MAT313 Fall 2013

Practice Final

The actual final will consist of ten problems

Problem 1. Consider a strip of equally spaced letters

$$\cdots - \mathrm{O} - \mathrm{O} - \mathrm{O} - \mathrm{O} - \cdots$$

Describe the symmetry group of the strip. Is the group abelian?

Solution. The group is an infinite Dihedral group $< s, r | s^2 = 1, srs = r^{-1} >$. The element r corresponds to the shift symmetry. s is the reflection symmetry. □

Problem 2. Give four non isomorphic examples of groups of order eight. You must explain why the groups are mutually non isomorphic.

Solution. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$(all elements have order two), $\mathbb{Z}_4 \times \mathbb{Z}_2$(the group contains an element of order four),$\mathbb{Z}_8$(the group contains an element of order eight). Isomorphisms preserve order of elements. □

Problem 3. Find a group that contains elements a, b such that $|a| = |b| = 2$ and

(1) $|ab| = 3$
(2) $|ab| = 4$
(3) $|ab| = 30$

Solution. The group $D_{2n} =< r, s | r^n = 1, s^2 = 1, srs = r^{-1} >$ satisfies these requirements. The elements are $a = sr, b = s$ in groups D_6, D_8 and D_{60}. □

Problem 4. Suppose H is a proper subgroup of $\mathbb{Z}$ under addition and H is generated by $18, 30$ and 40. Determine H.

Solution. The group is generated by the greatest common divisor of $18 = 3^2 \times 2$, $30 = 2 \times 3 \times 5$ and $40 = 2^3 \times 5$, which is 2 □

Problem 5. List all the subgroups of $U(5)$

Solution. The multiplicative group of a finite field is cyclic. We conclude that $U(5) \cong \mathbb{Z}_4$. The subgroups are $\{1\}$, $\mathbb{Z}_2$ and $\mathbb{Z}_4$. □

Problem 6. List all elements of $\mathbb{Z}_{40}$ that have order ten.

Solution. Let x be a generator of $\mathbb{Z}_n$. Recall that $|x^a| = \frac{n}{(n,a)}$. In our case $n = 40$ and $|x^a| = 10$. Thus $(40, a) = 40/10 = 4$. and $(10, a/4) = 1$. Then $a/4 = 1, 3, 7, 9$ and $a = 4, 12, 28, 36$. □

Problem 7. Suppose $|x| = n$. Find a necessary and sufficient condition on s and t such that $(x^t) \subset (x^s)$.

Solution. This condition is $(s, n)|l$. Indeed if $(x^t) \subset (x^s)$ then $\exists a, (x^s)^a = x^l \Rightarrow x^{sa} = x^l \Rightarrow sa \equiv l \bmod n \Rightarrow \exists b, sa + nb = l \Rightarrow (s, n)|l$.

Conversely if $d = (s, n)|l \Rightarrow \exists a, b, k, kd = k(as + bn) = l \Rightarrow l \equiv (ka)s \bmod n \Rightarrow x^l = (x^s)^{ka} \Rightarrow (x^t) \subset (x^s)$. □

Problem 8. Determine the sign of the following permutations.

- (135)
- (1356)
- (13567)
- (12)(134)(152)
- (1243)(3521)

Solution. Recall that the sign of the permutation $\epsilon(\sigma)$ satisfies $\epsilon(\sigma_1\sigma_2) = \epsilon(\sigma_1)\epsilon(\sigma_2)$. If σ is a cycle of length n, then $\epsilon(\sigma) = (-1)^{n+1}$.

- $\epsilon(135) = 1$
- $\epsilon(1356) = -1$
- $\epsilon(13567) = 1$
- $\epsilon(12)(134)(152) = (-1) \times 1 \times 1 = 1$
- $\epsilon(1243)(3521) = (-1) \times (-1) = 1$

□

Problem 9. What is the order of

- (124)(357)
- (124)(35)
- (345)(245)

Solution. Let x_i be generators of $\mathbb{Z}_{n_i}$. We know that $(x_1, \dots x_k) \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ has the order equal to $lcm(n_1, \dots, n_k)$. From this we conclude that

- $|(124)(357)| = lcm(3, 3)$ because (124) and (357) commute and generate $\mathbb{Z}_3 \times \mathbb{Z}_3 \subset S_7$.
- $|(124)(35)| = lcm(3, 2) = 6$ because (124) and (35) commute and generate $\mathbb{Z}_3 \times \mathbb{Z}_2 \subset S_5$
- $|(345)(245)| = |(25)(34)| = lcm(2, 2) = 2$ because (25) and (34) commute and generate $\mathbb{Z}_2 \times \mathbb{Z}_2 \subset S_5$.Notice that we first rewrote (345)(245) as a product of commuting cycles.

