Orbits, Stabilizers, and Characters

- Let $G$ be a permutation group on a finite set $X$.
- Let $x \in X$.
- $O_x = \{ g(x) : g \in G \} \subseteq X$ is the orbit of $x$.
  - Note that $x \in O_x$.
- $G_x = \{ g \in G : g(x) = x \} \subseteq G$ is the stabilizer of $x$.
- Let $g \in G$.
- $F(g) = \{ x \in X : g(x) = x \} \subseteq X$ is the permutation character of $g$. 
Orbit of $g_1$

Stabilizer of $g_1$

Permutation character of $g_1$
Orbits and Stabilizers of Permutation

- Let $g$ be a permutation of set $X = \{1, 2, \ldots, n\}$.
- Corollary 139 (p. 929) says \{ $g^0, g^1, \ldots$ \} is a finite cyclic group.
- Call it $G = \langle g \rangle$.
- Pick an arbitrary $i \in X$.
- By definition $O_i = \{ g^k(i) : k \in \mathbb{N} \}$.
- If $i$ is not moved by $g$, then $O_i = \{ i \}$ and $|O_i| = 1$. 
Orbits and Stabilizers of Permutation (continued)

- Now assume $i = i_1$ is moved by $g$.
- Let $g_1 \cdots g_m$ be the cycle decomposition of $g$.
- Let the cycle involving $i_1$ be $(i_1 \ i_2 \ \cdots \ i_r)$.
  - It is one of the $g_j$’s.
- Clearly, $g^k(i_1) = i_{k+1}$ for $0 \leq k \leq r - 1$.
- We conclude
  $$O_i = \{i_1, i_2, \ldots, i_r\}$$
  and $|O_i| = r$. 
Orbits and Stabilizers of Permutation (concluded)

- The stabilizer of \( i \) is \( G_i = \{ g^k : g^k(i) = i, k \in \mathbb{Z} \} \).

- If \( i \) is not moved by \( g \), then \( g^k(i) = i \) for all \( k \in \mathbb{Z} \); so \( G_i = G \).

- On the other hand, if \( g \) does not fix \( i \), then \( G_i \subsetneq G \).
  - For instance, \( g \notin G_i \).

- In fact, Theorem 145 (p. 947) will show that
  \[
  |G| = |G_i| \cdot |O_i|
  \]
  for all \( 1 \leq i \leq n \).
  - Recall that Theorem 135 (p. 912) says \( o(g) = |G| \).
Orbits as Partitions

Lemma 140 If $G$ be a permutation group on set $X$, then $G$’s orbits partition $X$.

- $\bigcup_x O_x = X$ because $x \in O_x$ for all $x \in X$.
- If $O_x \cap O_y \neq \emptyset$, then $O_x \subseteq O_y$.
  - For any $a \in O_x$, $a = g''(x)$ for some $g'' \in G$.
  - Suppose $z \in O_x \cap O_y$.
  - Then $z = g(x) = g'(y)$ for some $g, g' \in G$.
  - Hence $a = g''(g^{-1}(z)) = g''(g^{-1}(g'(y))) \in O_y$.
- The other direction $O_y \subseteq O_x$ is symmetric.
Orbithood as an Equivalence Relation

Lemma 141 Suppose $G$ be a permutation group on set $X$. Two $i, j \in X$ are in the same orbit if and only if there is a $g \in G$ such that $g(i) = j$.

- Suppose $i, j \in X$ are in the same orbit $O_x$.
  - $i = g_1(x)$ and $j = g_2(x)$ for some $g_1, g_2 \in G$.
  - Hence $j = g_2(x) = g_2(g_1^{-1}(i))$.

- On the other hand, suppose there is a $g \in G$ such that $g(i) = j$.

- Then $j \in O_i$ and also $i \in O_i$. 

©2023 Prof. Yuh-Dauh Lyuu, National Taiwan University
Grouphood of Stabilizers

**Lemma 142** A stabilizer is a subgroup.

- Let $G$ be a permutation group on set $X$.
- Consider a stabilizer $G_x = \{ g \in G : g(x) = x \}$ for $x \in X$.
- For all $g_1, g_2 \in G_x$, $g_1 \circ g_2 \in G_x$ because $g_2(g_1(x)) = x$.
- For all $g \in G_x$, $g^{-1} \in G_x$ because $g^{-1}(x) = x$.
- The lemma then follows by Theorem 111 (p. 835).
Stabilizers of Elements of an Orbit

**Lemma 143** Let $G$ be a permutation group and $x, y$ be in the same orbit. (1) $|G_x| = |G_y|$. (2) $G_x = hG_yh^{-1}$ for some $h \in G$.

