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.*

(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.*

(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 $x - y = z \neq 0$. But then since we are in a field, z^{-1} exists, so we have $\phi(zz^{-1}t) = \phi(z)\phi(z^{-1})\phi(t) = \phi(t) = 0 \ \forall t \in F$, so ϕ is the zero homomorphism, which is a contradiction. So we must have that ϕ is injective. □

Exercise 10. *Let p be a prime integer, and $k > 0$. Prove that in the ring $\mathbb{Z}_{p^k}$, every element is either nilpotent or a unit.*

Proof. This looks like an application of the chinese remainder theorem. Note that $\mathbb{Z}_{p^k} \cong \mathbb{Z}/p^k\mathbb{Z}$, and that the units in this ring are all the elements relatively prime with p^k, which we know by the construction of the multiplicative cyclic group of integers $\mathbb{Z}_n^\times$, whose elements are exactly those integers relatively prime with n. So the non-units in this ring are integers m which have $\gcd(m, p^k) > 0$ which implies $m = p^a$ for some $0 < a < k$. But note $m^k = (p^a)^k = p^{ak} = (p^k)^a \equiv 0 \mod p^k$, hence $p^k = 0$ in $\mathbb{Z}_{p^k}$, and hence is nilpotent. Well I guess it wasn't chinese remainder theorem. □

Exercise 11. *If $n \geq 2$, is not a power of a prime integer, prove that the ring $\mathbb{Z}_n$ has an idempotent element distinct from* 1.

Proof. Then we must have $n = p^\alpha q^\beta m$ for distinct primes p, q and some positive integer m, where $\alpha, \beta \geq 1$. Let $a = p^\alpha$ and $b = p^\beta m$. We want elements $x^2 = x$ in $\mathbb{Z}_n$ so we need solutions to the equation $x(x-1) \equiv 0 \mod ab$. Note $(a, b) = 1$. But by the chinese remainder theorem, we have solutions to the system of moduli:

$$\begin{aligned} x &\equiv 0 \mod a \\ x &\equiv 1 \mod b, \end{aligned} \tag{3}$$

hence $\exists x \in \mathbb{Z}$ s.t. $x^2 - x \equiv \mod n$, so $\overline{x} \in \mathbb{Z}_n$, and this is an idempotent element. □

Exercise 12. *Let R be an integral domain, let P be a prime ideal in R, and let $D = R - P$. Prove that the mapping $J \to J \cap R$ defines a bijection between the set of proper ideals of $D^{-1}R$ and the set of ideals of R contained in P, and that $D^{-1}P$ is a maximal ideal in $D^{-1}P$.*

Proof. Recall that P is a prime ideal if and only if R/P is an integral domain. **What the fuck is J?** □

Exercise 13. *Prove that the set $Nil(R) = \sqrt{(0)}$ of nilpotent elements of a ring is an ideal. Prove that $Nil(R)$ is the intersection of all prime ideals of R.*

Proof. Let $r \in R$, and let $N = Nil(R)$. Let $n \in N$. Then $\exists k \in \mathbb{Z}$ s.t. $n^k = 0$. So $(rn)^k = r^k n^k = r^k \cdot 0 = 0$ since we are in a commutative ring. So rn is a nilpotent element, hence $rN \subseteq N$ and thus N is an ideal. **See Eric for next part.** □

Exercise 14. *Let M be a maximal ideal of a ring R. Prove or disprove:*

(a) *Every nonzero element of $R - M$ is a unit.* False. Let $\mathbb{Z}$ be the ring and (2) be the ideal. Note it is prime since 2 is prime in $\mathbb{Z}$, and it is maximal since in a PID, every prime ideal is maximal, and $\mathbb{Z}$ is an ED, hence PID. Now consider $3 \in R - M = \mathbb{Z} - (2)$. 3 is not a unit in $\mathbb{Z}$.

(b) *Every nonzero element of R/M is a unit.* By the above, $27\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$ and in $\mathbb{Z}/27\mathbb{Z}$, 9 is not a unit.

Exercise 15. *If M is a maximal ideal in a ring R, and $a \in R - M$, prove that there exists $b \in M$ and $r \in R$ s.t. $ra + b = 1$.*

Proof. Suppose $ra + b \neq 1 \ \forall r \in R$, $b \in M$. □

Exercise 16. *Let $\phi : R \to S$ be a hom.*

(a) *Show that the preimage of a maximal ideal is not always maximal.* Consider $\phi : \mathbb{Z} \to \mathbb{Z}$ given by $\phi(x) = 2x$. Note that $2\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. But $\phi^{-1}(2\mathbb{Z}) = \mathbb{Z}$ which is not maximal since it is the whole ring.