□

Problem 10. Compute the centralizer of (12)(34) in S_4.

Solution. The following elements, besides 1 and (12)(34), commute with $\sigma =$ (12)(34): (13)(24), (14)(23). You have to finish this.

□

Problem 11. Prove that the group of nonzero complex number under multiplication is not isomorphic to the group of complex numbers under addition.

Solution. Elements of the form $e^{\frac{2\pi ik}{n}}$ have finite order in the multiplicative group $(\mathbb{C}^*, \times)$. The group $(\mathbb{C}, +)$ contains no such elements. □

Problem 12. Prove that the factor group of abelian group is abelian.

Solution. Let H be a (normal) subgroup of Abelian group G. By definition the product of two classes $xHyH$is equal to $xyH = yxH$. □

Problem 13. Let H be a normal subgroup of G and a be an element of G. If the element aH has order 3 in G/H and $|H| = 10$ what is the possibilities for the order of a.

Solution. Let $\psi : G \to G/H$ be the canonical homomorphism. Let $< \psi(a) >$ be a cyclic subgroup in G/H generated by $\psi(a)$ and K be the preimage of $< \psi(a) >$ in G. We have a homomorphism $K \to < \psi(a) >$ with a kernel H. We have $| < \psi(a) > | = 3$ and $|K| = | < \psi(a) > ||H| = 3 \times 10 = 30$. The element a generates a cyclic subgroup $< a >$ in K and its order should divide $|K| = 30$. Since we have an onto map $< a > \to < \psi(a) > 3 = |\psi(a)| \,|\, |a|$. Thus $|a| = 3k, 3k|30 \Rightarrow k|10 \Rightarrow k = 1, 2, 5, 10$ and $|a| = 3, 6, 15, 30$. □

Problem 14. Suppose $\mathbb{Z}_{10}$ and $\mathbb{Z}_{15}$ are homomorphic images of the group G. What can we say about $|G|$.

Solution. We conclude that $10||G|$ and $15||G|$ and $2 \times 3 \times 5||G|$. □

Problem 15. Determine all the homomorphisms of $\mathbb{Z}$ onto S_3. Determine all the homomorphisms of $\mathbb{Z}$ to S_3.

Solution. A homomorphisms $\psi : \mathbb{Z} \to G$ is completely determined by its value on the generator $x \in \mathbb{Z}$. If we know that $\psi(x) = a$ then $\psi(x^k) = a^k$. Thus there is one-to-one correspondence between homomorphisms of $\mathbb{Z}$ to G and elements of G. In our case $|G| = |S_3| = 6$ and we have 6 different homomorphism. However non of them are onto because G is noncommutative, but a factor-group of commutative $\mathbb{Z}$ must be commutative. □

Problem 16. Exhibit all Sylow 2-subgroups and Sylow 3-subgroups of D_{12} and $S_3 \times S_3$.

Solution. (1) The case $D_{12} =< s, r|s^2 = r^6 = 1, srs = r^{-1} >$. $|D_{12}| = 2^2 3$. The cyclic group $< r >$ is normal. It contains a normal subgroup of order 3 generated by r^2. Thus $n_3 = 1$. There is a commutative subgroup P_2 generated by s and r^3. Its all element have order two and $|P_2| = 4$.The subgroup is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 =< s, r^3 >$. It is one of the Sylow 2-subgroups. Subgroup $< r^3 >$ is invariant under conjugations, but $< s >$ is not. The conjugated subgroups $\{g^{-1} P_2 g\}$ are $\{< s, r^3 >, < r^{-2} s, r^3 >$

$, < r^{-4}s, r^3 >\}$. Additional consistency check: $n_2 = 1 + 2k$ $n_2||D_12| = 12$ and $n_2 \leq |D_12|/|P_2| = 3$. Possible values for n_2 are 1 and 3. We already found 3 distinct conjugated subgroup. Now we know that no subgroups were missed.

