MATH50005 Groups and Rings

Notes by Robert Weingart

Contents

1 Homomorphisms and normal subgroups

1.1 Homomorphisms, isomorphisms and automorphisms

Definition 1.1. $f : G \to H$ is a **homomorphism** iff $\forall a, b \in G,\ f(ab) = f(a)f(b)$.

Proposition 1.2. *For a homomorphism $f : G \to H$, $f(e_G) = e_H$ and for any $g \in G$, $f(g^{-1}) = (f(g))^{-1}$*

Example 1.3.

Definition 1.4. $f : G \to H$ is an **isomorphism** iff it is a homomorphism and a bijection. We then write $f : G \xrightarrow{\sim} H$. G and H are **isomorphic** (written $G \cong H$) iff there is an isomorphism between them.

Exercise 1.5. $\cong$ is an equivalence relation.

Definition 1.6. $f : G \xrightarrow{\sim} G$ is an **automorphism**.

Exercise 1.7. $\mathrm{Aut}(G)$ is the group of all automorphisms of G under composition.

Exercise 1.8.

Example 1.9. For $g \in G$, **conjugation by** g is the automorphism $x \mapsto gxg^{-1}$.

Definition. The **image** of a homomorphism is $\mathrm{Im}(f) := \{f(x) \mid x \in G\} \subset H$.

Definition. The **kernel** of a homomorphism is $\mathrm{Ker}(f) := \{x \in G \mid f(x) = e_H\} \subset G$.

Proposition 1.10. $\mathrm{Im}(f) \leq H$ *and* $\mathrm{Ker}(f) \trianglelefteq G$ *(see next definition).*

1.2 Normal subgroups, quotient groups and the isomorphism theorem

Definition 1.11. $S \leq G$ is **normal** iff $\forall x \in S, g \in G,\ gxg^{-1} \in S$. I will then write $S \trianglelefteq G$ (this is standard notation, but the official notes do not use it).

Definition 1.12. G is **simple** iff it has no normal subgroups except $\{e_G\}$ and G.

Exercise 1.13. For $H \leq G$, $(\forall g \in G,\ gH = Hg) \implies H \trianglelefteq G$.

Lemma 1.14. *For $N \trianglelefteq G, g_1, g_2 \in G$, we have $(g_1N)(g_2N) = g_1g_2N$.*

Lemma 1.15. *G/N is a group under $(g_1N, g_2N) \mapsto g_1g_2N$.*

Proposition 1.16. *$f : g \mapsto gN$ is a surjective homomorphism $f : G \to G/N$ with* $\mathrm{Ker}(f) = N$.

Definition 1.17. The **quotient group** of G modulo N is G/N under coset multiplication, as defined in Lemma 1.14.

Exercise 1.18.

Theorem 1.19. *(Isomorphism Theorem) For any $f : G \to H$, $g\,\mathrm{Ker}(f) \mapsto f(g)$ is an isomorphism $G/\mathrm{Ker}(f) \xrightarrow{\sim} f(G)$.*

Proposition 1.20. *For $N \trianglelefteq G$, $S \leq G$ where $N \subset S$, and $f : G \to G/N$ given by $f(g) = gN$:*

- $N \trianglelefteq S$
- $f(S) = S/N \leq G/N$
- *$S \mapsto f(S)$ gives a bijection between the subgroups of G containing N and the subgroups of G/N (TODO: what does that mean?)*
- $S \trianglelefteq G \iff S/N \trianglelefteq G/N$

1.3 Some group-theoretic constructions

1.3.1 The centre of a group

Definition. The **inner automorphism group** $\mathrm{Inn}(G)$ is the group of conjugations by elements of G. Note that $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

Definition. The **centre** of G is

$$Z(G) := \{g \in G \mid \forall x \in G,\ gxg^{-1} = x\}$$

. Note that $Z(G) \trianglelefteq G$, with $Z(G) = G \iff G$ is abelian.

1.3.2 The commutator of a group

Definition. The **commutator** of a and b is $[a, b] := aba^{-1}b^{-1}$.

Definition. The **commutator** or **derived subgroup** of G, written $[G, G]$, is the smallest subgroup of G containing all commutators of elements in G. Note $[G, G] = \{e_G\} \iff G$ is abelian.

