

More group theory

- An *automorphism* is an isomorphism from a group to itself. An *inner automorphism* is an automorphism of the form (for some  $g \in G$ )  $i_g : G \rightarrow G$  given by  $x \mapsto gxg^{-1}$ .
- Every subgroup  $H \leq G$  partitions  $G$  into *left cosets* (each of the form  $gN$  for some  $g \in G$ ) and also into *right cosets* (each of the form  $Ng$  for some  $g \in G$ ). These partitions are not necessarily the same; for example,  $H = \{\rho_0, \mu_1\}$  induces different partitions of  $S_3$ .
- Lagrange's Theorem concludes, in the case that  $G$  is finite, that  $|H|$  must divide  $|G|$  for every subgroup  $H$ . But if  $n \mid |G|$ , there is not necessarily a subgroup of  $G$  of order  $n$  (there *is* if  $G$  is abelian); it can be shown that  $A_4$  has no subgroup of order 6 even though  $6 \mid \frac{4!}{2}$ .
- Sometimes the binary operation of  $G$  can be used to make the set of (left or right) cosets into a group, and sometimes it can't. Those subgroups for which the set of cosets form a group are called *normal* subgroups; notation:  $N \trianglelefteq G$ .  $N \trianglelefteq G$  iff the left cosets and the right cosets of  $N$  coincide, i.e.,  $\forall g \in G, gN = Ng$ . In this case, the binary operation on the set of (left or right) cosets is  $(aN)(bN) = (ab)N$ ; using the usual equivalence class notation, this is equivalent to:  $\overline{ab} = \overline{a}\overline{b}$ . Note: the identity in  $G/N$  is  $eN = N$ .
- The standard way to show  $N \trianglelefteq G$  is to show  $\forall g \in G, \forall n \in N, gng^{-1} \in N$ .
- If  $\phi : G \rightarrow G'$  is a group homomorphism, then there is a bijection between the cosets of  $\ker \phi$  and the elements of  $\phi(G)$ . In fact, the *First Isomorphism Theorem* states, for any hom  $\phi : G \rightarrow G'$ , the image of  $\phi$  is isomorphic to  $G$  mod the kernel of  $\phi$ , i.e.,  $\phi(G) \cong G/\ker \phi$ .
- If  $\phi : G \rightarrow G'$  is a group homomorphism, then  $\ker \phi \trianglelefteq G$ . Conversely, if  $N \trianglelefteq G$ , then the canonical projection  $\pi : G \rightarrow G/N$  has kernel  $N$ . So every kernel is normal in the domain of the hom, and every normal subgroup is the kernel of some hom.
- If  $G$  is abelian [resp. cyclic], then  $G/H$  is abelian [resp. cyclic] for every  $H \leq G$ .
- If  $G$  is nonabelian, then  $G/H$  may be either abelian or nonabelian. Think of  $S_3/A_3 \cong \mathbb{Z}_2$  for the former.

Quotient (factor) rings and ideals

- Since a ring  $(R, +, \cdot)$  is always an abelian group under  $+$ , every subring  $N \subseteq R$  is a normal subgroup of  $(R, +)$ , so  $(R/N, +)$  is a group. But  $(R/N, +, \cdot)$  is a ring iff  $N$  is an *ideal*, i.e., a subring which also satisfies the condition  $\forall a \in R, \forall n \in N, an \in N$  and  $na \in N$ . In this case, addition and multiplication in  $R/N$  are defined by  $(a + N) + (b + N) = (a + b) + N$  and  $(a + N)(b + N) = (ab) + N$ , i.e.,  $\overline{a} + \overline{b} = \overline{a + b}$  and  $\overline{a}\overline{b} = \overline{ab}$ .
- The kernel of every ring homomorphism  $\phi : R \rightarrow S$  is an ideal of  $R$ , and every ideal  $M \subseteq R$  is the kernel of the ring homomorphism  $\gamma : R \rightarrow R/M$ . Compare this with kernels of group homomorphisms and normal subgroups.
- All "homomorphism theorems" for groups and normal subgroups have analogs for rings and ideals.
- An proper ideal  $I \subseteq R$  is *maximal* if there are no proper ideals properly containing  $I$ . If  $R$  is commutative with 1, then  $R/I$  is a field iff  $I$  is maximal.
- An proper ideal  $I \subseteq R$  is *prime* if  $ab \in I$  implies either  $a \in I$  or  $b \in I$ . If  $R$  is commutative with 1, then  $R/I$  is an integral domain iff  $I$  is prime.

- If  $R$  is commutative with 1, then every maximal ideal is a prime ideal.
- If  $R$  is commutative with 1 and  $I$  is an ideal of  $R$ , then a subset  $X = \{x_1, x_2, \dots, x_n\} \subseteq I$  generates  $I$  if  $I = \{a_1x_1 + a_2x_2 + \dots + a_nx_n \mid a_i \in R\}$ . Notation:  $\langle X \rangle = I$ . In this case,  $X$  is called a *basis* for  $I$ . Notice there is no “linear independence” criterion like there is for a basis of a vector space over a field.
- An ideal  $I \subseteq R$  is *principal* if it is generated by a single element, i.e.,  $\exists a \in I$  such that  $\langle a \rangle = I$ . Compare with cyclic subgroups.
- Every ideal in  $\mathbb{Z}$  and every ideal in  $F[x]$  (where  $F$  is a field) is principal. In addition, an ideal  $\langle a \rangle$  of  $\mathbb{Z}$  is maximal iff  $a$  is prime, and an ideal  $\langle f(x) \rangle$  of  $F[x]$  is maximal iff  $f(x)$  is irreducible over  $F$ .

### Extension fields

- Kronecker’s Theorem states that every nonconstant polynomial in  $F[x]$  has a zero in some extension field of  $F$ . The extension field is  $F[x]/\langle p(x) \rangle$ , where  $p(x)$  is an irreducible factor of the given nonconstant polynomial, and the zero is  $x + \langle p(x) \rangle$ .
- If  $F \leq E$  and  $\alpha \in E$ , then  $\alpha$  is *algebraic* over  $F$  if  $\alpha$  is the zero of some polynomial in  $F[x]$ , and  $\alpha$  is *transcendental* over  $F$  if it isn’t. In the case where  $F = \mathbb{Q}$  and  $E = \mathbb{C}$ ,  $\alpha$  is called an algebraic [resp. transcendental] *number*.
- If  $\alpha$  is transcendental over  $F$ , then  $\alpha$  behaves “like an indeterminate,” i.e.,  $F[\alpha] \cong F[x]$ .
- If  $\alpha$  is algebraic over  $F$ , then  $\text{irr}(\alpha, F)$  is the unique monic polynomial in  $F[x]$  which has  $\alpha$  as a zero. Its degree is  $\deg(\alpha, F)$ .
- If  $\alpha$  is algebraic over  $F$ , then  $F(\alpha)$  is isomorphic to  $F[x]/\langle \text{irr}(\alpha, F) \rangle$ . If  $\alpha$  is transcendental over  $F$ , then  $F(\alpha)$  is isomorphic to the field of quotients  $F(x)$  of the integral domain  $F[x]$ .
- $E \geq F$  is a *simple extension* if  $E = F(\alpha)$  for some  $\alpha \in E$ .
- If  $\alpha$  is algebraic over  $F$ , then  $F(\alpha)$  is a  $\deg(\alpha, F)$ -dimensional vector space over  $F$  with basis  $\{1, \alpha, \alpha^2, \dots, \alpha^{\deg(\alpha, F)-1}\}$ .