- By Lemma 141 (p. 936), $y = h(x)$ for some $h \in G$.
- $G(x, y) \triangleq \{ g \in G : g(x) = y \} \neq \emptyset$ as it contains $h$.
- Let $g \in G(x, y)$.
- Then $g(x) = h(x)$, which implies
  $$h^{-1}(g(x)) = x.$$  
- We conclude that
  $$g \circ h^{-1} \in G_x.$$  (114)
The Proof (continued)

- Recall that $G_x h = \{ g \circ h : g \in G, g(x) = x \}$, a right coset of the stabilizer $G_x$.
- Then $g \in G_x h$.
- As a result $G(x, y) \subseteq G_x h$ by Eq. (114).
- Similarly, we can prove that $G_x h \subseteq G(x, y)$.
- Hence $G(x, y) = G_x h$.
- Recall that $G_x$ is a subgroup by Lemma 142 (p. 937).
- By the coset partition theorem (p. 856),
  
  $$|G(x, y)| = |G_x|.$$
The Proof (concluded)

• By the same argument (why?), $G(x, y) = hG_y$, a left coset of $G_y$.

• Hence $|G(x, y)| = |G_y|$.

• We conclude $|G_x| = |G(x, y)| = |G_y|$.

• We move on to part (2).

• Recall

$$G(x, y) = G_x h = h G_y$$

when $x, y$ are in the same orbit.

• Hence $G_x = h G_y h^{-1}$.
Burnside’s Lemma\textsuperscript{a}

**Theorem 144** Let $G$ be a permutation group on a finite $X$. The number of orbits equals the average number of fixed points of permutations in $G$, i.e.,

$$\frac{\sum_{g \in G} |F(g)|}{|G|}.$$

- The proof counts the total number of fixed points, in two ways.\textsuperscript{b}

\textsuperscript{a}William Burnside (1852–1927) in 1911. The theorem is actually due to Cauchy and later Ferdinand Frobenius (1849–1917) in 1896! Rotman (2006), “Burnside was a fine mathematician, and there do exist theorems properly attributed to him.”

\textsuperscript{b}Recall $F(g) = \{ x \in X : g(x) = x \} \subseteq X$. 
The Proof (continued)

• Let $O_1, O_2, \ldots, O_k$ be the $k$ distinct orbits.

• They partition $X$ by Lemma 140 (p. 935).

• Define $o_i \triangleq |O_i|$.

• Recall stabilizer $G_x$ is the set of permutations fixing $x$.

• $G_x$ is a subgroup of $G$ by Lemma 142 (p. 937).
The Proof (continued)

- Consider $x \in X$ (recall that $x \in O_x$).

- Each right coset of $G_x$ consists of those permutations in $G$ that map $x$ to the same element of $O_x$.
  - Consider the right coset $G_x g$ for some $g \in G$.
  - Every permutation in $G_x g$ maps $x$ to the same $g(x) \in O_x$.

- Elements of $O_x$ (such as $x$) are mapped only to elements of $O_x$ by $G$ by Lemma 141 (p. 936).

- As $|O_x| = o_x$, the subgroup $G_x$ has $o_x$ right cosets.
The Proof (continued)

- By the coset partition theorem (p. 856),
  \[ |G_x| = \frac{|G|}{o_x} \]  \hspace{1cm} (115)

- Let \( \kappa(g) \) denote permutation \( g \)'s number of fixed points.

- By definition,
  \[ \kappa(g) = |F(g)|. \]
The Proof (continued)

- Clearly,
  \[ \sum_{g \in G} \kappa(g) \]
  gives the total number of fixed points.