Lemma 1.21. *$[G, G] \trianglelefteq G$. $G/[G, G]$ is abelian.*

Proposition 1.22. *G/N is abelian $\iff [G, G] \subset N$.*

Exercise 1.23. *$[G, G] \subset S \leq G \implies S \trianglelefteq G$.*

1.3.3 The product of groups

Definition. The **product** of groups A and B is the cartesian product $A \times B$ under $((a, b), (a', b')) \mapsto (aa', bb')$.

Proposition. *If we consider $a = (a, e_B)$ and $b = (e_A, b)$ then $A \trianglelefteq A \times B$ and $B \trianglelefteq A \times B$. The elements of A commute with all elements of B and vice versa.*

Proposition 1.24. *For $A \trianglelefteq G$, $B \trianglelefteq G$ where $A \cap B = \{e_G\}$ and every element of G can be written as ab with $a \in A$ and $b \in B$, we have $A \times B \cong G$ with the isomorphism $(a, b) \mapsto ab$.*

1.3.4 Abelian groups and p-primary subgroups

Lemma 1.25. *For G abelian, $a, b \in G$ with finite orders, ab also has finite order and* $\operatorname{ord} ab \mid \operatorname{lcm}(\operatorname{ord} a, \operatorname{ord} b)$.

Definition 1.26. For G abelian, the **torsion subgroup of** G is G_{tors}, the set of elements of finite order Note that $G_{tors} \leq G$. G is a **torsion abelian group** iff $G_{tors} = G$

Definition 1.27. For G abelian and p prime, the **p-primary subgroup** of G is $G\{p\}$, the set of elements with order p. Note that $G\{p\} \leq G$. G is a **p-primary torsion abelian group** iff $G\{p\} = G$.

Corollary 1.28. *For $p_1, \ldots, p_m$ prime and $a_1, \ldots a_m$ all ≥ 1, and $n = \prod_{i=1}^{m} p_i^{a_i}$,*

$$C_n \cong \prod_{i=1}^{m} C_{p_i^{a_i}}$$

1.3.5 Generators

Lemma 1.29. *An intersection of subgroups is also a subgroup.*

Definition 1.30. For $S \subset G$ (not necessarily a subgroup), the **subgroup generated by** S is the intersection of all subgroups containing S. If G is the only such subgroup then the elements of S **generate** G.

Example 1.31. If A is generated by n elements and B is generated by m elements then $A \times B$ is generated by $n + m$ elements.

Definition 1.32. G is **finitely generated** if it is generated by a positive finite number of elements.

2 Groups acting on sets

2.1 Actions, orbits and stabilisers

Definition. For a set X, $S(X)$ is the group of bijections $X \to X$ under composition.

Definition 2.1. An **action** of G on X is a homomorphism $G \to S(X)$. The bijection associated with g by an action is written simply as $g : X \to X$. Equivalently, an action is a function $G \times X \to X$ where $g_1(g_2(x)) = (g_1 g_2)(x)$ for any $g_1, g_2 \in G$ and $x \in X$.

Example 2.2.

Definition 2.3. An action is **faithful** iff it is injective.

Notation. The following definitions assume the existence of a particular action of G on X.

Definition 2.4. The **G-orbit of** x is $G(x) := \{g(x) \mid g \in G\} \subset X$. The **stabiliser** of x is $\operatorname{St}_G(x) := \{g \in G \mid g(x) = x\} \leq G$. We write St instead if G is clear from context.

Lemma 2.5. $\operatorname{St}(g(x)) = g \operatorname{St}(x) g^{-1}$.

Theorem 2.6. *(Orbit-stabiliser) For $x \in X$, $g \mapsto g(x)$ gives a bijection from $G/\operatorname{St}(x)$ (the set of left cosets, not necessarily a quotient group since $\operatorname{St}(x)$ may not be normal) to $G(x)$. If G is finite we thus have $|G(x)| = |G|/|\operatorname{St}(x)|$. If X is finite and $X = \bigcup_{i=1}^{n} G(x_i)$ where the G-orbits are disjoint then*

$$|X| = \sum_{i=1}^{n} |G(x_i)| = \sum_{i=1}^{n} (G : \operatorname{St}(x)i)$$

where : denotes the index (number of cosets).

