Z}_p$), then $F^*$ is cyclic.

(This is used frequently in cryptography.)

Irreducible Polynomials

**Definition.** Let $f \in F[x]$.

(a). We say that $f$ is **irreducible over** $F$, or **irreducible in** $F[x]$, if $f$ is nonconstant and cannot be factored as $f = gh$ with nonconstant $g, h \in F[x]$.

(b). We say that $f$ is **reducible over** $F$, or **reducible in** $F[x]$, if it can be factored in the above way.

Irreducible elements of $F[x]$ play a similar role as prime numbers in $\mathbb{Z}$.

Therefore $f \in F[x]$ is exactly one of: (i) reducible (in $F[x]$), (ii) irreducible (in $F[x]$), (iii) a unit in $F[x]$, or (iv) zero.

**Example.** $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, but reducible in $\mathbb{C}[x]$.

**Note:** Let $f \in F[x]$ and $c \in F^*$. Then $f$ is irreducible in $F[x]$ if and only if $cf$ is.

**Useful fact:** If $f \in F[x]$ has degree 2 or 3, then it is reducible in $F[x]$ if and only if it has a zero in $F$. This is because if it factors, then at least one of the factors must be linear. (The converse holds by the Factor Theorem.)
Example. \( x^3 + x + 1 \) is irreducible in \( \mathbb{Z}_2[x] \). (Neither 0 nor 1 is a zero of the polynomial.)

Example. \( f(x) = x^4 + x^3 + 1 \) is irreducible in \( \mathbb{Z}_2[x] \). Indeed, neither 0 nor 1 is a zero of \( f \), so the only possible factorizations would be \( f = gh \) with \( g \) and \( h \) quadratic. Also, neither \( g \) nor \( h \) would have zeroes in \( \mathbb{Z}_2 \) (those would also be zeroes of \( f \)). There are four polynomials of degree 2 in \( \mathbb{Z}_2[x] \):

\[
x^2, \quad x^2 + x, \quad x^2 + 1, \quad \text{and} \quad x^2 + x + 1.
\]

Of these, only \( x^2 + x + 1 \) has no zeroes. Therefore if \( f \) factors then we must have \( g = h = x^2 + x + 1 \). But then \( f = gh = (x^2 + x + 1)^2 = x^4 + x^2 + 1 \), contradiction. Therefore \( f \) is irreducible.

Gauss's Lemma

Theorem (Gauss’s Lemma). Let \( g, h \in \mathbb{Z}[x] \). Suppose that the gcd of the coefficients of \( g \) is 1, and that the same is true for \( h \). Then the same is true for the product \( gh \).

Proof. Omitted.

Corollary. Let \( f \in \mathbb{Z}[x] \). If \( f \) can be factored in \( \mathbb{Q}[x] \) as \( f(x) = g(x)h(x) \), then it can be factored in \( \mathbb{Z}[x] \) as \( f(x) = \tilde{g}(x)\tilde{h}(x) \) with \( \deg \tilde{g} = \deg g \) and \( \deg \tilde{h} = \deg h \).

(In fact, there is an \( a \in \mathbb{Q}^* \) such that \( \tilde{g} = ag \) and \( \tilde{h} = a^{-1}h \).)

Proof. Omitted.

Definition. A polynomial is monic if it is nonzero and its leading coefficient is 1.

Corollary. If a monic polynomial \( f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x] \) has a zero \( m \) in \( \mathbb{Q} \), then \( m \in \mathbb{Z} \) and \( m \mid a_0 \).

Proof. If \( f \) has a zero \( m \in \mathbb{Q} \), then \( f = gh \) in \( \mathbb{Q}[x] \) with \( g(x) = x - m \). By the second corollary, there is an \( a \in \mathbb{Q}^* \) such that both \( \tilde{g} = ag \) and \( \tilde{h} = a^{-1}h \) lie in \( \mathbb{Z}[x] \). Since \( g \) and \( h \) are monic, the leading coefficients of \( \tilde{g} \) and \( \tilde{h} \) are \( a \) and \( a^{-1} \), respectively, so \( a \) must be \( \pm 1 \). We may assume \( a = 1 \), so \( \tilde{g} = x - m \). This lies in \( \mathbb{Z} \), so \( m \in \mathbb{Z} \). Also \( h = \tilde{h} \) is in \( \mathbb{Z}[x] \), so its constant coefficient is \( b_0 \in \mathbb{Z} \) such that \( mb_0 = a_0 \). This gives \( m \mid a_0 \).

Clicker Questions!

(And please remind Prof. Vojta to return homeworks and pass out handouts)
Theorem (Eisenstein Criterion). Let \( p \in \mathbb{Z} \) be prime, and let
\[
f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x].
\]
Suppose: (1) \( p \nmid a_n \), (2) \( p \mid a_i \) for all \( i < n \), and (3) \( p^2 \nmid a_0 \). Then \( f \) is irreducible over \( \mathbb{Q} \).

Proof. See book.

Example. \( x^2 - 2 \) is irreducible over \( \mathbb{Q} \) (and therefore \( \sqrt{2} \notin \mathbb{Q} \)).

Proof 1. Use the Eisenstein criterion with \( p = 2 \).

Proof 2. Assume it is reducible. Then it has a zero \( m \in \mathbb{Q} \), hence a zero \( m \in \mathbb{Z} \). Such a root must satisfy \( m \mid 2 \), so \( m = \pm 1 \) or \( m = \pm 2 \). Checking these show that there is no such zero, so \( x^2 - 2 \) is irreducible.

**Unique Factorization in \( F[x] \)**

Lemma. Let \( p, r, s \in F[x] \) with \( p \) irreducible. If \( p \mid rs \) then \( p \mid r \) or \( p \mid s \).

