REVIEW
MATH 114

What do you have to know for the first midterm.

Groups. Definitions of a group, a subgroup, a normal subgroups and a quotient. Lagrange's theorem: the order of a subgroup divides the order of the group. Isomorphism theorems.

Action of G on a set X is the map $G \times X \to X$ such that

$$1x = x \text{ and } (gh)\,x = g\,(hx)\,.$$

A G-orbit O of $x \in X$ is the set $\{gx\}$ for all $g \in G$. The stabilizer of $x \in X$ is the subgroup $G_x = \{g \in G \mid gx = x\}$. There is the identity

$$|O||G_x| = |G|.$$

Sylow theorems. Let $|G| = p^n q$, p be prime and $(p, q) = 1$. A Sylow subgroup is a subgroup of order p^n in G. There exists at least one Sylow p-subgroup. The number of Sylow p-subgroups is 1 modulo p. All Sylow p-subgroups are conjugate.

A group G is solvable if there exist a chain of subgroups

$$G = G_1 \supset G_2 \supset \cdots \supset G_n = \{1\}$$

such that G_{i+1} is normal in G_i for all $i \leq n-1$ and G_i/G_{i+1} is abelian. If N is a solvable normal subgroup of G and G/N is solvable, then G is solvable. A subgroup and a quotient group of a solvable subgroup is solvable. A group of order p^n is solvable for any prime p and $n \geq 1$.

Fundamental theorem of abelian groups. Any finitely generated abelian group is a direct product of cyclic subgroups.

Polynomials. Irreducible polynomials, division algorithm, factorization theorem (theorem 11 in Artin). Eisenstein criterion and other ways to check if a polynomial is irreducible.

Field theory. Field extensions $F \subset E$. The degree (E/F) is the dimension of E over F. If $F \subset E \subset B$, then $(B/E)\,(E/F) = (B/F)$. Algebraic element, minimal polynomial, splitting fields, automorphism group $\operatorname{Aut} E$ and $\operatorname{Aut}_F E$. Theorems 7,8,9,10 and 13 in Artin.

Date: March 1, 2006.

Review exercises.

1. Let G be a group of order 312. Prove that G is solvable.

2. Let $n \geq 5$. Prove that a proper non-trivial normal subgroup of S_n coincides with A_n.

3. Peter makes toys by coloring the faces of wooden cubes in such way that no faces have the same color. How many different toys can he make if he has 9 colors?

4. Let p be a prime number and $x^2 + 1$ is reducible over $\mathbb{Z}_p$. Prove that $p \equiv 1 \mod 4$.

5. Find the degree of the splitting field of the polynomial $x^5 - 7$ over $\mathbb{Q}$.

6. Find the degree of the splitting field of the polynomial $x^{13} + 1$ over $\mathbb{Q}$.

7. Let F be a field. Prove that the number of irreducible polynomials in $F[x]$ is infinite.

8. Check that the number $\alpha = \cos 20^\circ$ is algebraic and find the minimal polynomial of α over $\mathbb{Q}$.

Solutions.

1. Use $312 = 3 \times 13 \times 8$. The number of 13-subgroups divides 24 and is congruent to 1 modulo 13. Therefore there is only one 13-subgroup. Denote it by N. Then N is cyclic, therefore solvable, G/N has 24 elements and therefore solvable by homework problem. Hence G is solvable.

2. Let N be a proper non-trivial subgroup of S_n. Then $N \cap A_n$ is a normal subgroup in A_n. But A_n is simple, hence $N \cap A_n = \{1\}$ or $N \cap A_n = A_n$. In the latter case $N = A_n$, since N is proper and the index of A_n in S_n is 2. If $N \cap A_n = \{1\}$, then N can contain at most one odd permutation. Indeed, if it contains two odd permutations s and t, then s^2, st be even permutations in N, hence $s^2 = st = 1$. Thus, $N = \{1, s\}$. On the other hand, one can find a permutation u such that $usu^{-1} \neq s$. But $usu^{-1} \in N$. Contradiction.

3. Let G be the group of rotations of a cube. We proved in class that G is isomorphic to S_4, in particular, $|G| = 24$. Enumerate faces in some way. There are $9 \times 8 \times 7 \times 6 \times 5 \times 4$ ways to assign a color to a number. The group G acts on the set of assignments. Each orbit has 24 elements, since the stabilizer of each color assignment is trivial. Therefore the number of orbits is

$$\frac{9 \times 8 \times 7 \times 6 \times 5 \times 4}{24} = 2520.$$

4. If $x^2 + 1$ is reducible, then it has a root $\alpha \in \mathbb{Z}_p$. Then $\alpha^2 = -1$ and $\alpha^4 = 1$. Therefore α has order 4 in the multiplicative group $\mathbb{Z}_p^\times$. By Lagrange's theorem 4 divides $|\mathbb{Z}_p^\times| = p - 1$.

5. The polynomial $x^5 - 7$ is irreducible by Eisenstein criterion and has one real root. Denote it by α. All other roots are $\alpha\omega$, $\alpha\omega^2, \alpha\omega^3$ and $\alpha\omega^4$, where ω is the fifth root of 1. Therefore the splitting field is $\mathbb{Q}(\omega, \alpha)$. Note that $(\mathbb{Q}(\omega)/\mathbb{Q}) = 4$ because the minimal polynomial of ω over $\mathbb{Q}$ is $x^4 + x^3 + x^2 + x + 1$ (irreducible as proved in homework), and $(\mathbb{Q}(\alpha)/\mathbb{Q}) = 5$ since the minimal polynomial of α over $\mathbb{Q}$ is $x^5 - 7$. Thus, 4 and 5 divide $(\mathbb{Q}(\alpha, \omega)/\mathbb{Q})$. On the other hand,

$$(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}) = (\mathbb{Q}(\alpha)/\mathbb{Q})(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}(\alpha)) \leq 20.$$

Therefore $(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}) = 20$.

6. Note that the roots of $x^{13} + 1$ are $-1, -\varepsilon, -\varepsilon^2, \cdots - \varepsilon^{12}$, where ε is the 13-th root of 1. Therefore $\mathbb{Q}(\varepsilon)$ is the splitting field of $x^{13}+1$. The degree $(\mathbb{Q}(\varepsilon)/\mathbb{Q}) = 12$, because the minimal polynomial for ε is

$$x^{12} + x^{11} + \cdots + 1.$$

7. Assume that the number of irreducible polynomials is finite. Let $p_1(x), \ldots, p_n(x)$ be all irreducible polynomial. Then

$$q(x) = p_1(x) \ldots p_n(x) + 1$$

must have an irreducible divisor but $p_i(x)$ do not divide $q(x)$. Contradiction.

8. Note that $\cos 60^\circ = \frac{1}{2}$. Use the formula

$$\cos 3\varphi = \cos^3\varphi - 3\cos\varphi\sin^2\varphi = \cos^3\varphi - 3\cos\varphi\left(1-\cos^2\varphi\right) = 4\cos^3\varphi - 3\cos\varphi.$$

Therefore

$$4\alpha^3 - 3\alpha - \frac{1}{2} = 0.$$

We claim that the minimal polynomial for α is $8x^3 - 6x - 1$. We need to check that it is irreducible. Make the substitution $x = \frac{y}{2}$. It suffices to show that $y^3 - 3y - 1$ is irreducible. Possible rational roots of $y^3 - 3y - 1$ are 1 and -1 but they are not roots by direct checking.