Abstract Algebra Prelim Aug. 2013

1. Let p and q be prime numbers such that $p < q$ and $q \not\equiv 1 \bmod p$. Show every group of order pq is abelian. (In fact it is cyclic, but it is not required to show that.)

2. Let G be a group.

   (a) For a nonempty subset S of G, define what the subgroup of G generated by S is.

   (b) For each positive integer n, let H_n be the subgroup of G generated by the nth powers of elements of G. Prove $H_n \lhd G$.

3. Let R be a commutative ring and M and N be R-modules. There are R-module homomorphisms $i\colon M \to M \oplus N$ and $j\colon N \to M \oplus N$ given by $i(m) = (m, 0)$ and $j(n) = (0, n)$.

   (a) Prove the universal mapping property of the direct sum of M and N: for any R-module P and any R-module homomorphisms $f\colon M \to P$ and $g\colon N \to P$, there exists exactly one R-module homomorphism $h\colon M \oplus N \to P$ such that $h \circ i = f$ and $h \circ j = g$.

   (b) Prove that the universal mapping property in part (a) characterizes $M \oplus N$ up to isomorphism: if there is an R-module U and R-module homomorphisms $i_U\colon M \to U$ and $j_U\colon N \to U$ such that U, i_U, j_U have the universal mapping property of $M \oplus N, i, j$ in part (a), then there is a unique R-module isomorphism $\varphi\colon M \oplus N \to U$ such that $\varphi \circ i = i_U$ and $\varphi \circ j = j_U$.

4. (a) Define a Euclidean domain.

   (b) Prove that every Euclidean domain is a PID.

   (c) Let F be a field and $a(x)$ and $b(x)$ be polynomials such that neither divides the other. Let $g(x)$ be the greatest common divisor of $a(x)$ and $b(x)$. (You can normalize $g(x)$ to have leading coefficient 1, although that isn't important.) Show there are nonzero $u(x)$ and $v(x)$ in $F[x]$ such that

   - $a(x)u(x) + b(x)v(x) = g(x)$,
   - $\deg u < \deg b$ and $\deg v < \deg a$.

5. Let p be a prime number and $f(x)$ be a polynomial in $\mathbf{Z}[x]$. Prove that the ideal $(p, f(x))$ in $\mathbf{Z}[x]$ is maximal if and only if the reduction $f(x) \bmod p$ is irreducible in $(\mathbf{Z}/(p))[x]$.

6. Give examples as requested, with brief justification.

   (a) A nontrivial character of $\mathbf{Z}/(9)$.

   (b) A polynomial $f(x)$ such that $(x^2 - x, x^2 - 1) = (f(x))$ in $\mathbf{Q}[x]$.

   (c) A basis of the vector space of 2×2 real matrices with trace 0.

   (d) An integral domain that is not a unique factorization domain.