- Alternatively,
  \[ \sum_{x \in X} |G_x| \]
  gives the total number of fixed points.\(^a\)

\(^a\)Recall p. 931.
The Proof (concluded)

- The average number of fixed points per permutation is

\[
\frac{1}{|G|} \sum_{g \in G} \kappa(g)
\]

\[
= \frac{1}{|G'|} \sum_{x \in X} |G_x|
\]

\[
= \frac{1}{|G|} \sum_{i=1}^{k} \sum_{x \in O_i} |G_x| \quad \text{by Lemma 140 on p. 935}
\]

\[
= \frac{1}{|G|} \sum_{i=1}^{k} o_i \frac{|G|}{o_i} \quad \text{by Eq. (115) on p. 944}
\]

\[
= k.
\]
The Orbit-Stabilizer Theorem

Equation (115) on p. 944 is of independent interest.

**Theorem 145** If $G$ is a permutation group on $X$ and $x \in X$, then

$$|O_x| = \frac{|G|}{|G_x|} = [G : G_x],$$

where we recall $O_x$ is the orbit of $x$.  

---

\textsuperscript{a}Recall p. 863.
An Example

• Consider $G = \langle g \rangle$, where

$$g = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
2 & 3 & 1 & 5 & 4 & 6
\end{pmatrix}.$$ 

• Clearly, $|F(g)| = 1$.

• Now

$$g^2 = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
3 & 1 & 2 & 4 & 5 & 6
\end{pmatrix}$$

with $|F(g^2)| = 3$. 
An Example (continued)

- And

\[ g^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 4 & 6 \end{pmatrix} \]

with \( |F(g^3)| = 4 \).

- And

\[ g^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix} \]

with \( |F(g^4)| = 3 \).
An Example (continued)

• And

\[
g^5 = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
3 & 1 & 2 & 5 & 4 & 6
\end{pmatrix}
\]

with \(|F(g^5)| = 1\).

• Finally,

\[
g^6 = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
1 & 2 & 3 & 4 & 5 & 6
\end{pmatrix} = I
\]

with \(|F(g^6)| = 6\).
An Example (continued)

- The average number of fixed points per permutation is
  \[
  \frac{1 + 3 + 4 + 3 + 1 + 6}{6} = 3.
  \]

- So we expect to find 3 orbits and proceed to verify it.

- Indeed,

  \[
  O_1 = O_2 = O_3 = \{1, 2, 3\},
  \]
  \[
  O_4 = O_5 = \{4, 5\},
  \]
  \[
  O_6 = \{6\}.
  \]
An Example (continued)

• The 3 orbits do partition \{1, 2, 3, 4, 5, 6\} as promised by Lemma 140 (p. 935).

• One can verify that Lemma 141 (p. 936) holds here.\(^a\)
  – For example, 1, 2, and 3 are in the same orbit \(O_1\).
  – Indeed, they can be mapped to each other under \(G\).

\(^a\)That is, two \(i, j \in X\) are in the same orbit if and only if there is a \(g \in G\) such that \(g(i) = j\).
An Example (concluded)

• One can verify that Lemma 142 (p. 937) holds here.\(^a\)
  – For example, the stabilizer \(G_1 = \{ g^3, g^6 \} \) is a subgroup.

• Finally, the orbit-stabilizer theorem (p. 947) holds.
  – For example,
    \[
    |O_1| = 3 = \frac{|G|}{|G_1|}.
    \]

\(^a\)That is, a stabilizer is a subgroup.
How To Use Burnside’s Lemma

- The set $X$ consists of possible “configurations” such as colorings, seatings, etc.

- By Lemma 141 (p. 936), $i, j \in X$ in the same orbit are considered identical (under $G$).

- Hence the number of orbits is the number of distinct configurations (under $G$).
Circular Seating (P. 19)
Circular Seating (continued)

Orbit 1

Orbit 2
Circular Seating (continued)

• In general, we want to seat \( n \) people around a circle.

• Two seatings are equivalent if one is the result of rotation of the other (i.e., in the same orbit).

• How many distinct seatings (i.e., orbits) are there?

• The permutation group consists of \( n \) clockwise rotations.

• Note that a rotation moves a seating into another.

• So the permutation group acts on the \( n! \) possible seatings, not merely the \( n \) people.
Circular Seating (concluded)

- The identity permutation \( g \) has \( |F(g)| = n! \) because every seating is fixed by \( g \).\(^a\)

- All other permutations \( g \) have \( |F(g)| = 0 \) because no seatings are fixed by \( g \).

