MATH 5590H FINAL INDEX

BRENDAN WHITAKER

Exercise 1. *Let G be finite. Assume that orders of G and $Aut(G)$ are relatively prime. Prove that G is abelian.*

Proof. Assume G nonabelian. Then $|G|/|Z(G)| = k > 1$, and $k \mid |G|$. But also note

$$G/Z(G) \cong Inn(G) \leq Aut(G),$$

by Corollary 4.4.15, and since G is finite, we have $k = |G/Z(G)|$. But since the orders of G and Aut(G) are coprime, and $G/Z(G)$ is a subgroup of $Aut(G)$, hence k divides the order of $Aut(G)$, we must have that k is also coprime with the order of G. But this is impossible since $k \mid |G|$, so our assumption that G is nonabelian must have been false. □

Exercise 2. *Find all, up to isomorphism groups of order 55.*

Note $n = 11 \cdot 5$. So $n_{11}|5$ and $n_{11} \equiv 1 \mod 11$, so $n_{11} = 1$. And $n_5|11$, and $n_5 \equiv 1 \mod 5$. So $n_5 = 1$ or 11. Let P be a sylow-11 subgroup and Q be a sylow 5 subgroup. Now since $n_{11} = 1$, we know P is characteristic in G. Also since their orders are coprime, $P \cap Q = 1$, and clearly $|PQ| = 55$, so we have $PQ = G$. And since $n_{11} = 1$, we know $P \trianglelefteq G$. Hence $G = P \rtimes Q$. We also know $|P| = 11$, and $|Q| = 5$, since they have power 1, so $P \cong \mathbb{Z}_{11}$ and $Q \cong \mathbb{Z}_5$. We need a homomorphism $\phi : \mathbb{Z}_5 \to Aut(\mathbb{Z}_{11}) = \mathbb{Z}_{10}$.
Case 1: Let ϕ be the trivial homomorphism. We have $G \cong \mathbb{Z}_{11} \times \mathbb{Z}_5 \cong \mathbb{Z}_{55}$.
Case 2: The only other homomorphism between these two groups is $\phi(q) = 2q$. And this induces a nontrivial semidirect product $G = P \rtimes Q \cong \mathbb{Z}_{11} \rtimes \mathbb{Z}_5$.
So the two groups of order 55 are $\mathbb{Z}_{55}$ and the nontrivial semidirect product $\mathbb{Z}_{11} \rtimes \mathbb{Z}_5$.

Exercise 3. *Prove that the group S_4 is solvable.*

Proof. Recall Burnside's Theorem, that any group of order $p^a q^b$ where $a, b \in \mathbb{Z}^{\geq 0}$ is solvable. We know S_4 has order $24 = 2^3 \cdot 3$. Hence S_4 must be solvable. □

Exercise 4. *If R is an integral domain, prove that R has the cancellation property.*

Proof. Suppose $ab = ac$, and $a, b, c \neq 0$. Then we have $a(b-c) = 0$. Then since we are in an integral domain, by definition, we have no zero divisors, so we must have $a = 0$, or $b - c = 0$. But since $a \neq 0$, we have that $b = c$, and hence we have cancellation. □

Exercise 5. *If e is an idempotent element in a ring R, prove that $1 - e$ is also idempotent, and that $R = Re \times R(1 - e)$.*

Proof. Recall that e is idempotent if and only if $e^2 = e$. Then we have $(1-e)^2 = 1-2e+e^2 = 1-2e+e = 1-e$, hence $1 - e$ is also idempotent. Note $Re + R(1 - e) = \{re : r \in R\} + \{r(1 - e) : r \in R\} = R$. So these two ideals are comaximal by definition. Then we have $R/(Re \cap R(1 - e)) \cong R/Re \times R/R(1 - e)$. But note that for any element t in Re, $te = t$ in Re. So suppose there was a nonzero element u in $R(1 - e)$ s.t. $u = r(1 - e) \in Re$. Then we have $r(1 - e)e = r(e - e^2) = r(e - e) = r0 = 0 \neq u$. So we must have that the intersection of the two ideals is trivial. Hence $R(0) = R \cong R/Re \times R/R(1 - e)$. Now we want to show that these two rings in the direct product are isomorphic to Re and $R(1 - e)$. So consider $\phi : R \to R(1 - e)$ given by $\phi(r) = r(1 - e)$. This is a homomorphism of rings since

$$\phi(x + y) = (x + y)(1 - e) = \phi(x) + \phi(y) = x(1 - e) + y(1 - e)$$

$$\phi(xy) = xy(1 - e) = \phi(x)\phi(y) = x(1 - e)y(1 - e) = xy(1 - e)^2 = xy(1 - e),$$

Date: AU17.