2.2 Applications of the orbit-stabiliser theorem

Theorem 2.7. *(Cayley) If G has finite order n then S_n has a subgroup isomorphic to G.*

Theorem 2.8. *(Cauchy) If G has finite order n and p is prime and divides n then G has an element of order p.*

Definition 2.9. For p prime and G finite, G is a **p-group** iff its order is a power of p.

Corollary 2.10. *A finite group is a p-group iff the orders of all its elements are powers of p.*

Theorem 2.11. *G is a p-group $\implies Z(G) \neq \{e_G\}$.*

Example 2.12.

Definition 2.13. For an action $G \times X \to X$, G **acts transitively on** X iff $X = G(x)$ for some $x \in X$.

Definition 2.14. x is a **fixed point** of g iff $g(x) = x$. The set of fixed points of g is $\operatorname{Fix}(g)$.

Theorem 2.15. *(Jordan) If G and X are finite and G acts transitively on X then*

$$\sum_{g \in G} |\operatorname{Fix}(g)| = |G|$$

In particular, $\operatorname{Fix}(g) = \emptyset$ for some $g \in G$.

Corollary 2.16. *If G and X are finite then the number of G-orbits in X is*

$$|G|^{-1} \sum_{g \in G} |\operatorname{Fix}(g)|$$

Example 2.17.

3 Finitely generated abelian groups

3.1 Smith normal form

Definition 3.1. The $m \times n$ matrix with entries $a_{ij} \in \mathbb{Z}$ is in **Smith normal form** iff

- $i \neq j \implies a_{ij} = 0$

- There exists $k \geq 0$ where $i \leq k \implies a_{ii} > 0$ and $i > k \implies a_{ii} = 0$
- $a_{11} \mid a_{22}$, $a_{22} \mid a_{33}$ and so on

Theorem 3.2. *A matrix with integer entries can be brought into Smith normal form using row and column operations.*

Definition. $d(A)$ is the greatest common divisor of the entries of A. Note this does not change under row and column operations. $t(A)$ is the smallest non-zero absolute value of an entry of A.

Lemma 3.3. *A matrix A with integer entries can be transformed by row and column operations into a matrix B with $t(B) = d(B) = d(A)$.*

3.2 Classification of finitely generated abelian groups

Definition 3.4. The **free abelian group of rank** n is $\mathbb{Z}^n = \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$ (n times).

Proposition 3.5. $\mathbb{Z}^m \cong \mathbb{Z}^n \implies m = n$. *Thus, the rank of a free abelian group is well-defined.*

Proposition 3.6. *Any subgroup of $\mathbb{Z}^n$ is isomorphic to $\mathbb{Z}^m$ for some $m \leq n$.*

Corollary 3.7. *For G finitely generated and abelian, there is a surjective homomorphism $f : \mathbb{Z}^n \to G$ for some n, and $\mathrm{Ker}(f) \cong \mathbb{Z}^m$ for some m.*

Theorem 3.8. *A finitely generated abelian group is isomorphic to a product of finitely many cyclic groups.*

Remark 3.9. The **rank** of a finitely generated abelian group G is m where $G \cong G_{tors} \times \mathbb{Z}^m$, which is well defined.

Corollary 3.10. *For a finite abelian group G, $G \cong \prod_{p \text{ prime}} G\{p\}$.*

Theorem 3.11. *A finitely generated abelian group is isomorphic to the product of finitely many infinite cyclic groups and finitely many cyclic groups whose orders are powers of primes. The number of factors of a given size is uniquely determined by the group.*

4 Basic theory of rings

4.1 Motivation, definitions, examples

Definition 4.1. A **ring** is a set R with two binary operations, $+ : R \to R$ and $\times : R \to R$ (as usual, written ab rather than $a \times b$), where

- $(R, +)$ is an abelian group with identity element 0 and the inverse of x being $-x$
- $\times$ is associative
- There is a unit element 1 which is the identity element for $\times$
- Distributivity: for any $a, b, c \in R$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$

Lemma 4.2. *For any $x, y \in R$, $0x = x0 = 0$, $(-x)y = x(-y) = -xy$, and $R \neq \{0\} \implies 1 \neq 0$.*

Definition 4.3. A **subring** is a subset of a ring which is also a ring with the same $+$, $\times$ and 1.