- As there are \( n \) permutations, Burnside’s lemma (p. 941) says that the number of distinct seatings is

\[
\frac{n! + 0 + 0 + \cdots + 0}{n} = (n - 1)!
\]

- This agrees with the easy result on p. 19.

\(^a\)Recall \( F(g) = \{ x \in X : g(x) = x \} \), where \( X \) is the set of \( n! \) seatings.
Bracelet Coloring

- How many ways are there to color a bracelet of \( n \) beads with \( k \) colors, where \( n \) is an odd prime?
- The bracelet can be rotated but not flipped over.
- The configurations are colorings.
- The permutation group consists of \( n \) clockwise rotations.
- The identity permutation \( g \) has \( |F(g)| = k^n \) because there are \( k^n \) colorings.\(^a\)

\(^a\)Now \( F(g) = \{ x \in X : g(x) = x \} \), where \( X \) is the set of \( k^n \) colorings.
Bracelet Coloring (continued)
Bracelet Coloring (continued)

• All nonidentity permutations $g$ have $|F(g)| \geq k$.
  – If a coloring is monochromatic, then it looks the same under rotations.
  – So colorings with beads painted with the same color are in the same equivalence class (orbit).
  – There are $k$ colorings.
Bracelet Coloring (continued)

• In fact, all nonidentity permutations $g$ have $|F(g)| = k$.
  – Suppose coloring $C$ paints beads at positions $a$ and $b$ with different colors.
  – There exists an $i \in \mathbb{N}$ such that $g^i$ moves the bead at location $a$ to location $b$.
    * Solve $di \equiv (b - a) \mod n$ for $i$ if $g$ rotates the bracelet by $d > 0$ positions.\(^a\)
  – If coloring $C$ is a fixed point under $g$, then it is also a fixed point under $g^i$ by induction.
  – But this is impossible as positions $a$ and $b$ receive different colors.

\(^a\)Because $n$ is a prime, $d^{-1} \mod n$ always exists (p. 808).
Bracelet Coloring (concluded)

- The number of distinct colorings is

\[
\frac{k^n + k + k + \cdots + k}{n} = \frac{k^n}{n} + \frac{n-1}{n} k.
\]  

(116)
Bracelet Coloring with $n = 5$ and $k = 2$

Equation (116) gives $\frac{2^5 + (5-1) \times 2}{5} = 8$. 
Striped Flags

- Suppose we have a striped flag with 6 stripes.
- Each stripe can be colored in red (r), green (g), or blue (b).
- Here is an example:
  
  $\begin{array}{cccc}
  r & g & b & r \\
  g & b & r & g \\
  \end{array}$

- Suppose two flags are considered equivalent if one looks the same as the other one when one stands in back of it.
- The following flag is considered equivalent to the one above:
  
  $\begin{array}{cccc}
  b & g & r & b \\
  g & r & b & g \\
  \end{array}$
Striped Flags (continued)

- Let $X$ contain all possible (6-tuple) colorings $(c_1, c_2, \ldots, c_6)$, where $c_i \in \{ r, g, b \}$.
- Let $\pi$ be the permutation that reverses the positions of the colors,

$$
\pi = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 \\
6 & 5 & 4 & 3 & 2 & 1
\end{pmatrix} = (1 \ 6)(2 \ 5)(3 \ 4).
$$

- It "turns over" the flag.
  - It makes $c_{\pi(i)}$ the $i$th color, $i = 1, 2, \ldots, 6$.
- Note that $\pi$ turns one coloring into another.
- The cyclic group $G = \langle \pi \rangle$ acts on $X$. 
Striped Flags (continued)

• It is clear that $|G| = 2$.
  
  – In fact, $G = \{ I, \pi \}$ as $\pi^2 = I$.

• By definition or Theorem 145 (p. 947), $|O_x| \leq |G|$.

• So each orbit contains either one coloring or two colorings.

• Here is the orbit we saw,

\[
\{ (r, g, b, r, g, b), (b, g, r, b, g, r) \}.
\]

• Note that

\[
\pi(r, g, b, r, g, b) = (b, g, r, b, g, r).
\]
Striped Flags (continued)

• Here is another orbit,

\[ \{ (r, g, b, b, g, r) \} , \]

and \( \pi \) fixes the coloring \((r, g, b, b, g, r)\), a palindrome!