(2) The group S_3 contains one normal subgroup $\mathbb{Z}_3$ generated by $(1, 2, 3)$. It also contains 3 subgroups of order two $< (12) >, < (13) >, < (23) >$. We can use them to construct subgroups $P_3 = \mathbb{Z}_3 \times \mathbb{Z}_3 \subset S_3 \times S_3$ of oder 9 and $P_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \subset S_3 \times S_3$. The order of $S_3 \times S_3$ is $2^2 \times 3^2$. Thus P_2, P_3 are Sylow subgroups. The group P_3 is normal, therefore it is the only 3-subgroup. $n_2 = 1 + 2k$, $n_2 \leq 36/4 = 9$ and $n_2|9$. Thus $n_2 = 1, 3, 9$. Combining different $\mathbb{Z}_2 \subset S_3$ we obtain 9 subgroups in $S_3 \times S_3$ of order 4. Thus $n_2 = 9$ and our list is complete.

□

Problem 17. Prove that a group of order 56 has a normal Sylow p-subgroup for some prime p dividing its order.

Solution. The order of the group 56 factors into $2^3 \times 7$. Recall that the number n_p of Sylow p-subgroups satisfy $n_p \equiv 1 \text{mod } p$ and $n_p = \frac{|G|}{|N(P)|}$, where $N(P)$ is the normalizer of a Sylow p-subgroup P. In particular $n_p \leq \frac{|G|}{|P|}$ and $n_p||G|$. With this information we get $n_7 \in \{1, 8\}$ and $n_2 \in \{1, 3, 5, 7\}$. Divisibility constraint reduces the last set to $n_2 \in \{1, 7\}$. Suppose that $P \cong \mathbb{Z}_7$ is not normal. Then $n_7 = 8$. The group P has no subgroups. This is why $g^{-1}Pg$ do not intersect. The union $X = \bigcup_{g \in G} g^{-1}Pg$of these subgroup consists of one element of order 1 and 6×8 element of order 7. Note that Sylow two-subgroup contains no elements of order 7. It must be a subset of $Y = \{1\} \cup G \backslash X$. Note that $|Y| = 56 - 6 \times 8 = 8$. From this we conclude that $n_2 = 1$. □

Problem 18. (Chinese Remainder Theorem for Rings) If R is a commutative ring and A and B are two proper ideals with $A + B = R$, prove that $R/(A \cap B)$ is isomorphic to $R/A \times R/B$.

Solution. Consider the map $\psi : R \to R/A \times R/B$ defined by $\psi(r) = (r\text{mod}\, A, r\text{mod}\, B)$, where mod A means the class in R/A containing r (that is, $r + A$). This map is a ring homomorphism because ψ is just the natural projection of R into R/A and R/B for the two components. The kernel of ψ consists of all the elements $r \in R$ that are in A and in B, i.e. $A \cap B$. To complete the proof in this case it remains to show that when $A + B = R$, ψ is surjective and $A \cap B = AB$. Since $A + B = R$, there are elements $x \in A$ and $y \in B$ such that $x + y = 1$. This equation shows that $\psi(x) = (0, 1)$ and $\psi(y) = (1, 0)$ since, for example, x is an element of A and $x = 1y \in 1 + B$. If now $(r_1\text{mod}\, A, r_2\text{mod}\, B)$ is an arbitrary element in $R/A \times R/B$, then the element $r_2x + r_1y$ maps to this element since

$$\psi(r_2x + r_1y) = \psi(r_2)\psi(x) + \psi(r_1)\psi(y) =$$
$$= (r_2\text{mod}\, A, r_2\text{mod}\, B)(0, 1) + (r_1\text{mod}\, A, r_1\text{mod}\, B)(1, 0)$$
$$= (0, r_2\text{mod}\, B) + (r_1\text{mod}\, A, 0)$$
$$= (r_1\text{mod}\, A, r_2\text{mod}\, B).$$

This shows that ψ is indeed surjective. Finally, the ideal AB is always contained in $A \cap B$. If $A + B = R$ and x and y are as above, then for any $c \in A \cap B$, $c = c1 = cx + cy \in AB$. This establishes the reverse inclusion $A \cap B \subset AB$. □

Problem 19.