Lemma 4.4. *For $S \subseteq R$ non-empty, S is a subring iff it contains 1 and is closed under $+$, $\times$ and taking inverses.*

Definition 4.5. R is **commutative** iff $\forall x, y \in R,\ xy = yx$.

Definition 4.6. $x \in R$ is **invertible** iff $\exists y, z \in R : xy = zx = 1$.

Remark 4.7. In the definition above, we necessarily have $y = z =: x^{-1}$. The **multiplicative group** of R is $R^\times$, the set of invertible elements. This is a group.

Definition 4.8. A **division ring** is a ring where all elements except 0 are invertible. A **field** is a commutative division ring.

Example 4.9. For any set X, the set of functions $X \to R$ under $(f+g)(x) := f(x)+g(x)$ and $(fg)(x) := f(x)g(x)$ is a ring.

Example 4.10. The set of $n \times n$ matrices with entries in R under matrix addition and multiplication is a ring.

Example 4.11. For an abelian group A, the set of endomorphisms $A \to A$ (written as $\mathrm{End}(A)$) under addition and function composition is a ring.

4.2 Homomorphisms, ideals, quotient rings

Definition 4.12. For rings R and S, $f : R \to S$ is a **homomorphism of rings** iff it is a homomorphism of the additive groups, $f(xy) = f(x)f(y)$ for any $x, y \in R$, and $f(1_R) = 1_S$.

Lemma 4.13. *For a homomorphism $f : R \to S$, $\mathrm{Ker}(f) \leq (R, +)$ and $\mathrm{Ker}(f)$ is an ideal of R (see definition below).*

Example 4.14.

Example 4.15.

Definition 4.16. $I \subseteq R$ is an **ideal** iff $I \leq (R, +)$ (note that this also means $I \trianglelefteq (R, +)$ since the additive group is abelian) and $\forall r \in R, x \in I$ we have $rx, xr \in I$. I is a **proper ideal** iff additionally $R \neq I$.

Definition 4.17. For a proper ideal $I \subsetneq R$, the **quotient ring** of R by I is R/I with the usual coset addition from $(R, +)$ and $\times$ inherited from R.

Definition 4.18. For a commutative ring R and $a \in R$, the **principal ideal** with **generator** a is $aR := \{ax \mid x \in R\}$. This is an ideal.

Definition 4.19. $f : R \to S$ is an **isomorphism** iff it is a homomorphism and a bijection. We then write $f : R \xrightarrow{\sim} S$. An **endomorphism** is a homomorphism $R \to R$. An **automorphism** is an isomorphism $R \xrightarrow{\sim} R$.

Theorem 4.20. *(Isomorphism Theorem) For a homomorphism $f : R \to S$, $f(R)$ is a subring with $f(R) \cong R/\mathrm{Ker}(f)$.*

4.3 Integral domains and fields

Definition 4.21. $a, b \in R$ are **zero-divisors** iff $a \neq 0$, $b \neq 0$ and $ab = 0$. An **integral domain** is a commutative ring with no zero-divisors.

Lemma 4.22. *For an integral domain R and $a \neq 0$, $ab = ac \iff b = c$.*

Lemma 4.23. *For an integral domain R and $a, b \in R$, $aR = bR \iff \exists r \in R^\times : a = br$.*

Proposition 4.24. *R is a field $\implies$ R is an integral domain.*

Theorem 4.25. *R is a finite integral domain $\implies$ R is a field.*

Corollary 4.26. *For a positive integer n, $\mathbb{Z}/n\mathbb{Z}$ is an integral domain $\iff$ it is a field $\iff$ n is prime.*

Definition 4.27. For a field F, $K \subseteq F$ is a **subfield** of F iff it is a field under the same $+$ and $\times$. Then F is a **field extension** of K.

Proposition 4.28. *For any ring R there is a unique homomorphism $\mathbb{Z} \to R$.*

Lemma 4.29. *For an integral domain R, the kernel of the unique homomorphism described above is either $\{0\}$ or $p\mathbb{Z}$ for some prime p.*

Definition 4.30. The **characteristic** of an integral domain R is $\mathrm{char}(R)$, the unique non-negative generator of the kernel described above (either 0 or prime).