• Palindromes form only a proper subset of all flags.
  – There are \( 3 \times 3 \times 3 = 27 \) palindromes as there are 3 choices for each of \( c_1, c_2, c_3 \).

• A distinct coloring of the flag corresponds to an orbit, and vice versa.
Striped Flags (continued)

- The number of distinct colorings of the flag is thus the number of orbits.
- Burnside’s lemma (p. 941) says the number of orbits is
  \[ \frac{|F(I)| + |F(\pi)|}{2}. \]
- The identity permutation \( I \) fixes every coloring \( x \in X \).
- So \( |F(I)| = 3^6 \).
Striped Flags (concluded)

- On the other hand, $\pi$ fixes a coloring $x \in X$ if and only if $x$ is a palindrome.
- Hence $|F(\pi)| = 3^3$.
- Our desired count is hence
  \[ \frac{3^6 + 3^3}{2} = 378. \]
- In general, if the flag has $2s$ stripes and $k$ colors, then the count equals
  \[ \frac{k^{2s} + k^s}{2}. \]
Finite Fields and Combinatorial Designs
Fields Revisited

• A ring \((R, +, \cdot)\) is a field if \((R - \{0\}, \cdot)\) is an abelian group.\(^a\)
  
  – This means there is a multiplicative identity \(1 \neq 0\) and every nonzero element is a unit.\(^b\)

• Alternatively, \((R, +, \cdot)\) is a field if:
  
  – \((R, +)\) is an abelian group.
  
  – \((R - \{0\}, \cdot)\) is an abelian group.
  
  – The distributive law of \(\cdot\) over \(+\) holds.

\(^{a}\)Recall p. 794.

\(^{b}\)That is, it has a multiplicative inverse (p. 776).
Proper Divisors of Zero and Fields

**Theorem 146** If \((F, +, \cdot)\) is a field, then it has no proper divisors of zero.

- Immediate from Theorem 108 (p. 797).
The Ring Properties of $\mathbb{Z}_n$

- $(\mathbb{Z}_n, +, \cdot)$ is a ring, where both $+$ and $\cdot$ are modulo $n$.
- It is in fact abelian under $\cdot$ as well as $+$.
- Furthermore, it has a multiplicative identity, 1.
- From p. 808, we know each $a \in \mathbb{Z}_n$ has a multiplicative inverse $a^{-1}$ if and only if $\gcd(a, n) = 1$.
- Hence in $\mathbb{Z}_n$, $[a]$ is a unit\(^a\) if and only if $\gcd(a, n) = 1$.\(^b\)

\(^a\)In other words, $a \in \mathbb{Z}_n$ has a multiplicative inverse (p. 776).
\(^b\)Recall p. 801 for the notation $[a]$: All the integers congruent to $a$ modulo $n$. 
When Is $\mathbb{Z}_n$ a (Finite) Field?

**Theorem 147** $\mathbb{Z}_n$ is a field if and only if $n$ is a prime.

Proof ($\Leftarrow$):

- Verify each condition.\(^a\)

Proof ($\Rightarrow$):

- Suppose $n = n_1n_2$ is not a prime, where $1 < n_1, n_2 < n$.
- Because $n_1n_2 \equiv 0 \mod n$, we have $n_1 \cdot n_2 = 0$.
- As $F$ has proper divisors of zero, it is not a field by Theorem 146 (p. 973).

\(^a\)Page 808 is helpful here.
A Finite Field with 4 Elements

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

So it cannot be isomorphic to $\mathbb{Z}_4$ by Theorem 147.
Polynomials

- Let \((R, +, \cdot)\) be a ring.
- Let \(x\) denote an indeterminate—a formal symbol that is not an element of \(R\).
- Then
  \[
  f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,
  \]
  where \(a_i \in R\), is called a polynomial in the indeterminate \(x\) with coefficients from \(R\).
Polynomials (continued)

• If $a_n \neq 0$, the $a_n$ is called the leading coefficient of $f(x)$, and the degree of $f(x)$ is $n$.
  – The degree of $f(x)$ is denoted by $\deg f(x)$, $\deg f$, or $\deg(f)$.

