Last revised: May 16, 2014

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

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.*

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.*

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.*

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.

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 $G_1 \not\simeq G_2$.

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

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.

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

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 $p(p+2)$.

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.

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

[1] CP is defined after Problem 4.

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*.*

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?*

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

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*

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

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* $p(x) = (x - \beta)^3$*.*

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: $f(g(x))' = f'(g(x))g'(x)$

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

Problem 23 *(Wed Mar 5) p is a prime and n a positive integer. Prove:*

(a) If F is a field such that $|F| = p^n$ and m is a positive integer then there is a field E with $F \subseteq E$ and $E = p^{nm}$.

(b) If $F \subseteq E$ are fields, $|F| = p^n$ and $|E| = p^N$, then n divides N.

Problem 24 *(Wed Mar 26) Prove or disprove:*

Using a straight edge and compass it is possible to construct an equilateral triangle with area 1.

Problem 25 *(Fri Mar 28) Prove that $[F_c : \mathbb{Q}]$ is infinite. F_c is the field of constructible reals (straight edge and compass).*

Problem 26 *(Fri Mar 28) Prove that if $2^m - 1$ is prime, then m is prime.*

Problem 27 *(Mon Mar 31) Find the roots of*

$$x^3 + 3x^2 + 6x + 5 = 0$$

using addition, subtraction, multiplication, division, and extraction of roots, i.e., solvability by radicals.

Problem 28 *(Wed Apr 2) Suppose $[F[\alpha] : F] = n$, $[F[\beta] : F] = m$, and $gcd(n, m) = 1$. Prove that $[F[\alpha, \beta] : F] = nm$.*

Problem 29 *(Fri Apr 4) Prove the following:*

(a) Suppose $\alpha + \beta$ is algebraic over F, then α is algebraic over $F[\beta]$.

(b) Suppose $\alpha + \beta$ and $\alpha\beta$ are both algebraic over F, then α is algebraic over F.

Problem 30 *(Mon Apr 7) Suppose that $F \subseteq K_1 \subseteq L$ and $F \subseteq K_2 \subseteq L$ and K_1 and K_2 are splitting fields over F. Prove that $K_1 \cap K_2$ is a splitting field over F.*

Problem 31 *(Wed Apr 9) Suppose that E is a splitting field over F and $p \in F[x]$ splits in E as $p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ where $\alpha_i \neq \alpha_j$ whenever $i \neq j$. Prove that the following are equivalent:*

(1) p is irreducible.

(2) for any i, j there is $\sigma \in \mathrm{aut}(E|F)$ such $\sigma(\alpha_i) = \alpha_j$.

Problem 32 *(Mon Apr 14) For each of the following polynomials compute its Galois group, i.e.,* $\mathrm{aut}(K|\mathbb{Q})$ *where* K *is the splitting field of the polynomial.*

(a) $x^5 - 1$
(b) $x^4 - 2$
(c) $x^4 - 2x^2 - 2$

Problem 33 *(Wed Apr 16) In the Lemma* **??** *(d) must* n *be prime?*
Prove or disprove: $\{(1,2,3,4),(1,3)\}$ *generates* S_4.

Problem 34 *(Mon Apr 21)* $\sigma, \tau \in A_5$ *are conjugate in* A_5 *iff there is* $\rho \in A_5$ *such that* $\sigma = \rho^{-1}\tau\rho$. *Prove that every element of* A_5 *except the identity is conjugate to exactly one of the following:*

(a) $(1,2,3)$
(b) $(1,2)(3,4)$
(c) $(1,2,3,4,5)$
(d) $(2,1,3,4,5)$

In particular (c) and (d) are not conjugates.

Problem 35 *(Wed Apr 23) Let* $K \supseteq \mathbb{Q}$ *be the splitting field of*

$$f(x) = (x^2+1)\cdot(x^2-2) = x^4 - x^2 - 2$$

(a) Prove that $\mathrm{aut}(K|\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$
(b) Find an irreducible polynomial $p(x)$ *whose splitting field is* K.

Problem 36 *(Mon Apr 28) Suppose* A *and* B *are matrices with real entries and there exists a matrix* P *with complex entries such that* $A = PBP^{-1}$. *Prove there exists a matrix* P *with real entries such that* $A = PBP^{-1}$.
Hint: Show $\{Q : AQ = QB\}$ *is a subspace.*