(b) *Prove that the preimage of a prime ideal is a prime ideal.*
Proof. Let P be a prime ideal in S. We want to show $\phi^{-1}(P)$ is a prime ideal in R. note that an ideal is prime if and only if when $ab \in I$, either $a \in I$ or $b \in I$. So let $xy \in \phi^{-1}(P)$. Then we have $\phi(xy) = \phi(x)\phi(y) \in P$. So we know One of these two images is in P. But then we know one of x or y is in the preimage of P, so its a prime ideal. □

(c) *Prove that if ϕ is surjective and P is a max ideal then the image is a max ideal, or the whole image.*
Proof. Let P be an ideal. Note $\phi(P)$ is an ideal by Theorem 20. Then $\phi(P) \subseteq I \subseteq S$ for some ideal I. Then we have $P \subseteq \phi^{-1}(I) \subseteq R$. Since M is max, we know the preimage of I is equal to M, or the preimage of I is the whole ring R. Hence the image of P is either the whole ring S or a maximal ideal. So since I was an arbitrary ideal containing the image of P, we can take I to be maximal. Then the image of P is maximal in the case where it is not the whole ring. □

(d) *Prove that the surjective image of a prime ideal is prime.*
Proof. Let P be a prime ideal in R. Then consider the image of P. Let $xy \in \phi(P)$. Then we know there are a, b in R s.t. x, y are their respective images. And note that $ab \in P$, hence $a \in P$ or $b \in P$ since P prime. But then the image of either a or b must be in the image of P, and hence either x or y is in the image of P and thus it is a prime ideal. □

Exercise 17. *Let I, J be ideals in a ring R.*

(a) *Prove that $IJ \subseteq I \cap J$, and give an example where $IJ \neq I \cap J$.*
Proof. Note that $IJ = \{\sum^r a_i b_i : a_i \in I, b_i \in J\}$, the set of all finite linear combinations of products of elements from I, J. Now note by properties of ideals that $a_i b_i$ is in both of these ideals, since each of these factors is an element in the parent ring, and any ideal element multiplied by any other element in the ring remains in the ideal by definition of ideal. So each of the terms of the sum is in both ideals, and since ideals are subrings, they are closed under addition, so we have that the whole sum is in both ideals, hence it is in their intersection. □
Note that if we let $I = 6\mathbb{Z}$ and $J = 4\mathbb{Z}$ we have IJ is the set of all finite sums of elements of the form $6x4y$ where x and y are integers, so we clearly get $IJ = 24\mathbb{Z}$. And $I \cap J = 12\mathbb{Z}$. So we have $IJ \subsetneq I \cap J$ since $24\mathbb{Z} \subsetneq 12\mathbb{Z}$. Also note that by definition, $I + J$ is the set of all elements of the form $6x + 10y$ which is $2\mathbb{Z}$.

(b) *If $I + J = (1) = R$, prove that $IJ = I \cap J$.*
Proof. Note that $I + J$ is the smallest ideal containing both ideals. What remains to be shown is that $I \cap J \subseteq IJ$. Observe that $(I \cap J) = (I \cap J)R = (I \cap J)(I + J) = (I \cap J)I + (I \cap J)J \subseteq JI + IJ = IJ$. □

Exercise 18. *Describe all ideals in $\mathbb{Z}[i]$. Which of them are maximal, which of them are prime?*

Note that $\mathbb{Z}[i]$ is an ED (page 272). So every prime ideal is maximal. Also since it's and ED, it is a PID, so every ideal is of the form $(a+bi)$. So the maximal/prime ideals are ideals of this form where the generator is prime. Refer to Proposition 18 on page 291 to see when a Gaussian integer is prime.

Exercise 19. *Describe all ideals in $\mathbb{Z} \times \mathbb{Z}$.*

Recall that $\mathbb{Z}[i] \cong \mathbb{Z}^2$. So the ideals are exactly those described in the above exercise.

Exercise 20. *Prove that $\mathbb{Z}_{nm}^\times \cong \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$.*

Proof. Note that we are in an ED. So we have the Euclidean algorithm. Now note that since n, m are coprime, we know $n\mathbb{Z} + m\mathbb{Z} = (1) = \mathbb{Z}$ since by euclidean algorithm, since the gcd is 1, we can write 1 as a linear combination of n, m, hence $1 \in n\mathbb{Z} + m\mathbb{Z}$. Then we know that these two ideals are comaximal. Then by a corollary of the Chinese remainder theorem, we know $\mathbb{Z}/nm\mathbb{Z}^\times \cong \mathbb{Z}/n\mathbb{Z}^\times \times \mathbb{Z}/m\mathbb{Z}^\times$ (bottom of page 266). □

Exercise 21. *See sheet.*

Exercise 22. *Let I be a nonzero ideal.*

(a) Quotient group is field, so is integral domain, so ideal is prime.
(b) False, $4\mathbb{Z} \subseteq 2\mathbb{Z}$. $4\mathbb{Z}$ not maximal, is prime.

(c) True by theorem.
(d) False, (x)prime, not maximal, contained in $(2, x)$.

Exercise 23. *Note gcd is distinct primes raised to min powers in common, lcm is distinct primes raised to max powers. These equal ab.*