Proof. Later. \( \Box \)

Lemma. Let \( p, r_1, \ldots, r_n \in F[x] \) with \( p \) irreducible and \( n \in \mathbb{N} \). If \( p \mid r_1 \ldots r_n \) then \( n > 0 \) and \( p \mid r_i \) for some \( i \).

Proof. When \( n = 0 \) this is impossible (due to degrees). When \( n = 1 \) it is trivial, and when \( n = 2 \) this is the previous lemma. For \( n > 2 \) it follows by induction. \( \Box \)

Theorem. Any nonconstant polynomial in \( F[x] \) can be factored in \( F[x] \) into a product of irreducible polynomials in \( F[x] \).

Moreover, such a factorization is unique, up to permuting the factors and multiplying them by nonzero constants (in \( F \)).

Proof. Existence: Clear (keep factoring until you can’t anymore).

[How do you know it eventually has to stop?]

Uniqueness: Let \( f \in F[x] \) be the polynomial to be factored. Suppose that \( f = p_1 \ldots p_r = q_1 \ldots q_s \) with all \( p_i \) and \( q_j \) irreducible.

We will use induction on \( r \). Since \( f \) is not constant, we have \( r, s > 0 \).

Base case. If \( r = 1 \) then \( f = p_1 \) is irreducible, so \( s \leq 1 \), hence \( s = 1 \) and \( p_1 = q_1 \).

Inductive step. If \( r > 1 \) then \( p_1 \mid q_j \) for some \( j \). Then \( p_1 u = q_j \) for some \( j \) and some \( u \in F[x] \). Since \( q_j \) is irreducible and \( p_1 \) is not constant, \( u \) is constant, necessarily nonzero. After permuting indices we may assume that \( j = 1 \). Since \( r > 1 \), we may replace \( p_1 \) with \( up_1 \) and \( p_2 \) with \( u^{-1}p_2 \) to obtain \( p_1 = q_1 \) (the new \( p_1 \) and \( p_2 \) are still irreducible).

Now cancel \( p_1 \) from both sides to get \( p_2 \ldots p_r = q_2 \ldots q_s \). Since \( r > 1 \) this common value is nonconstant. By the inductive hypothesis, \( r = s \) and the factors are the same up to permutation and multiplication by nonzero constants. \( \Box \)

[Compare this with the proof of unique factorization for (positive) integers.]
Ring Homomorphisms

Recall: A ring homomorphism \(\phi: R \rightarrow R'\) is a function \(\phi: R \rightarrow R'\) such that \(\phi(a + b) = \phi(a) + \phi(b)\) and \(\phi(ab) = \phi(a)\phi(b)\) for all \(a, b \in R\).

**Theorem.** Let \(\phi: R \rightarrow R'\) be a ring homomorphism. Then:

1. \(\phi(0) = 0'\) (where 0 and 0' are the additive identities in \(R\) and \(R'\), respectively)
2. \(\phi(-a) = -\phi(a)\) for all \(a \in R\)
3. If \(S \leq R\) then \(\phi[S] \leq R'\)
4. If \(S' \leq R'\) then \(\phi^{-1}[S'] \leq R\)
5. If \(R\) has unity \(1\) then \(\phi[R]\) has unity \(\phi(1)\).

**Proof.** See book. (Compare with Thm. 13.12.)

**Caution:** In (5), the unity \(\phi(1)\) for \(\phi[R]\) need not be the unity for all of \(R'\); in fact, \(R'\) need not have a unity element.

**Example.** \(\phi: \mathbb{Z} \rightarrow \mathbb{Z} \times 2\mathbb{Z}\) given by \(\phi(n) = (n, 0)\). \(\phi(1) = (1, 0)\) is not a unity element for \(\mathbb{Z} \times 2\mathbb{Z}\) (which has no unity element).

Kernels and Ideals

Recall: The kernel of a ring homomorphism \(\phi: R \rightarrow R'\) is \(\ker \phi = \{a \in R : \phi(a) = 0\}\). It is a subring of \(R\) because it equals \(\phi^{-1}[[0]]\) and \(\{0\}\) is a subring of \(R'\).

**Proposition.** Let \(\phi: R \rightarrow R'\) be a ring homomorphism and let \(I = \ker \phi\). Then

1. \(\langle I, + \rangle\) is a subgroup of \(\langle R, + \rangle\), and
2. \(ra \in I \text{ and } ar \in I\) for all \(a \in I\), \(r \in R\).

**Proof.** (1) is from group theory. For (2), \(\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0 = 0\), so \(ra \in I\) for all \(r \in R\) and \(a \in I\). Similarly, \(ar \in I\).

**Definition.** An ideal in a ring \(R\) is a subset \(I \subset R\) such that

1. \(\langle I, + \rangle\) is a subgroup of \(\langle R, + \rangle\), and
2. \(rI \subseteq I\) and \(Ir \subseteq I\) for all \(r \in R\). (Here \(rI = \{ra : a \in I\}\), \(Ir = \{ar : a \in I\}\).

Therefore the kernel of a ring homomorphism \(R \rightarrow R'\) is an ideal in \(R\).

Also, if \(I\) is an ideal in \(R\) then \(I\) is a subring of \(R\) (but not vice versa).

**Examples of Ideals in a Ring \(R\)**

1. In any ring \(R\), \(\{0\}\) and \(R\) are ideals.
2. Assume that \(R\) is commutative with unity and \(a \in R\). Then \(aR = \{ar : r \in R\}\) is an ideal in \(R\), called the principal ideal generated by \(a\) and denoted \(\langle a \rangle\).

(Why do we require \(R\) to be commutative?)
(Why do we require \(R\) to have unity?)

**Finis**

Have a good weekend!