

## HW ASSIGNMENT #8 (DUE THURSDAY, NOVEMBER 6)

Read Sections VIII.2 and VIII.3 in the course textbook. Then do the following exercises:

1. Let  $G$  be an abelian group, and assume that  $G$  has elements of order  $k$  and  $h$ , respectively. Prove that  $G$  has an element of order  $\text{LCM}(k, h)$ . [This result was used in our proof of the fact that a finite subgroup of the multiplicative group of a field is cyclic.]
2. Let  $R$  be a commutative ring with identity. For ideals  $I, J$  of  $R$ , if  $P$  is a prime ideal containing  $IJ$ , prove that either  $P$  contains  $I$  or  $P$  contains  $J$ .
3. (Knapp §VIII.12 # 17) Let  $\varphi : \mathbf{C}[x, y] \rightarrow \mathbf{C}[t]$  be the homomorphism defined by  $\varphi(x) = t^2, \varphi(y) = t^3$ , and  $\varphi(c) = c$  for  $c \in \mathbf{C}$ . Find the kernel and image of  $\varphi$ .
4. Let  $\varphi : R \rightarrow S$  be a homomorphism of commutative rings with identity.
  - (a) (Knapp §VIII.12 #9) If  $P$  is a prime ideal of  $S$  and  $\varphi(1) = 1$ , prove that  $\varphi^{-1}(P)$  is a prime ideal of  $R$ . Give an example to show that this need not be the case if  $\varphi(1) \neq 1$ .
  - (b) If  $M$  is maximal ideal of  $S$  and  $\varphi$  is surjective, prove that  $\varphi^{-1}(M)$  is a maximal ideal of  $R$ . Give an example to show that this need not be the case if  $\varphi$  is not surjective.
5. Let  $R$  be a commutative ring with identity, and let  $a \in R$ . Let  $n$  and  $m$  be positive integers. Prove that the ideal of  $R$  generated by  $a^n - 1$  and  $a^m - 1$  is the same as the ideal generated by  $a^d - 1$ , where  $d = \text{GCD}(m, n)$ .
6. A commutative ring  $R$  with identity is called a *local ring* if it has a unique maximal ideal.

- (a) Prove that if  $R$  is a local ring with maximal ideal  $M$ , then every element of  $R - M$  is a unit.
  - (b) Conversely, if the set of non-units in  $R$  forms an ideal  $M$ , prove that  $R$  is a local ring and that  $M$  is its maximal ideal.
  - (c) Find all commutative rings  $R$  with identity such that  $R$  has a unique maximal ideal and the group of units of  $R$  is trivial.
  - (d) Prove that the ring of all rational numbers whose denominator is odd is a local ring whose unique maximal ideal is the principal ideal generated by 2.
7. If  $R$  is a commutative ring with 1, prove that the following are equivalent: (i)  $R$  has a unique prime ideal; (ii) every element of  $R$  is either nilpotent or a unit; (iii)  $R/N(R)$  is a field, where  $N(R)$  is the nilradical of  $R$ .
8. (Knapp §VIII.12 #5) Let  $R$  be an integral domain which is not a field.
- (a) Prove that there is a nonzero prime ideal in  $R[x]$  that is not maximal.
  - (b) Prove that there is an ideal in  $R[x]$  that is not principal.
9. Let  $p$  be an odd prime. A *quadratic residue mod  $p$*  is an element of the set  $\{x^2 : x \in \mathbf{F}_p\} \subset \mathbf{F}_p$ .
- (a) Use the cyclicity of  $\mathbf{F}_p^*$  to prove that there are exactly  $(p-1)/2$  nonzero quadratic residues mod  $p$  and  $(p-1)/2$  quadratic non-residues.
  - (b) Prove that the product of two quadratic non-residues mod  $p$  is a quadratic residue mod  $p$ .
  - (c) Show that  $a \in \mathbf{F}_p^*$  is a quadratic residue mod  $p$  iff  $a^{(p-1)/2} \equiv 1 \pmod{p}$ .
  - (d) If  $b \in \mathbf{F}_p$  is a quadratic non-residue, prove that  $\mathbf{F} = \mathbf{F}_p[x]/(x^2 - b)$  is a field with  $p^2$  elements, and describe explicitly the addition and multiplication laws on  $\mathbf{F}$ .
  - (e) If  $b' \in \mathbf{F}_p$  is another quadratic non-residue and  $\mathbf{F}' = \mathbf{F}_p[x]/(x^2 - b')$ , find an explicit isomorphism between  $\mathbf{F}$  and  $\mathbf{F}'$ . [**Hint:** Use part (b).]