Last revised: March 3, 2014

A.Miller M542
www.math.wisc.edu/∼miller/

Each Problem is due one week from the date it is assigned. Do not hand them in early. Please put them on the desk in front of the room at the beginning or end of class. Include the statement of the problem as part of your solution.

The date the problem was assigned in class is in parentheses.

Theorem 1 *(Chinese remainder theorem) Given n, m relatively prime integers for every $i, j \in \mathbb{Z}$ there is an $x \in \mathbb{Z}$ such that $x = i \mod n$ and $x = j \mod m$.*

Problem 1 *(Fri Jan 24) (a) Find an integer x such that $x = 6 \mod 10$ and $x = 15 \mod 21$ and $0 \leq x \leq 210$. (b) Find the smallest positive integer y such that $y = 6 \mod 10$ and $y = 15 \mod 21$ and $y = 8 \mod 11$.*

Problem 2 *(Fri Jan 24) (a) Find integers i, j such that there is no integer x with $x = i \mod 6$ and $x = j \mod 15$. (b) Find all pairs i, j with $i = 0, 1, \ldots 5$ and $j = 0, 1, \ldots, 14$ such that there is an integer x with $x = i \mod 6$ and $x = j \mod 15$.*

Theorem 2 *$\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$ iff n, m are relatively prime.*

Lemma 3 *Suppose n, m are relatively prime, G is a finite abelian group such that $x^{nm} = e$ for every $x \in G$. Let $G_n = \{x \in G \ : \ x^n = e\}$ and $G_m = \{x \in G \ : \ x^m = e\}$. Then*

- *G_n and G_m are subgroups of G,*
- *$G_n \cap G_m = \{e\}$,*
- *$G_n G_m = G$, and therefore*
- *$G \simeq G_n \times G_m$*

Corollary 4 *(Decomposition into p-groups) Suppose G is an abelian group and $|G| = p_1^{i_1} \cdot p_2^{i_2} \cdots p_n^{i_n}$ where $p_1 < p_2 < \cdots < p_n$ are primes. Then*

$$G \simeq G_1 \times G_2 \times \cdots \times G_n$$

where for each j if $x \in G_j$ then $x^{n_j} = e$ where $n_j = p_j^{i_j}$.

Problem 3 *(Mon Jan 27) Prove that for any n there is only one abelian group (up to isomorphism) of size n iff n is square-free. Square-free mean that no p^2 divides n for p a prime.*

Lemma 5 *Suppose G is a finite abelian p-group and $a \in G$ has maximum order, then there exists a subgroup $K \subseteq G$ such that*

- $\langle a \rangle \cdot K = G$ *and*
- $\langle a \rangle \cap K = \{e\}$.

The proof given in class is like the one in Gallian or Judson.

Theorem 6 *Any finite abelian group is isomorphic to a product of cyclic groups each of which has prime-power order.*

Problem 4 *(Wed Jan 29) Let G be a finite abelian group. Prove that the following are equivalent*

1. *For every subgroup H of G there is a subgroup K of G with $HK = G$ and $H \cap K = \{e\}$.*
2. *Every element of G has square-free order.*

Hint: Polya's Dictum: "If you can't do a problem, then there is an easier problem you can't do. Find it."

Lets call property (1) the Complementation Property for G or CP for short. Here are some easier problems:

(a) Prove that C_{p^2} fails to have CP.

(b) Prove that $C_p \times C_p$ has CP.

(c) Let $|G|$ and $|H|$ be relatively prime. Prove that $G \times H$ has CP iff both G and H have CP.

Theorem 7 *(Uniqueness) Suppose*

$$C_{p^{n_1}} \times C_{p^{n_1}} \times \cdot \times C_{p^{n_k}} \simeq C_{p^{m_1}} \times C_{p^{m_1}} \times \cdot \times C_{p^{m_l}}$$

where $n_1 \geq n_2 \geq \cdots n_k \geq 1$ *and* $m_1 \geq m_2 \geq \cdots m_l \geq 1$. *Then* $k = l$ *and* $n_i = m_i$ *for all* i.

Problem 5 *(Fri Jan 31) How many abelian groups of order 144 are there up to isomorphism? Explain.*

Problem 6 *(Mon Feb 3) Suppose* G_1, G_2, H_1, H_2 *are finite abelian groups,* $G_1 \times G_2 \simeq H_1 \times H_2$ *and* $G_1 \simeq H_1$. *Prove that* $G_2 \simeq H_2$.

