Final Exam

Abstract Algebra 1

MATH 3140

Fall 2022

Sunday December 11, 2022

UPLOAD THIS COVER SHEET!

NAME: ____

PRACTICE EXAM

SOLUTIONS

Question:	**1**	**2**	**3**	**4**	**5**	**6**	Total
Points:	20	20	20	20	20	20	120
Score:							

- The exam is closed book. You **may not use any resources** whatsoever, other than paper, pencil, and pen, to complete this exam.
- You **may not discuss the exam** with anyone except me, in any way, under any circumstances.
- You **must explain your answers**, and you will be **graded on the clarity of your solutions**.
- You must upload your exam as a single **.pdf** to **Canvas**, with the questions in the correct order, etc.
- You have 70 minutes to complete the exam.

1. (20 points) • *Show that for a prime p, the polynomial $x^p + a \in \mathbb{Z}_p[x]$ is not irreducible for any $a \in \mathbb{Z}_p$.*

SOLUTION:

Solution. By Fermat's Little Theorem (see Fraleigh Corollary 20.2), we know that $b^p = b$ for all $b \in \mathbb{Z}_p$. Thus $-a$ is a root of $x^p + a$ in $\mathbb{Z}_p$. It follows from the Factor Theorem (Fraleigh Corollary 23.3) that $x + a$ is a factor of $x^p + a$. Thus, since $p \geq 2$, we have that $x^p + a$ is not irreducible for any $a \in \mathbb{Z}_p$. □

2. • This problem concerns finite groups of units in commutative rings with $1 \neq 0$.

(a) (10 points) *Show that any finite group of units in an integral domain is cyclic.*

[*Hint*: Use what you know about finite groups of units in a field.]

SOLUTION:

Solution. Let D be an integral domain, and let $G \subseteq D^*$ be a finite group of units. Under the inclusion $D \hookrightarrow K(D)$ of D into its field of fractions, we have an inclusion $D^* \hookrightarrow K(D)^*$, so that G is also a finite group of units in the field $K(D)^*$. Therefore, since every finite group of units in a field is cyclic (see Fraleigh Corollary 23.6, p.213), it follows that G is cyclic. $\square$

(b) (10 points) *What if R is any commutative ring with $1 \neq 0$? Is it still true that any finite group of units in R is cyclic?*

[*Hint*: Consider the ring $\mathbb{Z}_3 \times \mathbb{Z}_3$.]

SOLUTION:

Solution. We have seen that for any rings R_1 and R_2, the product $R_1 \times R_2$ has group of units $(R_1 \times R_2)^* = R_1^* \times R_2^*$. Therefore $(\mathbb{Z}_3 \times \mathbb{Z}_3)^* = \mathbb{Z}_3^* \times \mathbb{Z}_3^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, which is not cyclic. $\square$

REMARK

It is interesting to think about exactly where the proof of Fraleigh Corollary 23.6, p.213 (the assertion that a finite group of units in a field is cyclic) fails when the field F in the corollary is replaced with a commutative ring R with $1 \neq 0$, which is not an integral domain.

The first observation is that the same proof we gave to establish the division algorithm in $F[x]$, a polynomial ring in one variable over a field F, gives a division algorithm for $R[x]$ when R is any commutative ring with $1 \neq 0$: *Given a polynomial $f(x) \in R[x]$ and a* monic *polynomial $g(x) \in R[x]$, there are unique polynomials $q(x), r(x) \in R[x]$ such that $f(x) = q(x)g(x) + r(x)$ and either $r(x) = 0$ or* $\deg r(x) < \deg g(x)$ (see e.g., Artin, *Algebra*, Proposition 11.2.9, p.327).

Applying this, one finds that a polynomial $f(x) \in R[x]$ has a root $a \in R$ if and only if $f(x) = q(x)(x-a)$ for some $q(x) \in R[x]$. Note that since $(x-a)$ is monic of degree 1, it is easy to see that $\deg q(x) = (\deg f(x)) - 1$.

As a warning, just because $f(x)$ has distinct roots $a, b \in R$ does not mean that $f(x) = \hat{q}(x)(x-a)(x-b)$ for some $\hat{q}(x) \in R[x]$, unless R is an integral domain. Indeed, as a counter example, consider the polynomial $f(x) = x^2 - (1,1) \in (\mathbb{Z}_3 \times \mathbb{Z}_3)[x]$. Then every element in $\mathbb{Z}_3^* \times \mathbb{Z}_3^*$ is a root of $f(x)$, including for instance $a = (1,1)$ and $b = (1,-1)$, but $(x-(1,1))(x-(1,-1)) = x^2 - (2,0)x + (1,-1)$, no multiple of which can be equal to $x^2 - (1,1)$.