Definition 4.31. A **vector space** over a field K is an abelian group V together with an action of K on V written $(x, v) \mapsto xv$ where for any $x, y \in L$ and $v, w \in V$,

- $1v = v$
- $x(yv) = (xy)v$
- $(x + y)v = xv + yv$
- $x(v + w) = xv + xw$

Lemma 4.32. *A field extension F of K is a vector space over K.*

Theorem 4.33. *For a field K, if $\mathrm{char}(K) = 0$ then K contains a unique subfield isomorphic to Q (and therefore K is a vector space over Q). If $\mathrm{char}(K) = p$ prime then K contains a unique subfield isomorphic to $\mathbb{F}_p$ (and therefore K is a vector space over $\mathbb{F}_p$).*

Corollary 4.34. *The size of any finite field is a positive power of a prime.*

4.4 More on ideals

Proposition 4.35. *A commutative rings is also a field iff its only proper ideal is $\{0\}$.*

Proposition 4.36. *For a homomorphism $f : R \to S$, if $J \subseteq S$ is an ideal then so is $f^{-1}(J) \subseteq R$.*

Proposition 4.37. *For a surjective homomorphism $f : R \to S$, if $I \subseteq R$ is and ideal then so is $f(I) \subseteq S$. $I \mapsto f(I)$ and $J \mapsto f^{-1}(J)$ are inverses, so they give a bijection between the ideals of R which contain $\mathrm{Ker}(f)$ and the ideals of S.*

Definition 4.38. A proper ideal I of a commutative ring R is a **prime ideal** iff R/I is an integral domain.

Proposition 4.39. *A proper ideal I of a commutative ring R is prime* $\iff \forall x, y \in R,\ xy \in I \implies x \in I \vee y \in I$.

Definition 4.40. A proper ideal I of a commutative ring R is a **maximal ideal** iff R/I is a field. Note that maximal $\implies$ prime.

Proposition 4.41. *A proper ideal I of a commutative ring R is a maximal ideal* $\iff$ *there is no proper ideal J with $I \subsetneq J \subseteq R$.*

5 PID and UFD

5.1 Polynomial rings

Definition. For an integral domain R, the **ring of polynomials** with coefficients in R in one variable t is written $R[t]$. The **degree** of a polynomial is written $\deg(p)$.

Proposition 5.1. *For an integral domain R we have $\forall p, q \in R[t],\ \deg(pq) = \deg(p) + \deg(q)$. Futhermore, $R[t]$ is an integral domain, and $R[t]^\times = R^\times$.*

Proposition 5.2. *For a field K and $a, b \in K[t]$ with $b \neq 0$, $\exists q, r \in K[t] : a = qb + r$ where $r = 0$ or $\deg(r) < \deg(b)$.*

Definition 5.3. A **Euclidean domain** is an integral domain R with a function $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ where $\forall x, y \in R \setminus \{0\},\ \phi(xy) \geq \phi(x)$ and $\forall a, b \in R,\ \exists q, r \in R : a = qb + r$ where $r = 0$ or $\phi(r) < \phi(b)$.

Definition 5.4. A **principal ideal domain** is an integral domain where all ideals are principal.

Theorem 5.5. *R is a Euclidean domain $\implies$ R is a PID.*

5.2 Factorisation in integral domains

Definition 5.6. For an integral domain R, $x \in R \setminus R^\times$ is **irreducible** iff x is not a product of two elements in $R \setminus R^\times$.

Lemma 5.7. *x is irreducible $\implies \forall a \in R^\times$, ax is irreducible.*

Definition 5.8. A **unique factorisation domain** or **factorial ring** is an integral domain R where every element of $R \setminus R^\times$ can be written as a product of finitely many irreducibles, and where this decomposition is unique up to reordering the factors and multiplying them by elements of $R^\times$.

Definition 5.9. For an integral domain R and $a, b \in R$, a **divides** b (written $a \mid b$) iff $\exists r \in R : b = ra$. If $r \notin R^\times$ then a **properly divides** b. Otherwise if $r \in R^\times$ then a and b are **associates**.

Notation. The rest of this section will refer to the following properties which an integral domain R may or may not have:

1. There is no infinite sequence of non-zero elements of R such that each element properly divides the previous.
2. For any irreducible $p \in R$, $p \mid ab \implies p \mid a \vee p \mid b$.