• A degree-0 polynomial is an element of $R$.
  – They are called constant polynomials.
Polynomials (concluded)

- $R[x]$ is the set of all polynomials in the indeterminate $x$ with coefficients from $R$.

- By identifying constant polynomials with elements of $R$, we can view $R$ as a subring of $R[x]$.

- If $R$ has unity 1, a polynomial is **monic** if its leading coefficient is 1.
Polynomial Additions and Multiplications

• Let \( f(x) = \sum_{i=0}^{n} a_i x^i \) and \( g(x) = \sum_{i=0}^{m} b_i x^i \), with \( n \geq m \).

• \( f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i \), where \( b_i = 0 \) for \( i > m \).

• \( f(x) \cdot g(x) = \sum_{i=0}^{n+m} \left[ \sum_{j=0}^{i} (a_j \cdot b_{i-j}) \right] x^i \).

• Note that \( + \) and \( \cdot \) for polynomials are built on \( + \) and \( \cdot \) for elements of \( R \); they are not identical, however.

**Theorem 148** \((R[x], +, \cdot)\) is a ring called the polynomial ring over \( R \). The zero element is 0, the zero polynomial.
Polynomial Additions and Multiplications (concluded)

**Theorem 149** For $f, g \in R[x]$,

\[ \deg(f + g) \leq \max(\deg(f), \deg(g)), \]
\[ \deg(f \cdot g) \leq \deg(f) + \deg(g). \]

*If $R$ is an integral domain, then*

\[ \deg(f \cdot g) = \deg(f) + \deg(g). \]

- An integral domain has no proper divisors of zero.
- Hence the product of two leading coefficients cannot be zero.
Polynomial Rings over $\mathbb{Z}_n$

- $\mathbb{Z}_n[x]$ is a polynomial ring because $\mathbb{Z}_n$ is a ring.
- The multiplication of two polynomials of degrees $n$ and $m$ may produce a polynomial of degree \textit{less than} $n + m$.
- For example, in $\mathbb{Z}_8[x]$,

\[
(4x^2 + 1)(2x + 3) = 8x^3 + 12x^2 + 2x + 3 = 4x^2 + 2x + 3.
\]
Polynomial Ring over a Field

- We shall limit polynomial rings $R[x]$ to cases where $R$ is a field from now on.
- Hence $F$ will be used instead of $R$.
- The multiplication of two nonzero polynomials will produce a polynomial whose degree is the addition of the degrees of the original two polynomials.
The Division Algorithm

- Let \( f(x), g(x) \in F[x] \) with \( f(x) \neq 0 \).
- There exist unique polynomials \( q(x), r(x) \in F[x] \) such that
  \[
g(x) = q(x)f(x) + r(x),
\]
  where \( \deg r < \deg f \).
Divisors and Units

- The ideas of divisors and multiples for polynomials are the standard ones.
- The units\(^a\) of \(F[x]\) are the divisors of the constant polynomial 1.
- In other words, they are all the nonzero constant polynomials.

\(^a\)Recall p. 776.
Greatest Common Divisors Again

- Let \( f(x), g(x) \in F[x] \).
- Then \( h(x) \in F[x] \) is a greatest common divisor of \( f(x) \) and \( g(x) \) if:
  - \( h(x) \) divides both \( f(x) \) and \( g(x) \).
  - If \( k(x) \in F[x] \) and \( k(x) \) divides both \( f(x) \) and \( g(x) \), then \( k(x) \) divides \( h(x) \).
Greatest Common Divisors Again (concluded)

- A monic greatest common divisor, denoted by $\gcd(f(x), g(x))$, is unique.
- A greatest common divisor can be calculated by the Euclidean algorithm for polynomials.
- Two polynomials are relatively prime if their gcd is 1.
- The generalization to $\gcd(f_1(x), f_2(x), \ldots, f_n(x))$ is straightforward.
Irreducible Polynomials$^a$

• Let $f(x) \in F[x]$ with $F$ a field and $\text{deg } f(x) \geq 1$.

• We call $f(x)$ reducible (over $F$) if:
  
  – There exist $g(x), h(x) \in F[x]$ such that

  $$f(x) = g(x)h(x).$$

  – Besides, $\text{deg } g, \text{deg } h \geq 1$.