Find $x \in \mathbb{Z}_{105}$ such that

$$x \equiv 2 \text{ mod } 3$$
$$x \equiv 4 \text{ mod } 5$$
$$x \equiv 6 \text{ mod } 7.$$

Solution. Suppose $N = n_1 \dots n_k$ the product of relatively prime numbers n_i. We are given $a_i \in \mathbb{Z}_{n_i}$. By Chinese Remainder Theorem there is x such that $x \equiv a_i\text{mod}\, n_i$. We can recover x by the formula

$$x = \sum_i a_i \frac{N}{n_i} \left[\left(\frac{N}{n_i} \right)^{-1} \right]_{n_i}$$

Here how you should understand it: $\frac{N}{n_i}$ is relatively prime with n_i. It is invertible element in $\mathbb{Z}^*_{n_i}$. $\left[\left(\frac{N}{n_i}\right)^{-1}\right]_{n_i}$ is the integer mod n_i equal to the inverse. Note that by construction $a_i\frac{N}{n_i}\left[\left(\frac{N}{n_i}\right)^{-1}\right]_{n_i} \equiv a_i \text{mod } n_i$. On the other hand $n_j | a_i\frac{N}{n_i}\left[\left(\frac{N}{n_i}\right)^{-1}\right]_{n_i}$ for $j \neq i$. This is why $x \equiv a_i \text{mod } n_i$

In our case $\left[\left(\frac{105}{3}\right)^{-1}\right]_3 = 2$, $\left[\left(\frac{105}{5}\right)^{-1}\right]_5 = 1$ $\left[\left(\frac{105}{7}\right)^{-1}\right]_7 = 1$. and $x = 2 \times (5 \times 7) \times 2 + 4 \times (3 \times 7) \times 1 + 6 \times (3 \times 5) \times 1 = 314$ □

Problem 20. Determine whether the following polynomials are irreducible in the rings indicated.

(1) $x^4 + 10x^2 + 1 \in \mathbb{Z}[x]$.
(2) $x^4 + 1 \in \mathbb{Z}_5[x]$
(3) $x^4 - 4x^3 + 6 \in \mathbb{Z}[x]$.

Solution. (1) Possible rational roots (divisibility test $r = p/q$ is a root of $a_nx^n + \cdots + a_0$, then $p|a_0$ and $q|a_n$) are ± 1. By inspections these are not the actual roots. Remaining option is that $x^4 + 10x^2 + 1 = (ax^2 + bx + c)(ex^2 + fx + g)$. After expansion we immediately see that $a = 1, e = 1$ and $c = g = \pm 1$. Thus $x^4 + 10x^2 + 1 = (x^2 + bx + 1)(x^2 + fx + 1) = x^3(b + f) + x^2(bf + 2) + x(b + f) + x^4 + 1 \Rightarrow b = -f$ and $10 = 2 - b^2$. The last equation has no integral solutions. The case $(x^2 + bx - 1)(x^2 + fx - 1)$ is treated the same way.

(2) $x^4 = -1 \Rightarrow x^4 = 4 \Rightarrow x^2 = 2$ or $x^2 = -2 = 3$. The polynomials $x^2 - 2$ and $x^2 - 3$ have no roots in $\mathbb{Z}_5$. Therefore they are irreducible. We conclude that $x^4 + 1 = (x^2 - 2)(x^2 - 3) = (x^2 + 3)(x^2 + 2)$

(3) Irreducible. Use Eisenstein's criterion.

□

Problem 21. Prove that $U(20)$ and $U(24)$ are not isomorphic.

Solution. The isomorphisms of rings $\mathbb{Z}_{20} \to \mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_{24} \to \mathbb{Z}_3 \times \mathbb{Z}_8$ defines an isomorphism of groups of invertible elements $U(20) \to U(5) \times U(4)$, $U(24) \to U(3) \times U(8)$. The groups of invertible elements in the fields $\mathbb{Z}_3$ and $\mathbb{Z}_5$ are cyclic.

