

## 407 TOOL BOX

Throughout let  $G$  be a group with identity  $e$ , and  $a, b, x, y$ , be elements in  $G$ . Being a subgroup (ideal) is denoted by the symbol  $\leq (\triangleleft)$ .

### 1. Local Results:

- (a) (i)  $a^k = e \iff O(a) | k$ .  
(ii)  $a^k = a^r \iff O(a) | (k - r)$ .
- (b) If  $O(a) = pq$  then  $O(a^p) = q$ .
- (c) (i)  $O(a^k) = O(a)/(k, O(a))$  and  $O(a^k) | O(a)$ .  
(ii)  $O(a^k) = O(G)$  iff  $(k, O(G)) = 1$  and  $O(a) = O(G)$
- (d) if  $ab = ba$  then  
(i)  $a^k b^r = b^r a^k$  for all  $k, r$   
(ii)  $\frac{L}{d} | O(ab) | L$ , where  $d = (O(a), O(b))$  and  $L = [O(a), O(b)]$ .  
(iii) If  $d = (O(a), O(b)) = 1$ , then  $O(ab) = O(a)O(b)$ .
- (e)  $ab = bc$  then  $a^k b = b c^k$ . If  $ab = ba^{-1}$  then  $a^k b^{2s} = b^{2s} a^k$
- (f) In a finite abelian group  $G$ ,  
(i) If  $O(a) \nmid O(b)$ , then there exists  $z$  in  $G$ , such that  $O(b) | O(z)$ , but that  $b \neq z$ .  
(ii) If  $O(y)$  is maximal then  $O(a) | O(y)$ ,  $\forall a \in G$ .
- (g) (i)  $O(a) = O(a^{-1})$   
(ii)  $O(b^{-1} a b) = O(a)$   
(iii)  $(ab \dots c)^{-1} = c^{-1} \dots b^{-1} a^{-1}$ .

### 2. Global Results

- (a) (i) If  $H \leq G$  then  $O(H) | O(G)$   
(ii) index of  $H$  in  $G = \#\{\text{left-cosets}\} = \#\{\text{right-cosets}\} = O(G)/O(H)$   
(iii)  $O(a) | O(G)$   
(iv)  $H \leq G$  iff  $ab^{-1} \in H$  (subgroup)  
(v)  $S \leq R$  iff  $S - S \subseteq S$  and  $S.S \subseteq S$  (subring)  
(vi)  $I \triangleleft R$  iff  $I - I \subseteq I$  and  $R.I \subseteq I$ ,  $I.R \subseteq R$  (ideal)  
(vii)  $H \triangleleft G$  iff  $aH = Ha$ ,  $\forall a$  iff  $aH \subseteq Hb$ ,  $\forall a, \exists b$ .

### 3. Cyclic Stuff

- (a) (i) Let  $G = \langle a \rangle$  be cyclic with  $O(G) = n = gh$ .  
(ii)  $\exists$  exactly one subgroup  $H_h$  of order  $h$   
(iii)  $H_h = \langle a^{n/h} \rangle = \langle a^g \rangle$  is the **only** subgroup of order  $h$  in  $G$   
(iv)  $H_h$  contains all elements of order  $h$  in  $G$   
(v) These elements of order  $h$  are precisely the generators for  $H_h$ . They are  $\text{gen}(H_h) = \{b; b \in G, O(b) = h\} = \{(a^g)^k; (h, k) = 1\}$ .  
(vi) Their number is  $\#\{b; O(b) = h\} = \phi(h)$ ,

- (b) (i)  $k | r \implies \langle a^r \rangle \subseteq \langle a^k \rangle$ .  
(ii)  $a^m \in \langle a^k \rangle$  iff  $(k, O(a)) | m$ .  
(iii)  $\langle a^m \rangle = \langle a^n \rangle$  iff  $(m, O(a)) = (n, O(a))$

### 4. Permutations.

- (a) Let  $C, C_i$  be cycles with parity  $\text{par}(C), \text{par}(C_i)$ :  
(i)  $O(C) = \text{its length}$   
(ii)  $O(C) = k \implies \text{par}(C) = \text{par}(k-1)$   
(iii) For disjoint cycles:  $O(C_1 \dots C_k) = LCM[O(C_i)]$ .  
(iv) If  $\alpha^k = (i_1, i_2, \dots, i_r)$ , then  $O(\alpha) = r$ .