Give a counterexample if the word finite is dropped, i.e., $G_1 \times G_2 \simeq H_1 \times H_2$ *and* $G_1 \simeq H_1$ *but* G_2 *is not isomorphic to* H_2.

I do not know if problem 6 is true or false for finite non-abelian groups.

For the group G acting on the set X the orbit of $a \in X$ is

$$orb(a) =^{def} \{ga \ : \ g \in G\} \subseteq X.$$

Proposition 8 *Orbits are either disjoint or the same.*

Problem 7 *(Wed Feb 5) Prove or disprove:*

For any finite abelian groups G_1 *and* G_2 *with subgroups,* $H_1 \subseteq G_1$ *and* $H_2 \subseteq G_2$ *such that* $H_1 \simeq H_2$, *if* $G_1/H_1 \not\simeq G_2/H_2$ *then* $G_1 \not\simeq G_2$.

For a given group action of group G on set X, define $Stab(a) = \{g \in G \ : \ ga = a\}$ for each $a \in X$. Called stabilizer or fixed subgroup.

Proposition 9 *Stab*(a) *is a subgroup of* G.

Problem 8 *(Wed Feb 5) Prove that* $Stab(ga) = g\, Stab(a)\, g^{-1}$.

For $H \subseteq G$ a subgroup the index of H, $[G : H]$ is the number of H-cosets, $|\{gH \ : \ g \in G\}|$. Lagrange's Theorem says $|G| = [G : H] \cdot |H|$.

Proposition 10 *(Orbit-stabilizer formula)* $|orb(a)| = [G : Stab(a)]$.

The conjugacy action of G on G is given by $(g,h) \to ghg^{-1}$. Under this action the orbits are called the conjugacy classes. $Z(G)$ the center of G is the subgroup of all elements of G which commute with every other element of g. Equivalently it is the set of elements of G with orbits (conjugacy classes) of size one. $C(g) = Stab(g)$ is called the centralizer subgroup of g.

Theorem 11 *(Class formula) If* $conj(g_1)$, $\cdots$, $conj(g_n)$ *are the conjugacy classes of size greater than one, then*

$$|G| = |Z(G)| + \sum_{k=1}^{n} [G : C(g_k)]$$

Theorem 12 *(Cauchy) If* p *is a prime which divides* $|G|$*, then* G *has an element of order* p*.*

Group-discussion-graded Problem 9 *This is due in lecture on valentines day. It will be graded in class so do not hand-in.*

(a) Suppose G *is a finite abelian group which contains an element which has non-square-free order. Prove that for some prime* p *it has an element of order* p^2*.*

(b) Suppose a *is an element of a finite abelian group* G *with order* p^2 *let* $b = a^p$*, let* $H =< b >$ *be the subgroup generated by* b *and suppose* K *is a subgroup of* G *with* $K \cap H = \{e\}$*. Prove that* a *is not an element of* HK*.*

(c) Suppose G_1, G_2 *are finite abelian groups with* $|G_1|$ *and* $|G_2|$ *relatively prime. Show that for any subgroup* $H \subseteq G_1 \times G_2$ *there are subgroups* $H_1 \subseteq G_1$ *and* $H_2 \subseteq G_2$ *such that* $H = H_1 \times H_2$*. (Warning: the relatively prime hypothesis is necessary.)*

(d) Suppose G_1, G_2 *are finite abelian groups with* $|G_1|$ *and* $|G_2|$ *relatively prime. Show that if* G_1 *and* G_2 *both have the CP then* $G_1 \times G_2$ *has CP.*[1]

(e) Prove that $C_p \times C_p \times \cdots \times C_p$ *has the CP.*

(f) Prove Problem 4.

[1] CP is defined after Problem 4.

Corollary 13 *Groups of order p^2 are abelian.*

Theorem 14 *(Sylow 1) If G is a finite group and p^n divides $|G|$, then there exists a subgroup $H \subseteq G$ with $|H| = p^n$.*

Proposition 15 *Any two n-cycles in S_N are conjugates. If $\tau = c_1 c_2 \cdots c_n$ and $\rho = c_1' c_2' \cdots c_n'$ are disjoint cycle decomposition with $|c_i| = |c_i'|$ all i, then τ and ρ are conjugates. Similarly for the converse.*

Problem 10 *(Mon Feb 10) Prove for any $n \geq 3$ that $Z(S_n) = \{id\}$.*

Definition 16 *$H \subseteq G$ is a p-subgroup iff its order is a power of p. $P \subseteq G$ is a p-Sylow subgroup of G iff $|P| = p^n$ where $|G| = p^n m$ and p does not divide m.*

Theorem 17 *(Sylow 2) If G is a finite group, H a p-subgroup of G, and P a p-Sylow subgroup of G, then there exists $g \in G$ such that $H \subseteq gPg^{-1}$.*

Corollary 18 *Let G be a finite group such that p divides $|G|$.*

(a) Any p-subgroup of G is contained in a p-Sylow subgroup of G.