• If $f(x)$ is not reducible, it is called irreducible or prime.

$^a$I changed the book’s definition on p. 807, which is not quite correct.
Irreducible Polynomials (concluded)

• Every polynomial of degree one is irreducible.

• Members of $F$ are neither irreducible nor reducible.
  – We required $\deg f(x) \geq 1$.

• The reducibility or irreducibility of a polynomial depends on the field under consideration.
  – $x^2 - 2$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$.

• Testing irreducibility is not believed to be computationally easy unless factorization is easy.
Sieve Method to Enumerate Irreducible Polynomials over $\mathbb{Z}_p$

1: $P = \{ x, x + 1, \ldots, x + (p - 1) \}$;
2: {Find irreducible polynomials of degree $n$.}
3: for $n = 2, 3, \ldots$ do
4: for each polynomial $q(x)$ of degree $n$ over $\mathbb{Z}_p$ do
5: if $q_1(x) \nmid q(x)$ for all $q_1(x) \in P$ with degree $< n$
   then
6:     $P := P \cup \{ q(x) \}$;
7: end if
8: end for
9: end for
Irreducible Polynomials over $\mathbb{Z}_2$

For polynomials over the binary field $\mathbb{Z}_2$, the irreducible polynomials are

$$x, x + 1$$
$$x^2 + x + 1$$
$$x^3 + x + 1, x^3 + x^2 + 1$$
$$x^4 + x^3 + x^2 + x + 1, x^4 + x + 1, x^4 + x^3 + 1$$
$$\vdots$$
Characteristic

• Let \((R, +, \cdot)\) be a ring.

• Suppose there is a least positive integer \(n\) such \(nr = z\), the zero of \(R\), for all \(r \in R\).

  – Recall that \(nr\) is a shorthand for \(\underbrace{r + r + \cdots + r}_{n}\), not \(n \cdot r\), which is undefined.

• Then we say \(R\) has characteristic \(n\).

• When no such integer exists, \(R\) is said to have characteristic 0.
Examples

• The ring \((\mathbb{Z}_n, +, \cdot)\) has characteristic \(n\).
  – Clearly, \(nr = 0 \mod n\) for all \(r \in \mathbb{Z}_n\).
  – Any other number \(m < n\) cannot cut it.

• The ring \((\mathbb{Z}, +, \cdot)\) has characteristic 0.

• The ring \(\mathbb{Z}_n[x]\) has characteristic \(n\).
  – Clearly, \(np(x) = 0\) for all polynomial \(p(x) \in \mathbb{Z}_n[x]\).
  – Again, \(np(x)\) means \(\underbrace{p(x) + p(x) + \cdots + p(x)}_{n}\).
  – Any other number \(m < n\) cannot cut it.
The Characteristic of a Field

**Theorem 150**  *The characteristic of a field must be zero or a prime.*

- Let \( n > 0 \) be the characteristic.
- Write the unity of the field as \( u \) to distinguish it from integer 1 for clarity.
- Suppose instead that \( n = mk \), where \( 1 < m, k < n \).
- By definition, \( nu = z \), the zero of the field.
- Hence,

\[
(mk)u = z.
\]
The Proof (continued)

• But

\[(mk)u = \underbrace{mk} u + \cdots + u\]

\[= \underbrace{mk} u^2 + \cdots + u^2\]

\[= \underbrace{m} (u + \cdots + u) \cdot \underbrace{k} (u + \cdots + u)\]

\[= (mu) \cdot (ku).\]

– Note that \(u^2 = u\) (why?).
The Proof (concluded)

- As we are working with a field, \((mu) \cdot (ku) = z\) would imply \(mu = z\) or \(ku = z\).

- Assume \(ku = z\) (the case of \(mu = z\) is identical).

- Then for all \(r\) in the field,

  \[
  kr = k(u \cdot r) = u \cdot r + \cdots + u \cdot r = \underbrace{(u + \cdots + u)}_{k} \cdot r = (ku) \cdot r = z \cdot r = z.
  \]

- As \(k < n\), this contradicts the assumption that \(n\) is the characteristic.
Order of a Finite Field

Theorem 151  A finite field has order $p^t$ for some prime $p$ and $t \in \mathbb{Z}^+$. (And $p$ is the characteristic of the field.)