Note also that even if a polynomial $f(x)$ of degree d in $R[x]$ factors into a product of d linear polynomials, if R is not an integral domain, this does *not* imply that $f(x)$ has at most d roots in R (if R is not an integral domain and $f(x) = a_0(x-a_1)\cdots(x-a_d)$, then we could still have $f(a) = a_0(a-a_1)\cdots(a-a_d) = 0$, even if $a - a_i \neq 0$ for $i = 1, \ldots, d$). For instance, considering the same example as before, $f(x) = x^2 - (1,1) = (x+(1,1))(x-(1,1)) \in (\mathbb{Z}_3 \times \mathbb{Z}_3)[x]$, we see that $f(x)$ has 4 distinct roots (all the elements of $\mathbb{Z}_3^* \times \mathbb{Z}_3^*$).

On the other hand, if R *is an integral domain*, then the proof of Fraleigh Corollary 23.6, p.213 holds, essentially verbatim, to prove what we want. More precisely, if $G \subseteq R^*$ is a finite group of units, then it is abelian, and so by the FTFGAG, it is isomorphic to $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n}$ for some natural numbers $d_1 \mid \cdots \mid d_n$. As this implies that every element of G is a root of $f(x) = x^{d_n} - 1$ (every element has order dividing d_n), we see that G can have at most d_n elements (as we are assuming that R is an integral domain), so that $G \cong \mathbb{Z}_{d_n}$. This gives a second proof of part (a).

3. • Let R and S be commutative rings with $1 \neq 0$. In this problem we will show that for any ideal $I \subseteq R \times S$, there are ideals $I_R \subseteq R$ and $I_S \subseteq S$ such that $I = I_R \times I_S$, and moreover, we will show that $(R \times S)/I \cong (R/I_R) \times (S/I_S)$.

(a) (2 points) *If $\phi : R \to S$ is a homomorphism and $I_R \subseteq R$ is an ideal, show by example that $\phi(I_R)$ need not be an ideal of S.*

SOLUTION:

Solution. Let $\phi : \mathbb{Z} \hookrightarrow \mathbb{Q}$ be the natural inclusion, and let $I_R = \mathbb{Z}$. Then $\phi(I_R) = \mathbb{Z}$ is not closed under multiplication in $\mathbb{Q}$ (e.g., $\frac{1}{2}1 = \frac{1}{2} \notin \mathbb{Z}$), so $\mathbb{Z}$ is not an ideal. $\square$

(b) (3 points) *If $\phi : R \to S$ is a* surjective *homomorphism and $I_R \subseteq R$ is an ideal, show that $\phi(I_R)$ is an ideal of S.*

SOLUTION:

Solution. Since the image of a subgroup is a subgroup, we only need to show that $\phi(I_R)$ is closed under multiplication by elements in S. So let $s \in S$ and let $i \in I_R$. We have $s\phi(i) = \phi(r)\phi(i) = \phi(ri) \in \phi(I_R)$, where we are using that ϕ is surjective to conclude that there exists $r \in R$ such that $s = \phi(r)$, and we are using that I_R is an ideal to conclude that $ri \in I_R$. $\square$

(c) (3 points) The first projection map $\pi_1 : R \times S \to R$, $\pi_1(r,s) = r$, is a homomorphism of rings. *If $I \subseteq R \times S$ is an ideal, show that $I_R := \pi_1(I)$ is an ideal of R.* Similarly, the second projection map $\pi_2 : R \times S \to S$, $\pi_1(r,s) = s$, is a homomorphism of rings. *If $I \subseteq R \times S$ is an ideal, show that $I_S := \pi_2(I)$ is an ideal of S.*

SOLUTION:

Solution. The projection maps are surjective homomorphisms of rings. $\square$

(d) (3 points) *If $I_R \subseteq R$ and $I_S \subseteq S$ are ideals, show that $I_R \times I_S$ is an ideal in $R \times S$.*

SOLUTION:

Solution. The product of subgroups is a subgroup. Now given $(r,s) \in R \times S$ and $(i_R, i_S) \in I_R \times I_S$, we have that $(r,s)(i_R, i_S) = (ri_R, si_S) \in I_R \times I_S$. Therefore, $I_R \times I_S$ is an ideal of $R \times S$. $\square$

(e) (3 points) *If I is an ideal in $R \times S$ and we set $I_R := \pi_1(I)$ and $I_S := \pi_2(I)$, show that $I \subseteq I_R \times I_S$.*

SOLUTION:

Solution. If $(a,b) \in I$, then $a \in \pi_1(I)$ and $b \in \pi_2(I)$ so that $(a,b) \in \pi_1(I) \times \pi_2(I)$. $\square$

(f) (3 points) *If I is an ideal in $R \times S$ and we set $I_R := \pi_1(I)$ and $I_S := \pi_2(I)$, show that $I = I_R \times I_S$.*

[*Hint:* use that R and S have $1 \neq 0$, and consider $(1,0)I$ and $(0,1)I$ to show that $I \supseteq I_R \times I_S$.]

SOLUTION:

Solution. We have $\pi_1(I) \times \{0\} = (1,0)I \subseteq I$ and $\{0\} \times \pi_2(I) = (0,1)I \subseteq I$, so $\pi_1(I) \times \pi_2(I) \subseteq I$. $\square$

(g) (3 points) In the notation of the previous problem, *show there is an isomorphism*

$$(R \times S)/I \cong (R/I_R) \times (S/I_S).$$

[*Hint:* Define a homomorphism $\phi : R \times S \to (R/I_R) \times (S/I_S)$.]