(b) Any two p-Sylow subgroups of G are conjugates.

(c) Any two p-Sylow subgroups of G are isomorphic.

(d) A p-Sylow subgroup of G is normal iff it is the only p-Sylow subgroup of G.

Theorem 19 *(Sylow 3) If $|G| = p^n m$ where p does not divide m and $n(p)$ is the number of p-Sylow subgroups of G, then:*

(a) $n(p) = [G : N(P)]$ for any P a p-Sylow subgroup of G,

(b) $n(p)$ divides m, and

(c) $n(p) = 1 \mod p$

Problem 11 *(Wed Feb 12)*

(a) Prove that there are no simple groups of order either 575 or 272.

(b) For any prime p prove there are no simple groups of order $p(p-1)$ or $p(p+2)$.

Theorem 20 *If $p < q$ are primes and q is not $1 \mod p$, then every group of order pq is abelian.*

Problem 12 *(Fri Feb 14) Question (August J.) Suppose every subgroup of finite group G is a normal subgroup. Must G be abelian?*

Problem 13 *(Fri Feb 14)*

(a) Suppose P is a p-Sylow subgroup of G and H a subgroup such that $P \triangleleft H$ and $H \triangleleft G$. Prove that $P \triangleleft G$.

(b) If $K \triangleleft H$ and $H \triangleleft G$, does it follow that $K \triangleleft G$? Show that the answer is No. Consider $G = S_4$, $K = \{id, \sigma\}$ where $\sigma = (12)(34)$ and $H = \{id, \sigma, \tau, \rho\}$ where τ and ρ are conjugates of σ. Determine what τ and ρ are and show that $K \triangleleft H$ and $H \triangleleft G$, but K is not a normal subgroup of G.

Theorem 21 *$aut(\mathbb{Z}_p, +_p)$ is isomorphic to $(\mathbb{Z}_p^x, \times_p)$ the multiplicative group of nonzero elements.*

Example 22 *If $p < q$ are primes, then there is a twisted product of $\mathbb{Z}_p$ and $\mathbb{Z}_q$ which has order pq and is not abelian.*

Problem 14 *(Mon Feb 17) Suppose for every $x \in G$ that $x^2 = e$. Prove that G is abelian.*

Problem 15 *(Mon Feb 17) Suppose $H \subseteq G$ is subgroup of index 2, i.e., $[G : H] = 2$. Prove that it is a normal subgroup of G.*

Theorem 23 *Suppose that $p(x)$ is a polynomial over the field F and for some $\alpha \in F$ $p(\alpha) = 0$. Then $p(x) = (x - \alpha)q(x)$ for some polynomial $q(x)$.*

Corollary 24 *Any polynomial $p \in F[x]$ of degree $\leq n$ with more than n roots must be identically zero.*

Theorem 25 *Let the exponent of G be the least n such that $x^n = e$ for every $x \in G$. If G is finite abelian group then G is cyclic iff $exp(G) = |G|$.*

Corollary 26 *The multiplicative group of a finite field is cyclic.*

Problem 16 *(Wed Feb 19) For F a finite field call $a \in F$ a generator of F iff every nonzero element of F is a power of a.*

(a) Find a generator of $\mathbb{Z}_7$.

(b) How many generators does $\mathbb{Z}_{17}$ have?

(c) How many generators does $\mathbb{Z}_{31}$ have?

Theorem 27 *If $p < q$ are primes and $q = 1 \bmod p$, then up to isomorphism there is a unique nonabelian group of order pq.*

For elementary results on vector spaces see:
`http://www.math.wisc.edu/~miller/old/m542-00/vector.pdf`

Lemma 28 *(Exchange Lemma) Suppose* $\text{span}(A \cup B) = V$ *and* $a \notin \text{span}(A)$. *Then there exists* $b \in B$ *such that* $\text{span}(A \cup \{a\} \cup (B \setminus \{b\})) = V$.