So $U(3) \cong \mathbb{Z}_2$ and $U(5) \cong \mathbb{Z}_4$. The group $U(4)$ contains two elements and must be isomorphic to $\mathbb{Z}_2$. In the group $U(8)$ all it elements satisfy $x^2 = 1$. It is generated by 3 and 5. Thus $U(8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

We conclude that

$$U(20) \cong U(5) \times U(4) \cong \mathbb{Z}_4 \times \mathbb{Z}_2$$

and

$$U(24) \cong U(3) \times U(8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

We see that $U(20)$ contains an element of order 4, whereas in $U(24)$ all elements have order two. □

Problem 22. Use the fact that $R = \mathbb{Z}[\sqrt{2}]$ is a Unique Factorization Domain to prove that $x^2 - \sqrt{2}$ is irreducible in $R[x]$.

Solution. We have a norm $N : R \to \mathbb{Z}$. For $\alpha = a + \sqrt{2}b$ defined by the formula $N(\alpha) = \alpha\bar{\alpha}$, where $\bar{\alpha} = a - \sqrt{2}b$. The norm satisfies $N(\alpha\beta) = N(\alpha)N(\beta)$. Suppose $x^2 - \sqrt{2} = (x - \alpha)(x - \beta)$. Then $-2 = N(-\sqrt{2}) = N(\alpha)N(\beta)$. We infer that $N(\alpha)$ or $N(\beta)$ is equal to ± 1. This means that one of them is a unit u and $\sqrt{2}$ is irreducible. We now want to use UFD property of the ring, which to us means that $\alpha = -u$ and $\beta = u^{-1}\sqrt{2}$. Thus $x^2 - \sqrt{2} = (x + u)(x - u^{-1}\sqrt{2}) = x^2 + (u - u^{-1}\sqrt{2})x - \sqrt{2}$. The middle term vanishes if $u^2 = \sqrt{2}$, which is impossible because u is a unit but $\sqrt{2}$ is not. □

Problem 23. Prove that the quotient ring $\mathbb{Z}[i]/I$ is finite for any nonzero ideal I of $\mathbb{Z}[i]$.

Solution. $\mathbb{Z}[i]$ is an Euclidean Domain with a norm $N(a + ib) = a^2 + b^2$. Then it is automatically a PID and every ideal has a form $< a >$ for some $a \in \mathbb{Z}[i]$. Let b be an arbitrary element in $\mathbb{Z}[i]$. Then $b = aq + r$, where $N(r) < N(a)$. This means that any class $b+ < a >$ has a representative $b+ < a >= aq + r+ < a >= r+ < a >$, whose norm is less then the norm $N(a)$. Notice that there is a finite number of elements of the lattice $\{x + iy | x, y \in \mathbb{Z}$ in the circle of radius $R^2 = N(a)$. Thus the number of r is finite. □

Problem 24. Let R be an integral domain. Prove that if the following two conditions hold then R is a Principal Ideal Domain:

(1) any two nonzero elements a and b in R have a greatest common divisor which can be written in the form $ra + sb$ for some $r, s \in R$, and

(2) if $a_1, a_2, a_3, \ldots$ are nonzero elements of R such that $a_{i+1}|a_i$ for all i, then there is a positive integer N such that an is a unit times a_N for all $n > N$.

Solution. Let I be an ideal of R. We want to show that $\exists a$ such that $< a >= I$. Let a_1 be some element in I. Then $< a >\subset I$. If $< a >= I$ we stop. Otherwise we choose $b \in I, b \notin < a_1 >$. The first condition allows us to choose $a_2 = ra_1 + sb$ which is a generator of $< a_1, b >$. We continue this way and get a sequence of ideals $< a_1 >\subset< a_2 >\subset \cdots \subset< a_n >\subset I$. Then we must have $a_2|a_1, \ldots, a_{i+1}|a_i \ldots$. By the second assumption $\exists N$ such that $a_{N+i} = u_i a_N$, where u_i are units. Thus $< a_N >=< a_{N+i} >= I$. □