SOLUTION:

Solution. We have a surjective ring homomorphism

$$\phi : R \times S \to (R/\pi_1(I)) \times (S/\pi_2(I))$$

$$(a,b) \mapsto ([a],[b])$$

with kernel $\pi_1(I) \times \pi_2(I) = I$. $\square$

4. (20 points) • *Find the degree and a basis for the field extension* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ *over* $\mathbb{Q}$.

[*Hint:* Find a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, and then find a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$.]

SOLUTION:

Solution. $\boxed{\text{The field extension } \mathbb{Q}(\sqrt{2}, \sqrt{3}) \text{ over } \mathbb{Q} \text{ has degree 4, with a basis given by } 1, \sqrt{2}, \sqrt{3}, \sqrt{6}.}$

To see this, we start with the extension $\mathbb{Q}(\sqrt{2})$. By Eisenstein's Criterion applied to the prime $p = 2$ (or using the fact that $\sqrt{2}$ is not rational), we see that $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible, so that the extension $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ has degree 2, with basis given by $1, \sqrt{2}$ (see Theorem 29.18 or Theorem 30.23 of Fraleigh).

Next I claim that the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$ has degree 2, with basis given by $1, \sqrt{3}$. To prove this, it suffices to show (again, see Theorem 29.18 or Theorem 30.23) that $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$. Since this quadratic polynomial can only possibly factor into linear terms, it is equivalent to show that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ (see Corollary 23.3).

To show $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ assume for the sake of contradiction that $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Then since $1, \sqrt{2}$ give a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, we could write $\sqrt{3} = \frac{a}{b} + \frac{c}{d}\sqrt{2}$ with $a, b, c, d \in \mathbb{Z}$, and $b, d \neq 0$. Clearly $c \neq 0$, since otherwise $\sqrt{3}$ would be rational, which we know is not the case. On the other hand, I claim that $c \neq 0$, either. Otherwise, squaring both sides we would have $3 = \frac{c^2}{d^2}2$, or, rearranging, $3d^2 = 2c^2$; but the left hand side has an even number of factors of 2, while the right hand side has an odd number of factors of 2, giving a contradiction. Thus we may assume $a, c \neq 0$. Squaring both sides of $\sqrt{3} = \frac{a}{b} + \frac{c}{d}\sqrt{2}$ gives $3 = \left(\frac{a^2}{b^2} + \frac{2c^2}{d^2}\right) + 2\frac{ac}{bd}\sqrt{2}$, but since a, c are assumed not to be zero, it would follow that $\sqrt{2}$ is rational, giving a contradiction. Thus $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

For the degree of the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, we then conclude (Theorem 31.4) that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

For a basis, we can use the elements $1 \cdot 1$, $1 \cdot \sqrt{3}$, $\sqrt{2} \cdot 1$, $\sqrt{2}\sqrt{3}$ (see the proof of Theorem 31.4; we are taking the product of each element of the basis for $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ with each element of the basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$). In other words, a basis for the field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$ is $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$.

□

5. (20 points) • *Show that if F, E, and K are fields with $F \leq E \leq K$, then K is algebraic over F if and only if K is algebraic over E, and E is algebraic over F.* (You must *not* assume the extensions are finite.)

SOLUTION:

Solution. This is Fraleigh Exercise 31.31. The solution is available on the course webpage. □

6. • **TRUE** or **FALSE**. For this problem, and this problem only, **you do not need to justify your answer**.

(a) (4 points) **TRUE** or **FALSE** (circle one). *There exists a commutative ring with unity that has nonzero zero divisors, and has a quotient ring ("factor ring") that is an integral domain.*

SOLUTION: TRUE. Consider for example $\mathbb{C}[x]/(x^2)$ and the ideal (x), or $\mathbb{Z}/4\mathbb{Z}$ and (2).

(b) (4 points) **TRUE** or **FALSE** (circle one). *If F is a field and $\phi : F \to F$ is a ring isomorphism, then ϕ is equal to the identity.*

SOLUTION: FALSE. Consider complex conjugation on $\mathbb{C}$.

(c) (4 points) **TRUE** or **FALSE** (circle one). *An integral domain of characteristic 0 is infinite.*

SOLUTION: TRUE. We have an injective homomorphism $\mathbb{Z} \hookrightarrow D$.

(d) (4 points) **TRUE** or **FALSE** (circle one). *The remainder of 7^{122} when divided by 11 is 5.*

SOLUTION: TRUE. Fermat's Little Theorem; use $122 = 10 * 12 + 2$, so that $7^{122} = (7^{10})^{12} 7^2 \equiv 49 \pmod{11} \equiv 5 \pmod{11}$.

(e) (4 points) **TRUE** or **FALSE** (circle one). *If R is a commutative ring with $1 \neq 0$, and $f(x), g(x) \in R[x]$ are polynomials of degree two and three respectively, then the degree of $f(x)g(x)$ is five.*

SOLUTION: FALSE. Take $\mathbb{Z}_4[x]$ and $(2x^2)(2x^3)$.