Math 534
Problem Set 8

due Thursday, November 8, 2018

1. Let $\varphi\colon R \to S$ be a homomorphism of commutative rings with 1. Show that if P is a prime ideal in S, then $\varphi^{-1}(P)$ is a prime ideal in R.

2. Let G be a finite subgroup of the multiplicative group $F^\times$ of a field F.

   (a) Let d be a divisor of $|G|$. Show that G contains at most d elements whose order divides d.

   (b) Let $|G| = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ be the prime factorization of $|G|$. Show that for each $i = 1, 2, \dots, r$, there is an element of order $p_i^{e_i}$ in G. (Hint: First think about the case $r = 1$.)

   (c) Show that G contains an element of order $|G|$, and conclude that G is a cyclic group.

3. In this exercise, we denote by $\mathbb{F}_p$ the field with p elements.

   (a) Let $g(x) \in \mathbb{F}_p[x]$ be an irreducible monic polynomial of degree $n \geq 1$. Show that $F = \mathbb{F}_p[x]/(g(x))$ is a field with $q = p^n$ elements.

   (b) Show that $g(x)$, when considered as a polynomial in $F[x]$, has a root in F.

   (c) Show that every element of F is a root of the polynomial $x^q - x$. (Hint: Use Lagrange's theorem.)

   (d) Show that, in the polynomial ring $\mathbb{F}_p[x]$, the gcd of the two polynomials $g(x)$ and $x^q - x$ is not equal to 1.

   (e) Conclude that $g(x)$ divides $x^q - x$ in the ring $\mathbb{F}_p[x]$.

4. Let F be a field. Prove that the additive group $(F, +)$ is not isomorphic to the multiplicative group $(F^\times, \cdot)$.

5. Show that the polynomial $(x-1)(x-2)\cdots(x-n)+1$ is irreducible in the ring $\mathbb{Z}[x]$ for all $n \geq 1$, except when $n = 4$.

6. Let F be a field. Let R be the set of polynomials in $F[x]$ whose coefficient of x is equal to 0. Show that R is a subring of $F[x]$, and that R is not a UFD.

7. Show that the ideal $(x,y)^n = (x^n, x^{n-1}y, \ldots, y^n)$ in the ring $\mathbb{Q}[x,y]$ cannot be generated by fewer than $n+1$ elements.

8. Let R be a UFD, and F its field of fractions. Call a polynomial $f(x) \in R[x]$ *primitive* if the gcd of its coefficients is equal to 1.

   (a) Show that if $p \in R$ is irreducible, then the constant polynomial p is irreducible in $R[x]$.

   (b) Show that if $f(x) \in R[x]$ is primitive, and irreducible in $F[x]$, then $f(x)$ is irreducible in $R[x]$.

   (c) Suppose that we have two factorizations

   $$p_1 \cdots p_k \cdot f_1(x) \cdots f_m(x) = q_1 \cdots q_\ell \cdot g_1(x) \cdots g_n(x)$$

   in the ring $R[x]$, with $p_i, q_i \in R$ irreducible, and $f_i(x), g_i(x) \in R[x]$ primitive and irreducible in $F[x]$. Prove that $k = \ell$, $m = n$, and that the factors on both sides are equal up to reordering and multiplication by units (in R).