since $(1-e)$ is idempotent. Note that Re is in the kernel of ϕ, since for $re \in Re$, we have $\phi(re) = re(1-e) = 0$. Also note ϕ is clearly surjective by the definition of $R(1-e)$. We wish to use the first isomorphism theorem, which states that $R/ker(\phi) \cong \phi(R)$. Suppose there was $x \in R$ s.t. $x \notin Re$ but $\phi(x) = 0$. Then we have $\phi(x) = x(1-e) = x - xe = 0 \Rightarrow x = xe$, so thus x is in Re. So $Re = \ker \phi$, hence $R/Re \cong \phi(R) = R(1-e)$. And the proof that $R/R(1-e) \cong Re$ follows the same way from the mapping $\psi : R \to Re$ given by $\psi(r) = re$. Hence we have:

$$R \cong Re \times R(1-e).$$

Another proof is given by the natural homomorphism $\phi(r) = (re, r(1-e))$. It is a homomorphism since

$$\phi(r+s) = ((re+se, r(1-e)+s(1-e)) = (re, r(1-e)) + (se, s(1-e)) = \phi(r) + \phi(s),$$

And we also have:

$$\phi(rs) = (rese, r(1-e)s(1-e)) = \phi(r)\phi(s),$$

by idempotency. It is injective clearly injective by its definition, and we see it is surjective since if $(re, s(1-e)) \in Re \times R(1-e)$, we have

$$\phi(re + s(1-e)) = (re^2 + s(1-e)e, re(1-e) + s(1-e)^2) = (re + 0, 0 + s(1-e)),$$

by idempotency. Hence ϕ is an isomorphism. □

Exercise 6. *let $\phi : R \to S$ be a homomorphism of rings.*

(1) (a) *Give an example where $\phi(1) \neq 1$.*
Consider $\phi : \mathbb{Z} \to \mathbb{Z}$ given by $\phi(x) = 0$.

(b) *Prove that $\phi(1)$ is an idempotent in S.*

Proof. Observe:

$$\phi(1)\phi(1) = \phi(1 \cdot 1) = \phi(1). \tag{1}$$

□

(c) *If ϕ is surjective, prove that $\phi(1) = 1$.*
Proof. Let ϕ be surjective. Suppose $\phi(1) = t \neq 1$. But since we have surjectivity, we know $\exists r \in R$ s.t. $\phi(r) = 1$. So we have:

$$\phi(r \cdot 1) = \phi(r) = \phi(r)\phi(1) = 1 \cdot t = t, \tag{2}$$

But we said $\phi(r) = 1$, so we have a contradiction, since we assumed $\phi(1) = t \neq 1$, so we must have that $\phi(1) = 1$. □

Hello

Exercise 7. *See below.*

(1) (a) *Prove that any subring of $\mathbb{Z}$ is an ideal in $\mathbb{Z}$.*
Proof. Let $R \subseteq \mathbb{Z}$ be a subring. We want to show $Rx \subseteq R\ \forall x \in R$. So note that since $\mathbb{Z}$ as a group is cyclic, and every subgroup of a cyclic group is cyclic, each subgroup is of the form $R = \langle n \rangle = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. And since every subring must be an additive subgroup, we know every subring is also of the form $n\mathbb{Z}$. So let $x \in \mathbb{Z}$, then $\forall k \in n\mathbb{Z}$ we know xk is a multiple of n since k is a multiple of n, so $xk \in n\mathbb{Z}$, so $xn\mathbb{Z} \subset n\mathbb{Z}$, hence $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

□

(b) *Give an example of a subring of $\mathbb{Z}[i]$ which is not an ideal in $\mathbb{Z}[i]$.*

Exercise 8. *If $I, J \subseteq R$ are ideals, such that $I \subsetneq J$ and $R/I \cong \mathbb{Z}$, prove that R/J is a finite ring.*

Proof. Note that by the **Third Isomorphism Theorem**, we know since I, J are ideals in R and $I \subset J$, $J/I \subset R/I \cong \mathbb{Z}$ is an ideal, and $\frac{R/I}{J/I} \cong R/J \cong \mathbb{Z}/(J/I) \cong R/J$. So since every ideal is a subring in $\mathbb{Z}$ and we know what subrings look like, we know every ideal is of the form $n\mathbb{Z}$ in $\mathbb{Z}$, so $J/I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. So we have $\mathbb{Z}/n\mathbb{Z} \cong R/J$. And we know from our study of groups that $\mathbb{Z}/n\mathbb{Z}$ is finite. □

Exercise 9. *If F is a field, S is a ring, and $\phi : F \to S$ is a nonzero homomorphism, prove that ϕ is injective.*

Proof. Suppose ϕ is not injective. Then $\exists x, y \in F$ s.t. $\phi(x) = \phi(y) \neq 0$ but $x \neq y$. So $\phi(x) - \phi(y) = \phi(x - y) = 0$. But since $x \neq y$, we know $x - y = z \neq 0$. $\square$