A.Miller
M542
Spring 2000
http://www.math.wisc.edu/∼miller/m542/hmwk.html

Homework is due one week from the date it is assigned.

1. (1-27) Suppose $h : G_1 \to G_2$ is a homomorphism and H_2 is a subgroup of G_2. Prove that

$$H_1 = \{x \in G_1 : h(x) \in H_2\}$$

is a subgroup of G_1.

2. (1-27) 11-34

3,4. (2-1) 11-20, 11-32

5,6. (2-3) 11-10, 11-21 Prove that the answer in the back of the book is correct.

7. (2-3) Prove: Suppose $n/m_1m_2\cdots m_k$ where $n, m_1, m_2, \ldots, m_k \in \mathbb{N}$. Then there exists $n_i \in \mathbb{N}$ such that $n = n_1n_2\cdots n_k$ and n_i/m_i for each $i = 1, 2, \ldots, k$.
Hint: Prove for $k = 2$ and then use induction.

8. (2-3) Prove: If H is a subgroup of G of index 2, then H is a normal subgroup of G.

9. (2-3) Prove: If $X \subseteq V$ where V is a vector space over F, then span(span(X)) = span(X).

Extra Credit (no time limit) Prove or disprove: If G is a finite group and $6/|G|$ then G has a subgroup of order 6.

10,11,12. (2-8) exercises 16,24,25 from handout "Vector Spaces".

13. (2-10) Let $F \subseteq E$ be fields and $\alpha \in E$.
Define

$$F(\alpha) = \bigcap\{K : (F \cup \{\alpha\}) \subseteq K^{\text{field}} \subseteq E\}$$

$$\tilde{F}(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} : f(x), g(x) \in F[x], g(\alpha) \neq 0\}$$

Prove that $F(\alpha) = \tilde{F}(\alpha)$ and that it is a field.

14. (2-10) Suppose that $\sigma : F \to F$ is an automorphism of the field F and F contains the rationals $\mathbb{Q}$. Prove that for every $r \in \mathbb{Q}$ that $\sigma(r) = r$.

15. (2-15) Suppose $n, m \in \mathbb{N}$ and $n, m \geq 2$. Prove that

$$\sqrt[n]{m} \in \mathbb{Q} \text{ implies } \sqrt[n]{m} \in \mathbb{N}$$

16. (2-15) Prove or disprove:
$F = \{a + b\sqrt{2} + c\sqrt{3} : a, b, c \in \mathbb{Q}\}$ is a field.

17. (2-17) Prove that the regular pentagon can be constructed using straight edge and compass.

18. (2-17) Suppose $\mathbb{Q} \subseteq E$ is a field and $[E : \mathbb{Q}] = 2$. Prove that there exists a square free integer n such that $E = \mathbb{Q}(\sqrt{n})$.

Extra Credit: Prove or disprove: if α is real and $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2 then α is constructible.

19. (2-24) Suppose α, β are in a extension field of F and $\alpha + \beta$ is algebraic over F. Prove that α is algebraic over $F(\beta)$.

20. (2-24) Suppose $F \subseteq E \subseteq K$ and $\alpha \in K$ and $[K : F] < \infty$. Prove:
(a) $[E(\alpha) : F(\alpha)] \leq [E : F]$
(b) $[E(\alpha) : E] \leq [F(\alpha) : F]$

21. (2-24) Suppose α, β are in an extension field of F,
$[F(\alpha) : F] = n$ and $[F(\beta) : F] = m$ and n and m are relatively prime. Prove that $[F(\alpha, \beta) : F] = nm$.

22. (2-24) Prove or **Disprove**: Suppose α, β are in an extension field of F. Then
α algebraic over $F(\beta)$ implies β algebraic over $F(\alpha)$.

23. (2-24) Suppose α, β are in an extension field of F. Prove the exchange lemma:
α algebraic over $F(\beta)$ and α transcendental over F
implies
β algebraic over $F(\alpha)$ and β transcendental over F

24. (2-29) Suppose F is a field, $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\pi)$, and $[F : \mathbb{Q}] < \infty$. Prove that $F = \mathbb{Q}$.

25. (2-29) Suppose f and g are irreducible polynomials in $F[x]$ whose degrees are relatively prime. Suppose also that in some extension field of F there is an α such that $f(\alpha) = 0$. Prove that $g(x)$ is still irreducible over $F(\alpha)$.

From now on assume all fields have characteristic zero.

26. (3-23) Solve the equation

$$x^3 + 3x^2 + 15x + 6 = 0$$

using the method of Tartaglia (not some general equations). Find all "six" roots and show which ones are equal.

27. (3-28) Suppose $[K : F] < \infty$ Prove the following are equivalent:
(a) K is a Galois extension of F
(b) for every $L \supseteq K$ and every embedding $\sigma : K \to L$ which fixes F we have that $\sigma(K) = K$.

28. (3-28) Let p be a prime and let K be a splitting field of $x^p - 1$ over $\mathbb{Q}$. Prove that $\text{aut}(K|\mathbb{Q})$ is isomorphic to $\mathbb{Z}_{p-1}$.

