

Math 547, Exam 1. 2/9/10.

Name: _____

- Read problems carefully. Show all work.
- No notes, calculator, or text.
- The exam is approximately 15 percent of the total grade.
- There are 100 points total. Partial credit may be given.

1. **(10 points)** Let R be a commutative ring, let $\phi : R \rightarrow R$ be a ring homomorphism, and let $S = \{a \in R : \phi(a) = a\}$. Show that S is a subring of R .

Solution: Since ϕ is a ring homomorphism, we have $\phi(1) = 1$; it follows that $1 \in S$.

Let $s, s' \in S$. Then we have $\phi(s) = s$ and $\phi(s') = s'$.

Closure under +: Since ϕ is a ring homomorphism we have $\phi(s+s') = \phi(s) + \phi(s') = s+s'$. Therefore, we have $s + s' \in S$.

Closure under \times : Since ϕ is a ring homomorphism we have $\phi(ss') = \phi(s)\phi(s') = ss'$. Therefore, we have $ss' \in S$.

Inverses for +: Let $s \in S$. Since ϕ is a ring homomorphism we have $\phi(-s) = -\phi(s) = -s$. Therefore, we have $-s \in S$.

Combining these facts, we see that S is a subring of R .

2. (20 points) Let R be a commutative ring.

(a) (7 points) Define what it means for an ideal $P \triangleleft R$ to be prime.

Solution: An ideal $P \triangleleft R$ is prime if and only if whenever there are $a, b \in R$ with $ab \in P$, then we must have $a \in P$ or $b \in P$.

(b) (13 points) Let $P \triangleleft R$ be a prime ideal. Show that R/P is an integral domain.

Solution: Let $a + P, b + P \in R/P$, and suppose that

$$(a + P) \cdot (b + P) = ab + P = 0 + P = P.$$

Then we must have $ab \in P$. Since P is a prime ideal, it follows that $a \in P$ (in which case $a + P = 0 + P = P$) or $b \in P$ (in which case $b + P = 0 + P = P$).

3. (27 points) Let R be a commutative ring.

(a) (7 points) Define what it means for an ideal $M \triangleleft R$ to be maximal.

Solution: An ideal is maximal in R if and only if whenever there is an ideal $J \triangleleft R$ with $M \subseteq J \subseteq R$, we must have $J = M$ or $J = R$.

(b) (7 points) Give a simple condition on the ring R which guarantees that a prime ideal in R is maximal.

Solution: If R is a PID, then a prime ideal is also maximal. This is what I wanted.

(c) (13 points) Let $M \neq R$ be an ideal. Both of the following statements are true.

Prove **one** of the statements (your choice).

(1) Suppose that M is maximal. Show: For every $r \in R \setminus M$, there exists $x \in R$ such that $1_R - rx \in M$.

(2) Suppose that for every $r \in R \setminus M$, there exists $x \in R$ such that $1_R - rx \in M$. Show that M is maximal.

Solution: For (1), let $r \in R \setminus M$. Then we have $M \subsetneq (r) + M \subseteq R$. Since M is maximal, we must have $(r) + M = R$, and since $1_R \in R$, there exists $x \in R$ and $m \in M$ such that $rx + m = 1_R$. It follows that $1_R - rx = m \in M$.

For (2), suppose that $\exists J \triangleleft R$ with $M \subsetneq J \subseteq R$. Then there is $r \in J \setminus M \subseteq R \setminus M$. By hypothesis, there must be $x \in R$ such that $1_R - rx = m \in M$. Hence, we must have $rx + m = 1_R$. Now, $x \in R$, $r \in J \triangleleft R$ implies that $rx \in J$. Furthermore, since $m \in M \subseteq J$, we have $rx + m = 1_R \in J$, from which it follows that $J = R$. Therefore, M is maximal.

4. (23 points) Let R be a commutative ring.

(a) (10 points) Define what it means for R to be a **Euclidean ring**.

Use δ to denote the **norm function** in your definition.

Solution: A ring R is Euclidean if it is an integral domain and there is a norm function $\delta : R \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\}$ such that $\forall a, b \neq 0$ in R , we have

i. $\delta(a) \leq \delta(ab)$.

ii. $\exists q, r \in R$ such that $a = bq + r$ and either $\delta(r) < \delta(b)$ or $r = 0$.

(b) (13 points) Suppose that R is a Euclidean ring with norm function δ . Both of the following statements are true. Use the properties of δ from part (a) to prove **one** of the statements (your choice).

(1) If $u \in R^\times$ (u is a unit), then we have $\delta(u) = \delta(1_R)$.

(2) If $u \in R$ has $\delta(u) = \delta(1_R)$, then $u \in R^\times$ (u is a unit).