- We skip the proof.
Congruence Modulo a Polynomial

- Let $f(x), g(x), s(x) \in F[x]$, and $s(x) \neq 0$.
- Write $f(x) \equiv g(x) \pmod{s(x)}$ if $s(x)$ divides $f(x) - g(x)$.
  - We say $f(x)$ is congruent to $g(x)$ modulo $s(x)$.
- By the division algorithm, there exist polynomials $q(x), r(x) \in F[x]$ such that
  \[ f(x) = q(x)s(x) + r(x), \]
  where $r(x) = 0$ or $\deg r(x) < \deg s(x)$.
- Then $f(x) \equiv r(x) \pmod{s(x)}$. 
Algebra of Polynomials Modulo a Polynomial

- Let \( s(x) \in F[x] \) be a nonzero polynomial.
- Consider the algebra of polynomials over \( F \) where polynomial additions and multiplications are modulo \( s(x) \).
- This algebra is a ring, denoted by \( F[x]/(s(x)) \).
  - Just go over each condition required of a ring.
Finite Field Representation

**Theorem 152** \( F[x]/(s(x)) \) is a field if and only if \( s(x) \) is irreducible.

- We skip the proof.
- Let \( p \) be a prime.
- If \( \deg s(x) = n \), then
  \[
  | \mathbb{Z}_p[x]/(s(x)) | = p^n.
  \]
- This is consistent with Theorem 151 (p. 997).
The Galois Field

- Irreducible polynomial of degree \( n \) with coefficients in \( \mathbb{Z}_p \) exists for any prime \( p \) and \( n \in \mathbb{Z}^+ \).
- An irreducible polynomial \( s(x) \) can be used to generate the finite field \( \mathbb{Z}_p[x]/(s(x)) \) by Theorem 152 (p. 1000).
- We call the finite field \( \mathbb{Z}_p[x]/(s(x)) \) the **Galois field** of order \( p^n \).
- It is denoted by \( \text{GF}(p^n) \).
- All finite fields of order \( p^n \) are fundamentally identical.\(^a\)
- By Theorem 151 (p. 997), \( \text{GF}(p^n) \) exists for any prime \( p \) and any \( n \in \mathbb{Z}^+ \).

\(^a\)A finite field is also called a Galois field.
Equations

- By the Fermat–Euler theorem (p. 865), we know

\[ x^{p^n-1} = 1 \]

for any \( x \in GF(p^n) - \{0\} \).

- Hence,

\[ x^{p^n} - x = \prod_{a \in GF(p^n)} (x - a). \]
Equations (concluded)

• In particular,

\[ x^{p-1} = 1 \mod p \]

for any \( 0 < x < p \) by Fermat’s “little” theorem (p. 868).

– Hence,

\[ x^p - x = \prod_{0 \leq a < p} (x - a). \]
Examples

• For GF(3),

\[(x - 0)(x - 1)(x - 2)\]
\[= x^3 - 3x^2 + 2x\]
\[= x^3 + 2x\]
\[= x^3 - x.\]

• For GF(5),

\[(x - 0)(x - 1)(x - 2)(x - 3)(x - 4)\]
\[= x^5 - 10x^4 + 35x^3 - 50x^2 + 24x\]
\[= x^5 + 24x\]
\[= x^5 - x.\]
Generators of a Finite Field

• Every finite field has a generator (or primitive root) $g$ that generates its nonzero elements.
  – The multiplicative group $(F^*, \cdot)$ of a finite field $F$ is cyclic.\(^a\)

• The number of generators in $\text{GF}^*(p^n)$ is $\phi(p^n - 1) > 0$.
  – The four generators in $\text{GF}^*(11)$ are 2, 6, 7, and 8.
  – For $\text{GF}^*(p)$, the likelihood of drawing a generator from $\{1, 2, \ldots, p - 1\}$ is $\phi(p - 1)/(p - 1)$.

• For $\text{GF}^*(p)$, $\phi(k)$ numbers between 1 and $p - 1$ have an order of $k$, where $k \mid (p - 1)$.\(^b\)

\(^a\)Recall Theorem 132 (p. 893).
\(^b\)Recall Lemma 131 (p. 890).
Finis