29. (3-28) Let $p(x) = x^4 + 1$. Prove that p is irreducible over $\mathbb{Q}$ but there exists a Galois extension $K \supseteq \mathbb{Q}$ in which p is reducible but does not split.

30. (3-30) Compute the Galois group of $x^3 - 3x + 1$.

31. (3-30) Suppose $[E : F] < \infty$. Prove that the following are equivalent:
(a) E is a Galois extension of F
(b) For every K a Galois extension of F with $F \subseteq E \subseteq K$ $\text{aut}(K|E) \triangleleft \text{aut}(K|F)$.
(c) There exists K a Galois extension of F with $F \subseteq E \subseteq K$ $\text{aut}(K|E) \triangleleft \text{aut}(K|F)$.

32. (4-4) Suppose $F \subseteq K_1, K_2 \subseteq L$ and both K_1 and K_2 are Galois extensions of F. Prove $K_1 \cap K_2$ is a Galois extension of F.

33. (4-4) Prove that the inductive definition of solvable group is equivalent to the standard definition.

34. (4-4) Prove that a subgroup of a solvable group is solvable.

35. (4-6) Find a polynomial $p(x) \in \mathbb{Q}[x]$ of degree 7 whose Galois group is S_7 (and prove it is).

36. (4-11) Find groups H_1, H_2, H_3 such that $H_1 \triangleleft H_2$ and $H_2 \triangleleft H_3$ but H_1 is not a normal subgroup of H_3.
Hint: Use Galois groups.

37. (4-11) Let $f(x) \in \mathbb{Q}[x]$ be an irreducible cubic with one real and two nonreal roots, say α, $\beta + \gamma i$, and $\beta - \gamma i$. Let $S \subseteq \mathbb{R}$ be the smallest subfield S of the reals closed under taking real roots. Prove that $\alpha \in S$ iff $\beta \in S$ iff $\gamma \in S$.

Extra Credit: Does there exists a cubic irreducible polynomial in $\mathbb{Q}[x]$ as in problem 37 with $\alpha \notin S$?

38. (4-13) Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of odd prime degree p all of whose roots are real. Prove that f is not solvable by real radicals.

39. (4-18) Find the conjugacy classes of A_5.
Hint: They are the same as S_5 except that the five cycles are two conjugacy classes each of size 12.

$$\rho(a_1a_2a_3\cdots a_n)\rho^{-1} = (\rho(a_1)\rho(a_2)\rho(a_3)\cdots\rho(a_n))$$

Note that if $\rho \in S_n$ and τ is a transposition, then one of ρ and $\rho \circ \tau$ is in A_n.

Extra Credit. Prove that if H is a subgroup of G and $|H| = p^n$ and $|G| = p^{n+1}$, then H must be a normal subgroup of G.

40. (4-25) Prove there is no simple group of order 132.

41. (4-25) Suppose $H \triangleleft G$ and H contains a p-Sylow subgroup of G. Prove that H contains all p-subgroups of G.

42. (4-25) Suppose $x = zyz^{-1}$ in some group. Prove that $C(x) = zC(y)z^{-1}$.

43. (4-25) Suppose P is a p-Sylow subgroup of G and $P \triangleleft H \triangleleft G$. Prove that $P \triangleleft G$.

44. (4-25) Let $H = P_1 \cap P_2 \cap \cdots P_n$ where $P_1, P_2, \ldots, P_n$ are all the p-Sylow subgroups of G. Prove $H \triangleleft G$.

45. (4-25) Suppose P is a p-Sylow subgroup of G. Prove that $N(N(P)) = N(P)$.
Hint: If $a \in N(N(P))$ then P and $Q = aPa^{-1}$ are both subgroups of $N(P)$. Show $P = Q$ (and hence $a \in N(P)$).

46. (4-25) Give an example of subgroup H of a group G where $N(N(H)) \neq N(H)$. Hint $G = D_8$.

47. (4-25) Suppose $H \triangleleft G$ and P is a p-Sylow subgroup of G. Prove $H \cap P = Q$ is a p-Sylow subgroup of H.
Hint: $P \cap H$ is a p-subgroup of H and hence is contained in some Q a p-Sylow subgroup of H, $P \cap H \subseteq Q \subseteq H$. Q is a p-subgroup of G, hence $Q \subseteq aPa^{-1}$ for some $a \in G$. Show $Q = P \cap H$.

48. (5-2) 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.

49. (5-2) Show that a square complex matrix A is unitarily similar to a diagonal matrix iff $A^*A = AA^*$.

Hint: Show that if U is an upper triangular matrix, then $U^*U = UU^*$ iff U is diagonal.

50. (5-2) Show

(a) Similar matrices have the same minimal polynomial.

(b) If A is a matrix in Jordan normal form, then the minimal polynomial of A is

$$q(x) = (x - \lambda_1)^{k_1}(x - \lambda_2)^{k_2} \cdots (x - \lambda_n)^{k_n}$$

where $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the distinct eigenvalues of A (the diagonal elements of A) and for each l, k_l is the size of the largest Jordan Block with λ_l on its diagonal.