

NAME:

Write your answers in the space provided. Do not hand in loose sheets. You are allowed a letter size two-sided aid sheet. You may use any facts in the book or proved in class. You have 80 minutes.

1. [40]

(a) Complete the following definition:

A proper ideal I of a commutative ring R is said to be prime if and only if for any $a, b \in R$, _____.
 $ab \in I \Rightarrow a \in I$ or $b \in I$.

(b) Let $\phi : R \rightarrow R'$ be a homomorphism of unital commutative rings. Let I' be a prime ideal of R' . Prove that the ideal $\phi^{-1}(I')$ of R is prime.

The Ring Homomorphism Theorem implies that $\phi^{-1}(I')$ is an ideal of R . Since ϕ is a homomorphism of unital rings, $\phi(1_R) = 1_{R'}$. Since I' is a proper ideal of R' , $\phi(1_R) = 1_{R'} \notin I'$, which implies that $1_R \notin \phi^{-1}(I')$. So, $\phi^{-1}(I')$ is a proper ideal of R .

Let $a, b \in R$ such that $ab \in \phi^{-1}(I')$. Then $\phi(a), \phi(b) \in R'$ and $\phi(a)\phi(b) = \phi(ab) \in I'$. Since I' is a prime ideal of R' , we have $\phi(a) \in I'$ or $\phi(b) \in I'$. It follows that $a \in \phi^{-1}(I')$ or $b \in \phi^{-1}(I')$. This shows that $\phi^{-1}(I')$ is prime.

(c) Complete the following definition:

A proper ideal I of a commutative ring R is said to be maximal if and only if for any ideal J of R , _____.
 $I \subset J \Rightarrow J = I$ or $J = R$.

(d) Give an example of a homomorphism of unital commutative rings $\phi : R \rightarrow R'$ and a maximal ideal I' of R' , such that $\phi^{-1}(I')$ is *not* a maximal ideal of R .

The idea is to try to find an R' with very few ideals and R with some non maximal proper ideals. Consider the inclusion map $\phi : \mathbb{Z} \rightarrow \mathbb{Q}$, $x \mapsto x$. Since \mathbb{Q} is a field, (0) is a (the only) maximal ideal of \mathbb{Q} . But the pre-image under ϕ is (0) in \mathbb{Z} , which is not a maximal ideal of \mathbb{Z} .

2. [30]

(a) Let $f = x^3 + 3x^2 + 4x + 2 \in \mathbb{Q}[x]$. Verify that -1 is a root of f .

Plugging it in, we find $f(-1) = 0$.

(b) Find all irreducible monic polynomials in $\mathbb{Q}[x]$ that divide the f in (a). You must show that the list you have found is complete.

To find all irreducible divisors of f , we do long division $f/(x+1)$, and we find $f/(x+1) = x^2 + 2x + 2$. Now this is irreducible because otherwise it would have to factor into two linear polynomials over \mathbb{Q} . But it is equal to $(x+1)^2 + 1$, which has no root in \mathbb{Q} . So it cannot factor into two linear polynomials over \mathbb{Q} . So it is irreducible, and we have $f = (x+1)(x^2 + 2x + 2)$. By the Unique Factorization Theorem, $x+1, x^2 + 2x + 2$ are the only irreducible monic polynomials over \mathbb{Q} which divide f .

(c) Find a complex number $\alpha \in \mathbb{C}$ which is algebraic over \mathbb{Q} , of degree 2, such that the field $\mathbb{Q}(\alpha)$ contains all roots of f . You must prove that your choice of α has the required property.

Note that $-1 \pm \sqrt{-1}$ are the roots of $x^2 + 2x + 2$. It follows that $\mathbb{Q}(-1 + \sqrt{-1}) = \mathbb{Q}(\sqrt{-1})$ contains all roots of f . Since $x^2 + 2x + 2$ is an irreducible polynomial over \mathbb{Q} of degree 2, $-1 + \sqrt{-1}$ is algebraic over \mathbb{Q} , of degree 2.

3. [30] Let α satisfy the relation

$$\alpha^3 + \alpha^2 + \alpha + 2 = 0.$$

Express α^4 , $(\alpha^2 + \alpha + 1)(\alpha + \alpha)$ and $(\alpha - 1)^{-1}$ in the form

$$a\alpha^2 + b\alpha + c$$

with $a, b, c \in \mathbb{Q}$.

We have

$$\alpha^3 = -\alpha^2 - \alpha - 2.$$

So,

$$\alpha^4 = -\alpha^3 - \alpha^2 - 2\alpha = -\alpha + 2.$$

$$(\alpha^2 + \alpha + 1)(\alpha + \alpha) = (\alpha^3 + \alpha^2 + \alpha)2 = -4.$$

Next, we find $a, b, c \in \mathbb{Q}$ such that

$$(\alpha - 1)(a\alpha^2 + b\alpha + c) = 1.$$

Expanding the left side, substituting $\alpha^3 = -\alpha^2 - \alpha - 2$, and matching coefficients of $1, \alpha, \alpha^2$, we have

$$b - 2a = 0, \quad c - b - a = 0, \quad -c - 2a = 1.$$

Solving this yields

$$a = -1/5, \quad b = -2/5, \quad c = -3/5.$$

So

$$(\alpha - 1)^{-1} = -\frac{1}{5}(\alpha^2 + 2\alpha + 3).$$

4. (Bonus) Let F be a finite field with q elements. In class, we proved that if α is algebraic over F , then the cardinality of $F(\alpha)$ is a power of q . In no more than 10 lines, prove that if E is a finite field containing F as a subfield, then the cardinality of E is also a power of q .

Since E is finite, there exists a finite number of elements $\alpha_1, \dots, \alpha_n \in E$ such that $E = F(\alpha_1, \dots, \alpha_n)$. We now do induction on n . If $n = 1$, then we know that $\#F(\alpha_1)$ is a power of q by the result in class. Suppose $\#F(\alpha_1, \dots, \alpha_{n-1})$ is a power of q , say q^m . Then $E = F(\alpha_1, \dots, \alpha_n)$ is an extension field of $F(\alpha_1, \dots, \alpha_{n-1})$ by adjoining α_n . By the class result again, $\#E$ is a power of q^m , which is of course a power of q too.