Theorem 29 *Every vector space has a basis. Any two bases have the same cardinality.*

Corollary 30 *Any finite field F of characteristic p has cardinality p^n for some integer n.*

Problem 17 *(Fri Feb 21) Prove that $v_1, v_2, \ldots, v_n$ are linearly dependent iff $v_1 = \vec{0}$ or $v_{i+1} \in \text{span}\{v_1, v_2, \ldots, v_i\}$ for some i with $1 \leq i < n$.*

Theorem 31 *(Kronecker) If $p(x) \in F[x]$ is a non-constant polynomial, then there exists a field $E \supseteq F$ and $\alpha \in E$ with $p(\alpha) = 0$.*

Problem 18 *(Mon Feb 24) Let R be a commutative ring with 1. Let I be a maximal ideal in R. Suppose $ab = 0$. Prove that $a \in I$ or $b \in I$.*

Problem 19 *(Mon Feb 24) Consider $p(x) = x^3 + x + 1$ as a polynomial in $\mathbb{Z}_2[x]$. Suppose p has a root α is in some field extension. Construct the multiplication table for*

$$\mathbb{Z}_2[\alpha] =^{def} \{a + b\alpha + c\alpha^2 \ : \ a, b, c \in \mathbb{Z}_2\}$$

Corollary 32 *(Kronecker) If $p(x) \in F[x]$ is a polynomial of degree n, then there exists a field $E \supseteq F$ and $\alpha_i \in E$ such that*

$$p(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

Theorem 33 *If $p(x) \in F[x]$ is irreducible and α, β are roots in some extension fields of F then $F(\alpha)$ and $F(\beta)$ are isomorphic via an isomorphism which fixes F.*

Corollary 34 *If $p(x) \in F[x]$ is irreducible and splits in an extension field E of F then the multiplicity of each root of p is the same.*

Problem 20 *(Wed Feb 26) Let α be transcendental over $\mathbb{Z}_2$. Let $F = \mathbb{Z}_2(\alpha)$ and let $p(x) = x^2 - \alpha$.*

(a) Prove that p is irreducible over F.

(b) Prove that if β is a root of p in some some extension field, then $p(x) = (x - \beta)^2$.

(c) Suppose that F is a finite field of characteristic 2. Prove that for every $a \in F$ there is a $b \in F$ such that $b^2 = a$.

(d) Suppose that F is a finite field of odd characteristic. Prove that there exists $a \in F$ for every $b \in F$ such that $b^2 \neq a$.

(e) Find a field F and an irreducible polynomial $p(x)$ of degree three such that in any extension field in which p splits there exist a β such that $p(x) = (x - \beta)^3$.

Theorem 35 *The formal derivative for an abstract polynomial $f(x) \in F[x]$ satisfies the usual derivative laws:*

(a) If $a \in F$ and $f \in F[x]$, then $(af)' = af'$.

(b) If $f, g \in F[x]$, then $(f + g)' = f' + g'$.

(c) If $f, g \in F[x]$, then $(fg)' = f'g + fg'$.

Problem 21 *(Fri Feb 28) Prove that the formal derivative for polynomials in $F[x]$ satisfies*

(a) The power rule: $(f^n)' = n(f^{n-1})f'$

(b) The chain rule: $f(g(x))' = f'(g(x))g'(x)$

Theorem 36 *For any $\alpha \in F$ and $f \in F[x]$*
α is repeated root of f iff it is a root of f'.

Corollary 37 *The roots of an irreducible polynomial in a field of characteristic zero, are always distinct.*

Lemma 38 *If E is any field of characteristic p, then for any $\alpha, \beta \in E$*

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$$

Theorem 39 *For any p^n and there is a field F with $|F| = p^n$.*

Problem 22 *(Mon Mar 3) Prove for any prime p and positive integer n that p divides $\begin{pmatrix} p^n \\ k \end{pmatrix}$ for any k with $0 < k < p^n$.*

Definition 40 *For fields $F \subseteq E$ define $[E : F]$ to be the dimension of E viewed as a vector space over F.*

Theorem 41 *For fields $F \subseteq K \subseteq E$*

$$[E : F] = [E : K] \cdot [K : F]$$

Theorem 42 *For $p(x) \in F[x]$ irreducible and α a root of p in some extension field, $[F[\alpha] : F]$ is the degree of p.*

Theorem 43 *If $E \supseteq F$ is the splitting field of some polynomial in $F[x]$, then $[E : F]$ is finite.*

Theorem 44 *If $[E : F]$ is finite and $\alpha \in E$, then there is an irreducible polynomial $p \in F[x]$ with $p(\alpha) = 0$.*