### 5. Cosets (i) $O(aH) | O(a)$

- (ii)  $p | O(G) \implies p = O(x), \exists x$ . (Cauchy)

### 6. $\mathbb{Z}_n, \mathbb{Z}_n^*$

- (i)  $a^{\phi(n)} \equiv 1 \pmod n$  ( $a, n) = 1$  (Euler)  
(ii)  $a^{p-1} \equiv 1 \pmod p$  ( $a, p) = 1$  (Fermat)

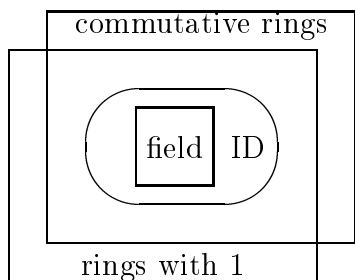
### 7. Direct Sums

- (i)  $O(\oplus G_i) = \prod O(G_i)$ .  
(ii)  $O(a_1, \dots, a_n) = LCM(O(a_i))$   
(iii)  $O(\oplus G_i)$  is cyclic iff  $G_i$  cyclic and  $(O(G_i), O(G_j)) = 1$ .

### 8. First Isomorphism Theorems

- (i) If  $f : G \rightarrow G'$  is a group homomorphism, then  $G/\ker(f) \cong f(G)$   
(ii) If  $f : R \rightarrow R'$  is a ring homomorphism, then  $R/\ker(f) \cong f(R)$

Here is a nesting of rings:



Lord of the Rings

9. (i) A finite ID is a field  
 (ii)  $\mathbb{Z}_n$  is a field iff  $n$  is prime iff  $\mathbb{Z}_n$  is an ID  
 (iii) If  $D$  is an ID then so is  $D[x]$

### 10. Left/Right Evaluation

$a \in R, f(x) \in R[x]$ :

$$f_r(a) = \sum_{i=0}^n f_i a^i, \quad f_\ell(a) = \sum_{i=0}^n a^i f_i$$

$(f + g)_r(a) = f_r(a) + g_r(a)$ . If  $R$  is commutative  $(f \cdot g)(a) = f(a)g(a)$

11. Over an ID,  
 $f(x)g(x) = 0(x)$  with  $f \neq 0 \Rightarrow g = 0$ .  
 Over any  $R$ ,  
 $f(x)g(x) = 0(x)$  with  $f$  regular  $\Rightarrow g = 0$ .

### 12. NC Division Algorithm in $R[x]$

Let  $f(x) = \sum_{i=0}^n f_i x^i$ , and  $g(x) = \sum_{i=0}^m g_i x^i$ ,

with  $n = \partial(f) > \partial(g) = m$  and  $g(x)$  regular. that is,  $g_m$  a **unit** in  $R$ . Then

$$f(x) = q_R(x)g(x) + r_R(x) \text{ and}$$

$$f(x) = g(x)q_L(x) + r_L(x),$$

where  $q_R(q_L)$  is the *right(left)* quotient, and  $r_R(r_L)$  is the right(left) remainder of  $f$  after division by  $g$ . Both are unique!

Moreover either  $r_R(x) = 0(x)$  or  $\partial(r_R) < \partial(g)$ . Likewise either  $r_L(x) = 0(x)$  or  $\partial(r_L) < \partial(g)$ .

### 13. Remainder (Bezout) Theorem

$$f(x) = q_R(x)(x - a) + f_R(a)$$

$$f(x) = (x - a)q_L(x) + f_L(a).$$

$$(x - a)|_L f(x) \text{ iff } f_L(a) = 0$$

$$(x - a)|_R f(x) \text{ iff } f_R(a) = 0$$

14. If  $R$  is commutative with 1, then  
 $f(a) = 0$  (i.e.  $a$  is a root) iff  $(x - a)|f(x)$
15. Over a field  $\mathbb{F}$ , If  $\partial(f(x)) = n$ , then  $f$  has at most  $n$  distinct roots. But  $x^2 - 1$  has 4 roots over  $\mathbb{Z}_8$ !
16. A non-unit  $a$  in  $R$  is irreducible if  $a = bc$  implies  $b$  or  $c$  is a unit.  
 In  $\mathbb{F}[x]$ ,  $f(x)$  is reducible iff  $f(x) = g(x)h(x)$  with  $\partial(g), \partial(h) < \partial(f)$
17. Over a field if  $\partial(f) \leq 3$  then  $f(x)$  is irreducible iff it has no roots