Solution: For (1), suppose that $a \in R^\times$. Then there exists $b \in R^\times$ with $ab = 1$. Applying property (i) of the norm function, we find that $\delta(a) \leq \delta(ab) = \delta(1_R)$. On the other hand, applying property (i) again to $a = a \cdot 1_R$ gives $\delta(1_R) \leq \delta(a \cdot 1_R) \leq \delta(a)$. Combining these facts, we find that $\delta(1_R) = \delta(a)$.

For (2), property (ii) implies that we may write $1 = aq + r$ with $q, r \in R$ and $\delta(r) < \delta(a)$ or $r = 0$. If $r \neq 0$, then we have $\delta(r) < \delta(a)$. But also, property (i) implies that $\delta(a) = \delta(1_r) \leq \delta(r \cdot 1_R) = \delta(r)$. This is a contradiction. Hence we must have $r = 0$, $1 = aq$, and $a \in R^\times$.

5. **(20 points):** Let $R = \mathbb{Z}[\sqrt{7}] = \{a + b\sqrt{7} : a, b \in \mathbb{Z}\}$.

(a) **(10 points):** Show that $I = \{a + b\sqrt{7} : a \equiv 0 \pmod{7}\}$ is an ideal in R .

(b) **(10 points):** Is I a maximal ideal? Is it a prime ideal? Explain your answer.

(What is R/I ? Think about how R/I determines whether I is maximal or not or whether I is prime or not. You should either try to use the Fundamental Ring Homomorphism Theorem, or you should try to count elements in R/I .)

6. **Challenge problem:** You may attempt this problem if you have completed problems 1 - 5.

Let $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

(a) Show that the principal ideal $(3) = 3R \triangleleft R$ is maximal.

(Imitate the proof that (3) is maximal in $\mathbb{Z}[i]$; use the fact that if either $3 \nmid a$ or $3 \nmid b$, then we have $3 \nmid a^2 - 2b^2$.)

Solution: Suppose that $I \triangleleft R$ has $(3) \subsetneq I \subseteq R$. Then there is $x = a + b\sqrt{2} \in I \setminus (3)$; we must have $3 \nmid a$ or $3 \nmid b$, from which it follows that $3 \nmid t = a^2 - 2b^2$. Hence, we have $\gcd(3, t) = 1$. Therefore, there are $u, v \in \mathbb{Z}$ with $3u + tv = 1$. Since $(3) \subseteq I$, we have $3u \in I$. Observe also that $tv = (a + b\sqrt{2})(a - b\sqrt{2})v = x(a - b\sqrt{2})v \in I$ since $x \in I$, $(a - b\sqrt{2})v \in R$, and $I \triangleleft R$. Combining these facts, we see that $3u + tv = 1 \in I$; we conclude that $I = R$ and (3) is maximal.

(b) Show that the principal ideal $(7) = 7R \triangleleft R$ is not maximal.

(Can you "factor" 7 in R ?)

Solution: Observe that $7 = (3 - \sqrt{2})(3 + \sqrt{2})$. We claim that $(7) \subsetneq (3 + \sqrt{2}) \subsetneq R$.

Suppose that $3 + \sqrt{2} \in (7)$. Then there is $a + b\sqrt{2} \in R$ with $3 + \sqrt{2} = 7(a + b\sqrt{2}) = 7a + 7b\sqrt{2}$ which holds if and only if $7a = 3$ and $7b = 1$. This contradicts the fact that $a, b \in \mathbb{Z}$. Hence, we have $(7) \subsetneq (3 + \sqrt{2})$.

Suppose that $1 \in (3 + \sqrt{2})$. Then there is $a + b\sqrt{2} \in R$ with $1 = (3 + \sqrt{2})(a + b\sqrt{2}) = (3a + 2b) + (a + 3b)\sqrt{2}$, which holds if and only if $3a + 2b = 1$ and $a + 3b = 0$. But $a + 3b$ implies that $a = -3b$; substituting in $3a + 2b = 1$ yields $3(-3b) + 2b = -7b = 1$, which contradicts the fact that $b \in \mathbb{Z}$. Hence, we have $(3 + \sqrt{2}) \subsetneq R$.

(c) Let $p \neq 2$ be prime. Can you conjecture (and prove) a general rule for when

$(p) = pR \triangleleft R$ is maximal?

Solution: It is a fact that $(p) \triangleleft R$ is maximal if and only if $p \equiv 3, 5 \pmod{8}$. This is a special case of a more general phenomenon. Let $m \equiv 2, 3 \pmod{4}$ be a square-free integer, and let $p \nmid 4m$ be prime. Then we have $(p) \triangleleft \mathbb{Z}[\sqrt{m}]$ if and only if the congruence $x^2 \equiv 4m \pmod{p}$ does not have a solution. In terms of the Legendre symbol from number theory, this condition is that the Legendre symbol $\left(\frac{m}{p}\right) = -1$.