Proposition 5.10. *R is a UFD $\implies$ (1) holds.*

Proposition 5.11. *R is a UFD $\implies$ (2) holds.*

Theorem 5.12. *An integral domain R is a UFD iff (1) and (2) hold.*

Example 5.13.

Proposition 5.14. *In a PID, any sequence of ideals $I_1, I_2, \ldots$ where $I_1 \subseteq I_2 \subseteq \ldots$ **stabilises** (is eventually constant).*

Example 5.15.

Proposition 5.16. *R is a PID $\implies$ (2) holds.*

Theorem 5.17. *R is a PID $\implies$ R is a UFD.*

6 Fields

6.1 Field extensions

Definition 6.1. A field extension $K \supset k$ is **finite** iff K is a finite-dimensional vector space over k. Then the **degree** of the extension is $[K : k] := \dim_k(K)$.

Theorem 6.2. *For field extensions $K \supset F \supset k$, K is a finite extension of k iff K is a finite extension of F and F is a finite extension of k. In that case, $[K : k] = [K : F][F : k]$.*

6.2 Constructing fields from irreducible polynomials

Proposition 6.3. *For a PID R and $a \in R \setminus \{0\}$, aR is maximal $\iff$ a is irreducible.*

Corollary 6.4. *For a PID R and $a \in R$, a is irreducible $\implies$ R/aR is a field.*

Remark 6.5. For any irreducible polynomial over k, there is a field extension $K \supset k$ in which it has a root.

Proposition 6.6. *For $f \in k[t]$ with $\deg(f) \in \{2, 3\}$, f is irreducible $\iff$ f has no root in k.*

Example 6.7.

Proposition 6.8. *For an odd prime p, the number of non-squares in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is $\frac{p-1}{2} \geq 1$. For any non-square $a \in \mathbb{F}_p$, $t^2 - a$ is irreducible in $\mathbb{F}_p[t]$ and $\mathbb{F}_p[t]/(t^2 - a)\mathbb{F}_p[t]$ is a quadratic (degree 2) extension of $\mathbb{F}_p$.*

Proposition 6.9. *For $p(t) \in k[t]$, there exists a field extension $K \supset k$ such that $p(t) = c\prod_{i=1}^{n}(t - \alpha_i)$ for some $c \in k^*$ and $\alpha_1, \ldots, \alpha_n \in K$.*

6.3 Existence of finite fields

Lemma 6.10. *For a field k with prime characteristic p, any $x, y \in k$ and a positive integer m, $(x+y)^{p^m} = x^{p^m} + y^{p^m}$.*

Lemma 6.11. *For a field k, $p(t) = \prod_{i=1}^{n}(t-\alpha_i)$ with $\alpha_1, \ldots, \alpha_n \in k$ and $i \neq j$, $a_i \neq a_j \iff p(t)$ and $p'(t)$ have not roots in common.*

Theorem 6.12. *For a prime p and positive integer n, there exists a field of size p^n.*

A Problem Sheets

A.1 Problem Sheet 1

Question 1 $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \{[u]_n : (u,n) = 1\}$.
Question 2.a $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.
Question 2.b $\mathrm{Inn}(S_3) \cong S_3/Z(S_3)$ and $\mathrm{Inn}(S_4) \cong S_4/Z(S_4)$.
Question 3.b Index of $H \leq G$ is $2 \implies H \trianglelefteq G$.
Question 5 $G/Z(G)$ is cyclic $\implies G$ is abelian.
Question 6.a If $G = A \times B$ then $G/A \cong B$ and $G/B \cong A$.
Question 6.b If $G = A \times B$, $A_1 \trianglelefteq A$ and $B_1 \trianglelefteq B$ then $A_1 \times B_1 \trianglelefteq G$ and $G/(A_1 \times B_1) \cong (A/A_1) \times (B/B_1)$.
Question 6.c $Z(A \times B) = Z(A) \times Z(B)$.
Question 8 $C_{mn} \cong C_m \times C_n \iff (m,n) = 1$.

