Groups and Rings Useful results

Daniel Lin

April 18, 2022

Basic number theory results can be used without proof, e.g. Bezout's identity. The following results are collected from notes and problem sheets, so you may use them without proof. (Except for those with (*) mark)

Number Theory

- $gcd(m,n) = 1 \Leftrightarrow \exists k, l \in \mathbb{Z}$ s.t. $km + ln = 1$. Backward implication does not hold for other gcd values.
- If p is prime, $m \in \mathbb{N}$, then $gcd(k, p^m) = 1 \Leftrightarrow p \not| k$
- $\phi(n)$ is defined as number of elements in $\{1, 2, ..., n-1\}$ that are coprime to n. $\phi(p^m) = p^m - p^{m-1}$ if p is prime, $m \in \mathbb{N}$. And if $gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$. Explicit formulae for ϕ is

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

- $d = \sum_{\delta|d} \phi(\delta)$ for any $d \in \mathbb{N}$.
- Mod of Squares
  - $x^2 \mod 2 \equiv 0$ (even x) or 1 (odd x)
  - $x^2 \mod 3 \equiv 0$ (x is multiple of 3) or 1
  - $x^2 \mod 4 \equiv 0$ (even x) or 1 (odd x)
  - $x^2 \mod 5 \equiv 0$ (x is multiple of 4) or 1 or 4
  - $x^2 \mod 8 \equiv 0$ (x is multiple of 4) or 1 (odd x, but not multiple of 5) or 4 (even x, but not multiple of 5)
  - for other numbers, there is no clear pattern.

Groups

- Subgroups of $\mathbb{Z}$ are of the form $a\mathbb{Z}$ where $a \in \mathbb{Z}$.
- for a group G with commutative operation $+$, if H, K are subgroups of G, then $H + K := \{h + k : h \in H, k \in K\}$ is also subgroup of G. (This may fail for non-commutative operations)

- Subgroup of any cyclic group(including infinite ones) must be cyclic.
- Abelian group of prime order must be cyclic.
- In cyclic group G with order n, there must be an element with order n. And an element g has order $n \Leftrightarrow \langle g \rangle = G$.
- If G is finite, a subset S that is closed under multiplication must be a subgroup. This fails if G is infinite.
- $H \triangleleft G$ i.e. $gHg^{-1} \subseteq H$ for all $g \in G \Leftrightarrow gH = Hg \ \ \forall g \in G$
- $Z(S_n) = \{e\}$ for $n \geq 3$. (S_n is the symmetric group)
- Every subgroup of index 2 is normal.
- Every normal subgroup is a union of disjoint conjugacy classes.
- Automorphisms send generators to generators.
- $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$
- $\mathrm{Inn}(G) \cong G/Z(G)$
- (*) for S_n, $\mathrm{Inn}(S_n) = \mathrm{Aut}(S_n)$ if $n \neq 2, 6$.
- $G/Z(G)$ is cyclic $\Rightarrow g$ is abelian
- If $G = A \times B$, then $G/A \cong B, G/B \cong A$ (Here, A is shorthand for $A \times \{e_B\}$) And if $A_1 \triangleleft A, B_1 \triangleleft B$ then $A_1 \times B_1 \triangleleft G$ and

$$\frac{G}{A_1 \times B_1} \cong \frac{A}{A_1} \times \frac{B}{B_1}$$

- $Z(A \times B) = Z(A) \times Z(B)$
- For $(x, y) \in A \times B$ where A, B are groups, $\mathrm{ord}((x, y)) = \mathrm{lcm}(\mathrm{ord}(x), \mathrm{ord}(y))$
- $[G, G] \triangleleft G, G/[G, G]$ is abelian and every subgroup of G containing $[G, G]$ is normal in G.
- $C_m \times C_n \cong C_{mn}$ iff $gcd(m, n) = 1$
- Symmetric group S_n is generated by $(12), (12...n)$ and alternating group A_n is generated by 3-cycles. In S_n, a, b are conjugate iff they have the same cyclic shape, so number of conjugacy classes equals number of partitions of n.
- If $H \triangleleft G$ and groups $H, G/H$ are finitely generated, then G is finitely generated.
- $(G/G_{\mathrm{tors}})_{\mathrm{tors}} = \{0\}$. i.e. all non-trivial elements in G/G_{tors} have infinite order.

- Given abelian p-group with $|G| = p^n$ and given $1 \leq m \leq n$, there must be a subgroup of G with order p^m.
- Abelian group is not cyclic $\Leftrightarrow$ there is prime p s.t. a subgroup of G is isomorphic to $C_p \times C_p$.

Rings

- Subring of integral domain must be integral domain.
- (*) But subring of UFD may NOT be UFD, subring of PID may NOT be PID, subring of Euclidean domain may NOT be Euclidean domain.
- (*) R is integral domain $\Rightarrow R[x]$ is integral domain.
- For commutative ring R and its ideals I, J and $a, b \in R$, $aI + bJ := \{ax + by : x \in I, y \in J\}$ is also an ideal. Also $I \cap J, IJ := \{x_1y_1 + \cdots x_ny_n : n \in \mathbb{N}, x_i \in I, y_j \in J\}$ will be ideal.
- $IJ \subseteq I \cap J$, equality hold if $I + J = R$ (I, J are called coprime)
- One can define product ring $R_1 \times R_2$, but it will never be integral domain.
- If I, J are ideals of commutative ring R, then $R/(I \cap J) \cong (R/I) \times (R/J)$
- Given field F s.t. $|F| = p^n$, then $r^{p^n} = r$ for any $r \in F$.
- And $x^{p^n-1} = 1$ has exactly $p^n - 1$ roots in F.
- If a field F has q elements, polynomial $x^{q-1} - 1$ has $q - 1$ roots in F. Further, for any factor $d|(q-1)$, $x^d - 1$ has d roots in F, and number of elements with order d is $\phi(d)$. (where ϕ is Euler's function)
- Multiplicative group of any finite field is cyclic.
- The only endomorphism on $\mathbb{Q}$ is identity map. And only subfield of $\mathbb{Q}$ is $\mathbb{Q}$ itself. But it has infinite subdomains (subrings that are integral domain), namely

$$k_p := \left\{ \frac{a}{b} : gcd(a, b) = 1, b = p^n \text{ for some } n \in \mathbb{N}^0 \right\}$$

- F_1, F_2 are subfields of $K \Rightarrow F_1 \cap F_2$ is subfield of K.
- (*) There is no irreducible element in a field. (As $F/F^\times = \{0\}$, but we require irreducible element to be non-zero)
- Field extension preserves characteristic of the field.
- If we choose an irreducible element a in PID R, then R/aR will be a field. (One way to construct field)

- Given field k, we can construct a larger field by picking irreducible polynomial $p(t) \in k[t]$. Then $K := k[t]/p(t)k[t]$ will be a larger field with $[K : k] = \deg p$. And in K, $p(t)$ must have a root, which is $t + p(t)k[t]$.
- Isomorphism of rings $\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ happens when $gcd(a, b) = 1$.
- If $R = \mathbb{Q}[t]$ and $p(t) = t^2 - d$ where $d \in \mathbb{Z}$ is not divisible by any p^2 (p is prime), then $p(t)$ is irreducible in R and $\mathbb{Q}[t]/p(t)\mathbb{Q}[t] \cong \mathbb{Q}(\sqrt{d})$. Where $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$. This isomorphism is accomplished by $a + bt \mapsto a + b\sqrt{d}$. Same works for $R = \mathbb{Z}[t], \mathbb{Z}/n\mathbb{Z}[t]$.