A.2 Unseen Problem Sheet 1

Question 3 If $H \leq G$ and $\forall g \in G,\ g^2 \in H$ then $H \trianglelefteq G$.
Question 4 An infinite group has infinitely many subgroups.
Question 5 For $H \leq G$, $K \leq G$ and $L \trianglelefteq G$ with $HL = KL$ and $H \cap L = K \cap L$, we have $H \cong K$ but not necessarily $H = K$.

A.3 Problem Sheet 2

Question 6 If $|G| = 4$ then G is abelian and in fact $G \cong C_4$ or $G \cong C_2 \times C_2$.
Question 7 If $|G| = p^n$ for p prime then G has a subgroup of order p^m for any $1 \leq m \leq n$.

A.4 Unseen Problem Sheet 2

Question 1 $\forall g \in G \setminus \{e\},\ \mathrm{ord}\, g = 2 \implies G$ is abelian.

A.5 Problem Sheet 3

Question 3 G is abelian $\implies G/G_{tors} = \{e\}$.
Question 4 $Z^m \cong Z^n \implies m = n$.
Question 7 G is not cyclic $\iff$ there is a subgroup $H \leq G$ with $H \cong C_p \times C_p$ for some prime p.
Question 8 If $S \subseteq G$ is finite and closed under the group operation then $S \leq G$.

A.6 Unseen Problem Sheet 3

Question 1 If $|G| = p$ for some prime p then either $G \cong C_{p^2}$ or $G \cong C_p \times C_p$.
Question 2 For a finite abelian group G and a prime p dividing $|G|$, if there are N_p elements of order p then $N_p \equiv -1 \pmod{p}$.
Question 3 If G is finite and the index of $H \leq G$ is the smallest prime divisor of $|G|$ then $H \trianglelefteq G$.

A.7 Problem Sheet 4

Question 6 If F_1 and F_2 are subfields of a field K then $F_1 \cap F_2$ is a subfield of K.
Question 7 If R is a commutative ring and I and J are ideals then $I + J := \{a + b : a \in I, b \in J\}$ is also an ideal of R.
Question 8 If F is a finite field with $|F| = p^n$ then $\forall r \in F,\ r^{p^n} = r$.
Question 9 If R is a ring with $\forall x \in R,\ x^2 = x$ then R is commutative.

A.8 Problem Sheet 5

Euler's function $\varphi(n)$ is the number of integers less than n which are comprime to n.
Question 1.a $(\mathbb{Z}/n\mathbb{Z}, +)$ has $\varphi(n)$ elements of order n.
Question 1.b $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.
Question 1.c For a prime p and a positive integer m, $\varphi(p^m) = p^m - p^{m-1}$.
Question 1.d If $(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$. Furthermore, $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$
Question 2 $\forall d \in \mathbb{N},\ d = \sum_{\delta|d} \varphi(\delta)$.
Question 4 In a field with q elements, if $d \mid q - 1$ then $x^d - 1$ has d distinct roots.
Question 5 In a field F with q elements, if $d \mid q - 1$ then $F^\times$ has $\varphi(d)$ elements of order d.
Question 6 The multiplicative group of a finite field is cyclic.
Question 7 If F is a field with p^n elements for some prime p then the additive group of F is cyclic $\iff n = 1$.

A.9 Problem Sheet 6

Definition A.1. For commutative rings R_1 and R_2, the **product ring** R is $R_1 \times R_2$ under coordinate-wise addition and multiplication.

Question 5.a R is always a ring but never an integral domain.

Notation. Let R be a commutative ring, I and J be ideals of R, and IJ be the set of all finite sums $\sum_{i=1}^n x_i y_i$ with $x_i \in I$ and $y_i \in J$.

Question 6.a $I \cap J$ is an ideal of R.
Question 6.b IJ is an ideal in R.
Question 6.c $IJ \subseteq I \cap J$.
Question 6.d $x \mapsto (x + I, x + J)$ is a homomorphism $R \to (R/I) \times (R/J)$ with kernel $I \cap J$.

Definition A.2. Ideals I and J of R are **coprime** $\iff I + J = R$ (see PS 4 Q 7).

Question 7.a If I and J are coprime then $IJ = I \cap J$.
Question 7.b If I and J are coprime then the homomorphism from PS 6 Q 6d gives an isomorphism $R/IJ \cong (R/I) \times (R/J)$.
Question 7.c $\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.